

# StorageTek Virtual Tape Library VTL Prime

---

User's Guide

Version 1.1



Part Number: 316198201  
September 2010  
Revision AE

Submit comments about this document by clicking the Feedback [+] link at: <http://docs.sun.com>



Copyright © 2005, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.



## Revision History

---

Name	Part #	Revision	Date	Comments
VTL Prime 1.1 User's Guide	316198201	AA	September 2009	Initial release.
	316198201	AB	December 2009	Added Error Codes section.
	316198201	AC	January 2010	Added Reclamation thresholds and Manual reclamation procedure.
	316198201	AD	June 2010	Rebranding.
	316198201	AE	September 2010	Added SNMP Messages.



# Contents

---

## Preface

Related Documentation . . . . .	xiii
Documentation, Support, and Training . . . . .	xiv
Oracle Welcomes Your Comments . . . . .	xiv

## Introduction

Important Note about ECO references in this document . . . . .	1
Oracle's StorageTek Virtual Tape Library overview . . . . .	1
VTL components . . . . .	1
Sun VTL Operational Restrictions . . . . .	2

## Getting Started

Obtain VTL Prime Licensing Keys . . . . .	3
Obtain VTL Appliance Network Information . . . . .	3
Install the VTL console on an administrative computer . . . . .	3
Start the vtconsole (VTL GUI) utility . . . . .	4
Load VTL console software on a laptop or workstation . . . . .	4
Connect to the VTL server . . . . .	4
Launch the VTL Console . . . . .	5
Configure your VTL server using the configuration wizard . . . . .	6
Step 1: Enter license keys . . . . .	6
Step 2: Set up network . . . . .	6
Step 3: Set hostname . . . . .	8
Step 4: Enable Fibre Channel . . . . .	9
Step 5: Switch to target mode . . . . .	9
Step 6: Prepare devices for virtual libraries . . . . .	10
Step 7: Create Virtual Tape Library database . . . . .	10
Step 8: Create virtual libraries . . . . .	11
Step 9: Add SAN clients . . . . .	11
Step 10: Assign virtual library to clients . . . . .	12
Step 11: Enable deduplication . . . . .	12
Step 12: Create deduplication policy . . . . .	13
Prepare for backups . . . . .	14
Backup server access to the VTL server . . . . .	14
FC backup servers . . . . .	14
iSCSI backup servers . . . . .	14
Discover the virtual tape library from your backup server . . . . .	15
Create and run backup jobs . . . . .	17

---

Confirm successful backups .....	18
----------------------------------	----

## **VTL Console**

Launch the console .....	19
Connect to your VTL server .....	19
VTL console user interface .....	20
Understanding the objects in the tree .....	21
Server object .....	21
Virtual Tape Library System object .....	22
Virtual Tape Libraries .....	22
Virtual Tape Drives .....	22
Virtual Vault .....	22
Replica Resources .....	23
Deduplication Policies .....	23
Database .....	23
Virtual tape icons .....	23
Disk Resources object .....	23
SAN Clients object .....	24
Reports object .....	24
Physical Resources object .....	24
Physical resource icons .....	25
Rescan physical devices .....	25
Console options .....	27
System maintenance .....	28
Network configuration .....	28
Set hostname .....	28
Set date and time .....	28
Restart server .....	28
Restart network .....	28
Reboot .....	28
Halt .....	28
Administrators .....	29
Event Log .....	30
Sort the Event Log .....	30
Filter the Event Log .....	30
Export data from the Event Log .....	30
Print the Event Log .....	31
Clear the Event Log .....	31
Reports .....	32
Create a report .....	33
View a report .....	34
Schedule a report .....	34
Export data from a report .....	34
Set report properties .....	35
Email a report .....	36
Refresh report display .....	36
Delete a report .....	36
Attention Required tab .....	37

---

Performance statistics . . . . .	38
Server properties . . . . .	39
Software patch updates . . . . .	40
SNMP traps . . . . .	41
Mirror the VTL database to protect your VTL configuration . . . . .	42
Check mirroring status . . . . .	42
Replace a failed disk . . . . .	43
Fix a minor disk failure . . . . .	43
Replace a disk that is part of an active mirror configuration . . . . .	43
Swap the primary disk with the mirrored copy. . . . .	43
Remove a mirror configuration . . . . .	43

## Manage Tape Drives and Tapes

Create virtual tape libraries . . . . .	44
Create virtual tapes . . . . .	48
How virtual tapes are allocated from multiple LUNs . . . . .	50
Round Robin Logic with Tape Capacity on Demand disabled . . . . .	50
Round Robin Logic with Tape Capacity on Demand enabled . . . . .	50
Considerations . . . . .	51
Locate and display virtual tapes in the console . . . . .	51
Search by barcode . . . . .	51
Display virtual tapes . . . . .	51
Sort all tapes . . . . .	52
Filter the display of tapes . . . . .	52
Add SAN Clients (backup servers) . . . . .	55
Assign virtual tape libraries to clients . . . . .	57

## Data Deduplication

Enable deduplication . . . . .	61
Replicating the deduplication repository . . . . .	62
Requirements . . . . .	63
Connect appliances . . . . .	64
Add the replication target server . . . . .	64
Data deduplication policies . . . . .	66
Add deduplication policies . . . . .	66
Modify deduplication policies . . . . .	69
Perform deduplication . . . . .	69
Monitor deduplication and view statistics . . . . .	70
Deduplication Policies object . . . . .	70
Individual deduplication policies . . . . .	71
Repository statistics . . . . .	75
Reclaim disk space . . . . .	77
Reclamation thresholds . . . . .	77
Manual reclamation . . . . .	78

---

## Data Replication

Auto Replication	.80
Remote Copy	.81
Replication of virtual tapes	.82
Remote Replication	.82
Local Replication	.82
Replication of deduplicated tapes	.84
Replication requirements	.86
Configure replication for virtual tapes	.88
Configure replication for deduplicated tapes	.94
Add the replication target for ECO data	.94
Replicating deduplicated tapes from a server using an alternate NIC	.96
Check replication status	.99
Promote a replica resource	.101
Promote a replica resource without breaking the replication configuration	.101
Access data on a replicated virtual tape	.102
Change your replication configuration options	.102
Suspend/resume replication schedule	.102
Stop a replication in progress	.103
Manually start the replication process	.103
Remove a replication configuration	.103
Consolidate tapes from multiple locations to a single data center	.106

## Fibre Channel Configuration

Overview	.107
Installation and configuration overview	.107
Configure Fibre Channel hardware on server	.109
Ports	.109
Zoning	.109
Switches	.110
Persistent binding	.111
Configure Fibre Channel hardware on clients	.112
NetWare clients	.112
HBA settings for Fibre Channel clients	.113
Windows 2000/2003	.113
HP-UX 10, 11, and 11i	.114
AIX 4.3 and higher	.114
Linux – all versions	.114
Solaris 7, 8, 9, and 10	.115
NetWare – all versions	.115
Verify your hardware configuration	.116
Set QLogic ports to target mode	.119
Single port QLogic HBAs	.119
Associate World Wide Port Names with clients	.120

---

## iSCSI Clients

Overview	122
Supported platforms	122
iSCSI users	122
Windows configuration	123
Requirements	123
Prepare client initiators to access your VTL server	123
Enable iSCSI	123
Add an iSCSI client	124
Create targets for the iSCSI client to log onto	125
Assign a virtual tape library to the iSCSI target	126
Log the client onto the target	126
Disable iSCSI	126
Linux client configuration	127
Prepare the iSCSI initiator	127
Enable iSCSI	127
Add an iSCSI client	127
Create targets for the iSCSI client to log onto	128
Assign a virtual tape library to the iSCSI target	128
Log the client onto the target	128

## Email Alerts

Configure Email Alerts	129
Modify Email Alerts properties	133
Script/program trigger information	134
Customize email for a specific trigger	134
New script/program	134

## VTL Server

Start the VTL server	137
Restart the VTL server	137
Check the VTL Server processes	138
Stop the VTL Server	139

## Command Line

Using the command line utility	140
Commands	140
Common arguments	141
Login/logout to the VTL Server	142
Virtual devices / Clients	143
System configuration	157
Replication	159
Physical devices	166
Event Log	169

---

Reports .....	170
Technical support .....	178
Deduplication .....	179

## **Appendix**

System security .....	182
LUN migration .....	183
SNMP Messages .....	185
Critical Messages .....	185
Error Messages .....	186
Information Messages .....	213
Warning Messages .....	233

## **Troubleshooting**

General console operations .....	238
Physical resources .....	240
Logical resources .....	241
Replication .....	244
Take an X-ray of your system for technical support .....	245

## **Error Codes**

VTL Prime Error Codes .....	246
-----------------------------	-----

## **Index**

# Preface

---

This book guides you through the configuration and usage of Oracle's StorageTek VTL Prime appliance. The book has been designed for anyone who is engaged in configuring, administering and using the VTL Prime appliance.

## Related Documentation

The following list contains the name and part number of publications that provide additional information about VTL Prime.

This documentation is available for authorized service personnel at:

<http://docs.sfbay.sun.com/app/docs/prod/tape.virtual#hic>

Function	Title	Part Number
Installation	VTL Prime 1.1 Installation Manual	316197801

---

## Documentation, Support, and Training

Function	URL
Web Site	<ul style="list-style-type: none"><li>• <a href="http://www.oracle.com/index.html">http://www.oracle.com/index.html</a></li></ul>
Documentation	<ul style="list-style-type: none"><li>• Customer: <a href="http://docs.sun.com">http://docs.sun.com</a></li><li>• Employee: <a href="http://docs.sfbay.sun.com/">http://docs.sfbay.sun.com/</a></li><li>• Partner: <a href="https://spe.sun.com/spx/control/Login">https://spe.sun.com/spx/control/Login</a></li></ul>
Downloads	<ul style="list-style-type: none"><li>• Customer: <a href="http://www.sun.com/download/index.jsp">http://www.sun.com/download/index.jsp</a></li><li>• Employee: <a href="https://dlrequest-zn-dlapps1.sfbay.sun.com/usr/login">https://dlrequest-zn-dlapps1.sfbay.sun.com/usr/login</a></li></ul>
Support	<ul style="list-style-type: none"><li>• <a href="http://www.sun.com/support/">http://www.sun.com/support/</a></li></ul>
Training	<ul style="list-style-type: none"><li>• <a href="http://www.oracle.com/global/us/education/sun_select_country.html">http://www.oracle.com/global/us/education/sun_select_country.html</a></li></ul>
Online Account	<ul style="list-style-type: none"><li>• <a href="https://reg.sun.com/register">https://reg.sun.com/register</a></li></ul>

## Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions. Submit your comments by clicking the Feedback[+] link at:

<http://docs.sun.com>

Please include the title and part number of your document with your feedback:

*VTL Prime 1.1 User's Guide, 316198201*

# Introduction

---

## Important Note about ECO references in this document

This document describes Oracle's StorageTek™ VTL Prime 1.1 and also makes occasional reference to the Enterprise Capacity Optimizer (ECO) data deduplication feature. ECO is not included in VTL Prime 1.1. Please disregard references to ECO in this document.

## Oracle's StorageTek Virtual Tape Library overview

Oracle's StorageTek Virtual Tape 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 a physical tape library really has, more backup streams can run simultaneously, enabling organizations to easily complete their backups within the allotted backup window.

## VTL components

There are several components to VTL:

- VTL Server - Manages the VTL system, which comprises Virtual Tape Library functionality.
- VTL storage - Storage used by VTL, including the VTL database and VTL storage.
- VTL Console - The graphical administration tool where you configure VTL, add/configure clients, configure replication and deduplication and monitor their processes, and set properties and manage storage.
- VTL Clients - The backup servers that use the VTL. VTL supports Fibre Channel and iSCSI backup servers on most major platforms.

---

## Sun VTL Operational Restrictions

VTL Prime and VTL Plus 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. Do not rely on general email aliases like vtl@sun.

# Getting Started

---

The following steps guide you through configuring your VTL Prime appliance.

## Obtain VTL Prime Licensing Keys

VTL license keys must be activated during the configuration process. You should obtain these keys before you perform the configuration steps that follow.

1. License keys are obtained from <http://www.sun.com/storagetek/support/index.jsp>
2. On the Sun Storage Support page, click on More under Software keys to display the License Key window.
3. On the License Keys window, click on VTL & IPSTOR Key.
4. A key request form will appear. Complete the form and click on the Submit button at the bottom of the screen. After submitting the form, a confirmation email will be sent to the email address provided.

## Obtain VTL Appliance Network Information

Contact your network administrator to obtain the following:

- IP address
- Netmask
- Default gateway
- Primary name server information

## Install the VTL console on an administrative computer

The VTL console is the graphical administration tool where you can manage your VTL server. The computer that runs the VTL 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.

---

## Start the vtconsole (VTL GUI) utility

On the VTL server or a Solaris workstation with vtconsole installed, change the directory location to the directory where the vtconsole program resides and start the vtconsole GUI:

```
cd /usr/local/vtconsole
./vtconsole&
```

If you need to install vtconsole on a laptop or workstation, follow the procedure below.

## Load VTL console software on a laptop or workstation

VTL Console can be installed on any number of laptops or workstations provided they have a graphical user interface.

1. Transfer the Console1813.zip file from the VTL Prime server's /Software directory to a laptop or workstation.
2. Unzip the file.
3. Install the software.

Go to the Solaris directory and run:

```
# pkgadd -d vtconsole - 5.01-1813.i386.pkg
```

4. Start the VTL console.

Go to /usr/local/vtconsole and type:

```
# ./vtconsole &
```

## Connect to the VTL server

Either set your laptop or workstation to an IP address compatible with the private IP addresses pre-configured for the VTL servers or use ILOM if the ILOM Network Management (NetMGT) port has been configured with an IP address compatible with the customer LAN.

If logging into the VTL server using ILOM, you may use the root userid.

If logging into the VTL server using ssh from a workstation configured on the private network, use the vtladmin userid and once logged in, use the *su* command to become the root userid.

IP addresses pre-configured on the VTL Prime servers:

- nge0 or e1000g0: 10.0.0.10
- Net Management port (ILOM): 10.0.0.100
- Disk controllers: 10.0.0.1 and up, to the number of controllers in the solution.

---

Do not edit the Solaris network flat files (/etc/inet/hosts, /etc/inet/ipnodes, /etc/netmasks etc.) to change the IP address. Use the VTL console step in the Wizard that updates the hostname and IP address of the VTL server to a value supplied by the customer.

Since there is no current configuration, the VTL Configuration Wizard appears once the connection has been established to the server.

Exit this wizard by clicking on the *Cancel* button.

## Launch the VTL Console

To launch the console, select *Start --> Programs --> Sun Microsystems--> VTL 5.10 --> VTL console*.

If your server already appears in the tree, right-click it and select *Connect*.

If your server does not appear in the tree, do the following to add it:

1. Right-click the *Servers* object and select *Add*.

If you are running on a Windows machine, you can right-click the *Servers* object and select *Discover* to detect servers in a range of IP addresses. You should then specify the subnet range of your server and wait for the server hostname to appear in the navigation tree.

2. Type the server name or address (for example, 10.7.12.91) and enter a valid user name and password (both are case sensitive) to log in.

Once you are connected to a server, the server icon will change to show that you are connected:



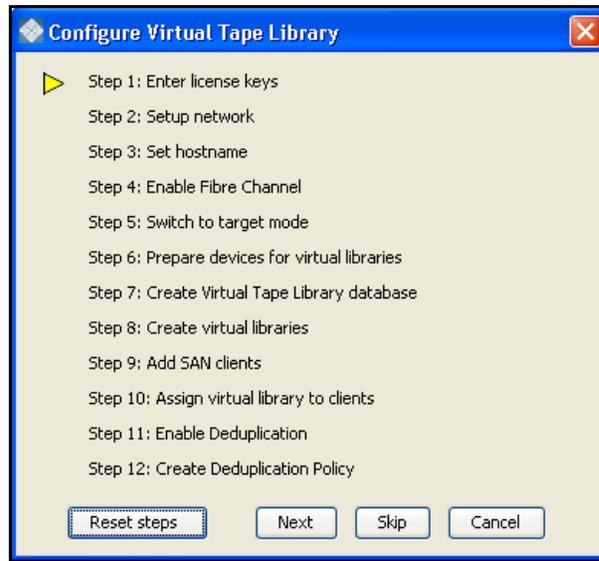
The VTL Configuration Wizard appears once the connection has been established to the server. You will perform configuration steps using this wizard.

---

## Configure your VTL server using the configuration wizard

**Note:** If you are using VTL in a Fibre Channel environment, refer to the “[Fibre Channel Configuration](#)” section first before beginning the wizard.

Virtual Tape Library (VTL) provides a convenient wizard that leads you through your VTL configuration. If your VTL server has not been configured yet, the configuration wizard will be launched when you connect to it.



3. Click *Next* to begin the steps in the wizard and to progress from one step to another.

If you want to skip a step, click *Skip*.

### *Step 1: Enter license keys*

Click the *Add* button and enter your keycodes.

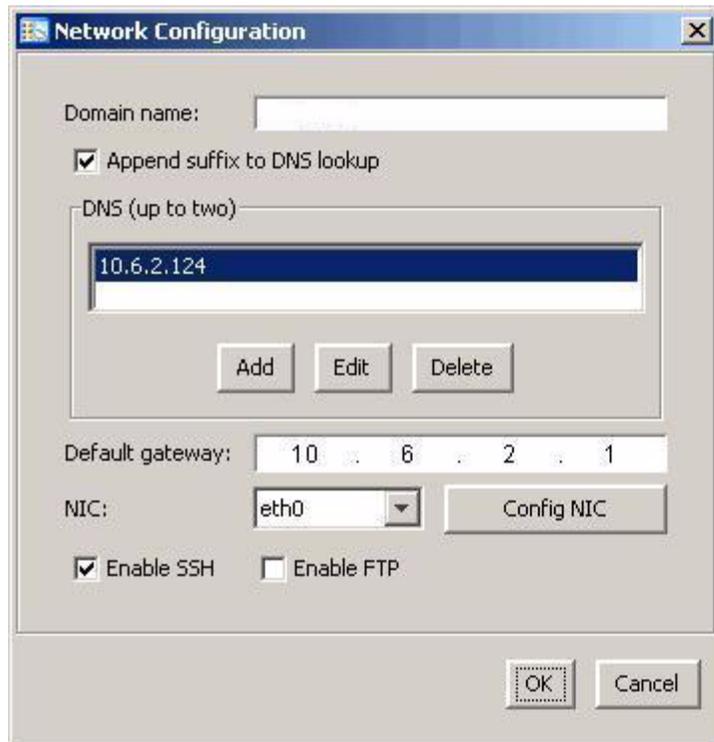
Be sure to enter keycodes for any options you have purchased. Each VTL option requires that a keycode be entered before the option can be configured and used.

- ➡ **Configuration note:** After completing the configuration wizard, if you need to add license keys, you can right-click the VTL server object in the console and select *License*.

### *Step 2: Set up network*

1. Enter information about your network configuration.

**Note:** Some of this information is pre-configured for the VTL Prime appliance.



*Domain name* - Internal domain name.

*Append suffix to DNS lookup* - If a domain name is entered, it will be appended to the machine name for name resolution.

*DNS* - IP address of your Domain Name Server.

*Default gateway* - IP address of your default gateway.

*NIC* - List of Ethernet cards in the server.

*Enable SSH* - Enable/disable the ability to use the SSH protocol. The VTL server must have “openssh” installed in order to use SSH.

*Enable FTP* - Enable/disable the ability to FTP into the server. The VTL server must have “vsftpd” installed in order to use FTP.

2. Click *Config NIC* to configure each network interface card (NIC).



If you select *Static*, you must click the *Add* button to add IP addresses and subnet masks.

*MTU* - Set the maximum transfer unit of each IP packet. If your card supports it, set this value to 9000 for jumbo frames.

- ➔ **Configuration note:** After completing the configuration wizard, if you need to change these settings, you can right-click the VTL server object in the console and select *System Maintenance --> Network Configuration*.

### Step 3: Set hostname

Enter a valid name for your VTL appliance.

Valid characters are letters, numbers, underscore, or dash. The server will automatically reboot when the hostname is changed.



- ➔ **Configuration note:** After completing the configuration wizard, if you need to change the name again, you can right-click the VTL server object in the console and select *System Maintenance --> Set Hostname*.

## Step 4: Enable Fibre Channel

Before you enable Fibre Channel, verify that your Fibre Channel configuration is set properly. Refer to the [“Fibre Channel Configuration”](#) section for information.

(FC edition only) This step takes just a few seconds and there are no additional screens to go through.

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*.

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. For security purposes, you should assign specific WWPNs to specific clients.

## Step 5: Switch to target mode

(FC edition only) Target mode allows a port to receive requests from your backup server(s).

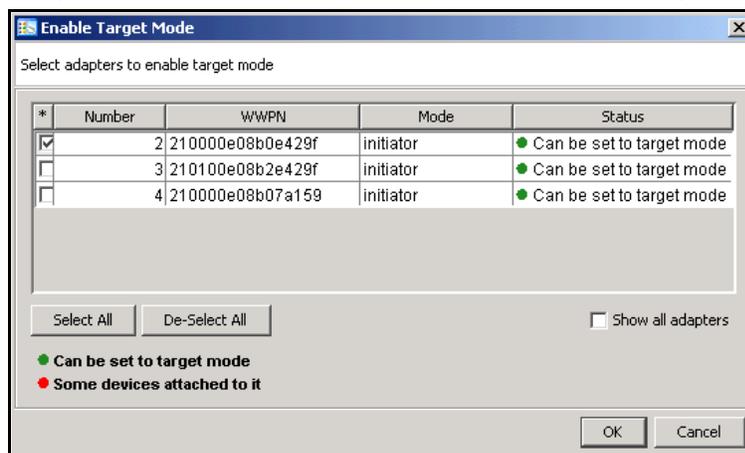
In order to identify your ports, you need to know the WWPN of each. One way to find the WWPN is through the SNS table at your Fibre Channel switch.

Alternatively, for QLogic HBAs, you can find the WWPN in the BIOS (press Ctrl+Q during boot up).

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

You will get a *Link Up* message on your VTL server if a QLogic port has successfully been placed in target mode.

(Single-ID HBAs) Select which ports should be in target mode.



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.

- ➡ **Configuration note:** After completing the configuration wizard, if you need to switch a port's mode, you can right-click the adapter and select *Enable/Disable Target Mode*.

## Step 6: Prepare devices for virtual libraries

This step takes just a few seconds and there are no additional screens to go through.

- ➡ **Configuration note:** After completing the configuration wizard, if you add new hardware that you need to prepare, you can right-click *Physical Resources* and select *Prepare Devices*. Hard drives should be set to *Reserved for Virtual Device* while tape libraries/drives should be set to *Reserved for Direct Device*. You may need to [Rescan physical devices](#) if all devices are not shown.

## Step 7: Create Virtual Tape Library database

1. Select how you want to create the Virtual Tape Library database.

The Virtual Tape Library's Database Resource needs at least 6,015 MB of disk space. The Database Resource contains the configuration information for the VTL.

*Custom* lets you select which physical device(s) to use and lets you designate how much space to allocate from each (use 10 GB LUNs).

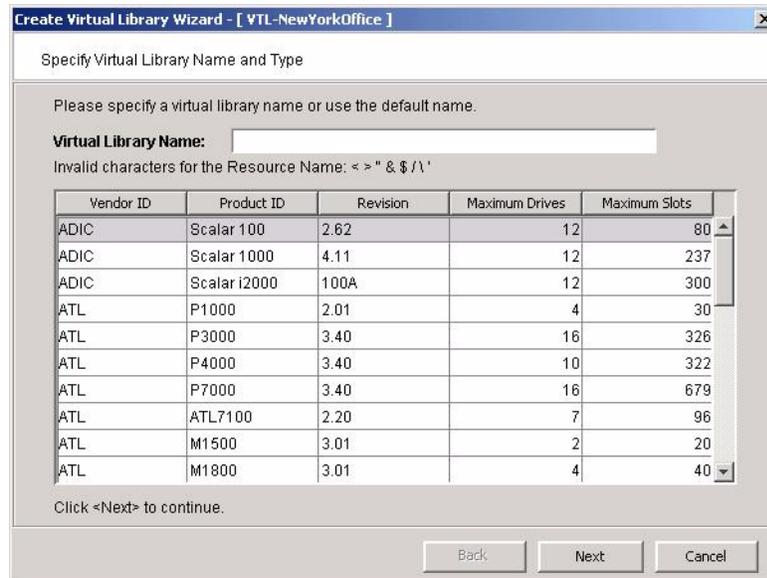
*Express* automatically creates the resource for you using an available device(s).

2. Click *Finish* to create the database.

You will be asked if you want to mirror the database. Refer to '[Mirror the VTL database to protect your VTL configuration](#)' for more information.

## Step 8: Create virtual libraries

Select the Sun tape library that you are emulating.



You will have to enter information about the tape drives in your library, including:

- Barcode information
- Tape properties such as Tape Capacity On Demand and maximum tape capacity.
- Determine if you want to use auto replication for this virtual library.

Refer to '[Create virtual tape libraries](#)' for detailed information about creating virtual tape libraries.

After you create a virtual tape library you will be prompted to create new virtual tapes. Refer to '[Create virtual tapes](#)' for detailed information about creating virtual tapes. After you create virtual tapes, you will be prompted to create more virtual libraries or to continue with the next step.

## Step 9: Add SAN clients

This step allows you to select the type of clients (backup servers) to which you will be assigning a tape library.

Refer to '[Add SAN Clients \(backup servers\)](#)' for detailed information about adding clients.

- ➡ **Configuration note:** After completing the configuration wizard, if you need to add new clients, you can right-click *Virtual Tape Library System* and select *Configuration wizard* or you can right-click the *SAN Clients* object and select *Add*.

---

## Step 10: Assign virtual library to clients

1. Select a client to assign.
2. Click *Finish* when you are done.

 **Configuration note:** After completing the configuration wizard, if you need to assign new virtual libraries, you can right-click *Virtual Tape Library System* and select *Configuration wizard* or you can click a virtual tape library or a client and select *Assign*.

## Step 11: Enable deduplication

1. From the SIR Repository Window, select the SIR Repository Storage Method:
  - **Physical Device:** The qualified physical devices are virtualized physical disks without any segments.
  - **Virtual Device:** The qualified virtual devices are the ones with a name in the front.

Index: SIR\_Index\_<Hostname>\_<SequenceNumber>

Data: SIR\_Data\_<Hostname>\_<SequenceNumber>\_<StartSlice>\_<EndSlice>

2. Before enabling Deduplication Cluster, enable the Configuration Repository option.
3. Select the SIR\_Index and click Next.
4. Select the SIR Data to be used from the displayed menu box and click Next.
5. A Single Instance Repository window opens with the following statement:  
Hash codes are evenly distributed among cluster members and are further distributed among physical devices most efficiently, it is best to have disks of equal size.  
In addition, the quantity of disks should be represented by 2 to the Nth power (for example 2, 4, 8, or 16 disks). The current configuration does not meet this recommendation.  
Do you want to continue with your current configuration?

6. Select yes, and continue.

A new Single Instance Repository window is displayed.

7. Choose a disk/hash scenario for the configuration.

For example:

Sun27

Hash range: 0 – F; total of 16 drives

Scenario 1: 16 slices; 1 hash per drive; all drives used

Scenario 2: 8 slices; 2 hashes per drive; all drives used

Scenario 3: 4 slices; 4 hashes per drive; all drives used

Scenario 4: 2 slices; 8 hashes per drive; all drives used

Scenario 5: 1 slice; 16 hashes per drive; all drives used

The recommended choice for:

- 
- Models 4365 and 4329 is 8 hashes per drive (Scenario 4) to take advantage of all the drives in a customer configuration.
  - Models 4320, 4310, 4305, and 4302 should use 4 hashes per drive; however, depending on the configuration, a 16 hash per drive solution may take better advantage of all the drives.
8. After making the selection, click next.  
You will be asked to confirm the selection.
  9. Click finish to enable the configuration.  
At this point the SIR Repository is created.  
The Single Instance Repository Cluster window shows the status as the repository is being created.

### *Step 12: Create deduplication policy*

This step displays the Deduplication Policy wizard, which lets you specify which virtual tapes need to have deduplication and when deduplication should occur. You must have at least one virtual tape library in order to create a policy (refer to '[Data deduplication policies](#)' for details on creating deduplication policies).

---

## Prepare for backups

### *Backup server access to the VTL server*

There are two access schemes that determine how backup servers access the VTL server:

- In the "Open Access" scheme, access is controlled purely by zoning. The pre-defined *Everyone\_iSCSI* or *Everyone\_FC* client represents the backup server and all or some of your virtual tape libraries/drives must be assigned to the *Everyone* client.
- In the "Secured Access" scheme, access is dictated by creating specific clients to represent specific backup servers instead of using the built-in *Everyone\_iSCSI* or *Everyone\_FC* client. In this mode, each backup server can access *only* its own designated virtual tape library or drives.

**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. For security purposes, you should assign specific WWPNs to specific clients.

### *FC backup servers*

In order for Fibre Channel backup servers to access VTL resources, you must do the following:

1. Set QLogic HBA ports to target mode.
2. Add a FC client for each backup server ("Secured Access").
3. Create and assign a virtual tape library to clients.
4. Discover the virtual tape library from your backup server.

Refer to '[Discover the virtual tape library from your backup server](#)' for more information.

Additional information about steps 1-3 can be found in the '[Fibre Channel Configuration](#)' chapter.

### *iSCSI backup servers*

In order for iSCSI backup servers to access VTL resources, you must do the following:

1. Add an iSCSI client for each backup server ("Secured Access").
2. Create targets for the iSCSI client to log into.
3. Create and assign a virtual tape library to the iSCSI target.

- 
4. Register client initiators with your VTL server.
  5. Log the client onto the target.
  6. Discover the virtual tape library from your backup server.

Refer to '[Discover the virtual tape library from your backup server](#)' for more information.

Additional information about steps 1-5 can be found in the '[iSCSI Clients](#)' chapter.

## *Discover the virtual tape library from your backup server*

To enable your backup server to recognize the default virtual tape library and drives, perform a device scan on your backup server at the operating system level and then use your backup software to scan for new devices as well.

Use your operating system to scan for hardware changes

The steps to do this vary according to the backup server's operating system.

For Fibre Channel environments, if your zoning has been correctly configured, and devices have been properly assigned to clients, a simple bus rescan performed on the client should show the new backup devices. Of course, this procedure varies depending on the OS.

Windows

To discover a tape library on a backup server running a Windows operating system:

1. Select *Control Panel --> Administrative Tools --> Computer Management*.
2. In the left pane, under *System Tools*, select *Device Manager*.
3. In the right pane, right-click the backup server and select *Scan for hardware changes*.

New devices representing the specific VTL resources will appear (the library under *Medium Changers* and tape drives under *Tape Drives*) and if the appropriate tape drive and tape library device drivers are installed on the backup server, the correct device name and type are associated and the devices will become ready for use by the backup software.

If a new device is unknown, right-click it to display its *Properties*. Acquire and update the driver according to your Windows documentation. Your backup software may include a procedure that updates drivers.

Linux

To discover a tape library on a backup server running a Linux operating system:

1. Rescan your host adapter.

Rescanning in Linux is host adapter-specific. For QLogic:

```
echo "scsi-qlascan" > /proc/scsi/qla<model no>/<adapter-instance>
```

For Emulex:

```
sh force_lpfsc_scan.sh "lpfc<adapter-instance>"
```

- 
2. Identify the detected devices.

```
# cat /proc/scsi/scsi
```

3. For each identified device do the following:

```
# echo "scsi add-single-device <host> <channel> <id> <lun>" >/proc/scsi/scsi
```

where *<host>* is the host adapter number, *<channel>* is channel number *<id>* is the target id and *<lun>* is the LUN number.

HP-UX To discover a tape library on a backup server running HP-UX:

1. Rescan the devices.

```
# ioscan -fnC <tape>
```

2. Generate device files.

```
# insf -e
```

3. Verify the new devices.

```
# ioscan -funC <tape>
```

AIX To discover a tape library on a backup server running AIX:

1. Rescan devices.

```
# cfgmgr -vl fcsX
```

where *X* is the number of the FC adapter.

2. Verify the new devices.

```
# lsdev -Cc <disk|tape>
```

Solaris 1. Determine the FC channels.

```
# cfgadm -al
```

2. Force a rescan.

```
cfgadm -o force_update -c configure cX
```

where *X* is the FC channel number.

3. Install device files.

```
# devfsadm
```

Use backup software to detect new devices

The steps to do this vary according to your backup software.

After you complete the procedure, you are ready to create and run backup jobs.

For all other platforms, such as Unix and Linux, consult the appropriate reference material that came with your backup software for details on how to load drivers and how to perform discovery for hardware changes.

---

## Create and run backup jobs

Once your backup server software can discover and access the virtual tape library/ drives defined in the VTL Server, you can start to use the VTL as if it were a real tape library.

The preparation required to start a backup job successfully is identical whether you are using a real tape library or a virtual one. You simply configure the backup software to use the VTL just like you would a physical tape library.

Generally, in order to perform a backup to a newly acquired/configured tape library, you need to:

1. Add new tape media.
  - Real library: Buy new tapes and insert into the mail slot followed by a sequence of keys pressed on the keypad of the tape library.
  - VTL: Virtual tapes are typically created when you create a virtual tape library. Additional virtual tapes can be created as needed.
2. Start a "tape inventory" process in your backup software.
3. Format the tapes and assign them into various "tape pools".
4. Define backup jobs and associate tapes with each job.

When one or more backup jobs start to kick-off, tapes are allocated by the backup software and are loaded into the tape drives. Backup data is then sent to the tapes until the backup job is done. The backup software then sends commands to unload the tapes and return them to their assigned slot within the library. All of the above actions are emulated by VTL.

When it is time to remove a tape from a physical library and to store it onto a nearby tape shelf, the administrator must physically walk over to the library, use a key pad/console to select the tape to be removed, and then catch the tape as it is physically being ejected from the "mail slot". The above can sometimes be done via commands from within the backup software.

For a VTL server, obviously there is no keypad or physical mail slot for this purpose. However, the Sun StorageTek VTL server has a *Virtual Tape Vault* to hold all the virtually "ejected" tapes from any virtual tape library. In the case where an "eject" is performed by the backup software, the ejected virtual tape will be automatically placed in the Virtual Tape Vault. This can be confirmed using the VTL console (select the *Virtual Tape Vault* object and verify the virtual tape is indeed there). If tape removal is not done using the backup software, the equivalent of a "keypad" is to use the VTL console and right-click the virtual tape and select *Move to Vault*.

Typically, after the backup is complete, the backup software will automatically remove the tape from the drive and store it back in its assigned library slot.

---

## Confirm successful backups

While a backup job is running, you can use the VTL console to verify that data is being written to virtual tapes.

1. In the VTL console, expand the *Virtual Tape Library System* object.
2. Expand *Virtual Tape Libraries*, the specific library, and then *Tapes*.
3. Under the *Tapes* object, select each tape that is included in a backup job.

In the right-hand pane, you should see a value for *Data Written*, which updates dynamically during a backup job.

After the backup job completes, use your backup software to verify that the data was written completely and can be restored.

# VTL Console

---

The VTL console is the administration tool that allows you to manage your VTL appliance. It is a graphical administration tool that can be used to configure VTL, add/configure clients, and set properties, as well as run/view reports, enter licensing information, and add/delete administrators.

## Launch the console

To launch the console, select *Start --> Programs --> Sun Microsystems --> VTL 5.10 --> VTL console*.

## Connect to your VTL server

1. Right-click your VTL server and select *Connect*.

If you want to connect to a server that is not listed, right-click the *Servers* object and select *Add*.

If you are running on a Windows machine, you can right-click the *Servers* object and select *Discover* to detect servers in a range of IP addresses.

2. Enter a valid user name and password (both are case sensitive).

Once you are connected to a server, the server icon will change to show that you are connected:



**Note:** Two administrators can access a server at the same time. Changes to the server's configuration are saved on a first-come, first-served basis.

3. Two administrators can access a server at the same time. Changes to the server's configuration are saved on a first-come, first-served basis.

The VTL console remembers the servers to which the console has successfully connected. If you close and restart the console, the servers will still be displayed in the tree but you will not be connected to them.

## VTL console user interface

The VTL console displays the configuration for your VTL appliance. The information is organized in a familiar Explorer-like tree view.

The screenshot shows the VTL console user interface. On the left is a tree view under 'VTL Servers' with the following items:

- Virtual Tape Library System
  - Virtual Tape Libraries
  - Virtual Tape Drives
  - Virtual Vault [17 tapes]
  - Import/Export Queue [0 Jobs]
- Physical Tape Libraries
  - Physical Tape Drives
  - Replica Resources [0 replicas]
  - Physical Tape Database
  - Deduplication Policies
- Database
- SAN Clients
- Reports
- Physical Resources

The right-hand pane shows the configuration for the selected server 'vtlsvr201'. It has tabs for 'General', 'Location', 'Event Log', 'Version Info', and 'Performance Statistics'. The 'General' tab is active, displaying a table of configuration items:

Name	Value
Server Name	vtlsvr201
Login Machine Name	10.6.2.201
Login User Name	root
O.S. Version	Falconstor Hardened Enterprise Linux 5 Update 1
Kernel Version	Linux 2.6.18-53.1.19.el5 #1 SMP Tue Apr 22 03:01:10 EDT 2008 x86_64
Processor 1 - 2	Intel(R) Xeon(TM) CPU 2.80GHz 2793 MHz
Memory	3956 MB
Swap	4094 MB
Network Interface	eth1 - mtu 1500 inet 10.6.2.201 mac 0:7:e9:32:fa:c1
Protocol(s)	Fibre Channel
Admin Mode	Read/Write
Server Status	Online
System Up Time	19 days 1 hour 20 minutes 27 seconds
VTL Up Time	21 hours 43 seconds
Fibre Channel WWPN	21-00-00-e0-8b-9b-69-f6 [target]
Fibre Channel WWPN	21-01-00-e0-8b-bb-69-f6 [initiator]

Below the table is a section titled 'Storage Capacity Usage' with a table and a pie chart:

Total Size:	13,946.48 GB		
Available Size:	3,988.09 GB	Free	28.60%
Used Size:	9,958.38 GB	Used (MB)	71.40%
Unconfigured Size:	0.00 GB	Unconfigured	0.00%

The pie chart shows 28.60% Free (green), 71.40% Used (MB) (red), and 0.00% Unconfigured (yellow).

Below this is a section titled 'System Drive Usage' with a progress bar.

The status bar at the bottom shows: 07/29/2008 12:44:02 [PRAKASH-51-TEST-MACHINE] Logged out Server: vtlsvr201 8:43 AM

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 a collapsed item, click the  symbol next to the item. To collapse an item, click the  symbol next to the item. Double-clicking 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 features a drop-down box that allows you to see activity from this console session. The bottom right also displays the local server name and time.

---

## Understanding the objects in the tree

### Server object



From the server object, you can manage administrator accounts for that server, add/remove licenses, configure server-level options such as email alerts, perform system maintenance, generate an x-ray file, and set server properties.

For each server, you will see the following objects: *Virtual Tape Library System*, *SAN Clients*, *Reports*, and *Physical Resources*.

When you are connected to a server, you will see the following tabs:

- General - Displays the configuration and status of the VTL Server. Configuration information includes the version of the base operating system, the type and number of processors, amount of physical and swappable memory, supported protocols, network adapter information, storage capacity usage, and system drive usage.
- Event Log - Displays system events and errors.
- Version Info - Displays the version of the VTL Server and console software.
- Performance Statistics - Displays read and write throughput for the last 60 minutes.
- Folders
- Deduplication Statistics

---

## Virtual Tape Library System object



The *Virtual Tape Library System* object contains all of the information about your VTL appliance.

### 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 tape properties for the library (enable/modify tape capacity on demand, change maximum tape capacity)
- View performance statistics

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)
- View performance statistics

### 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 and view performance statistics.

### 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 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.

---

## Replica Resources



This object lists the Replica Resources that are on this VTL server. Replica Resources store data from local and remotely replicated virtual tapes. Clients do not have access to Replica Resources.

## Deduplication Policies



This object lists the deduplication policies that have been set for virtual tapes. You can create or modify deduplication policies from this object, perform deduplication, and view deduplication and replication statistics and status.

## Database



This object contains configuration information for the VTL. The database can be mirrored for high availability. Refer to '[Mirror the VTL database to protect your VTL configuration](#)' for more detailed information.

## Virtual tape 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 yellow O icon indicates that data has been written to the virtual tape and not yet cached to physical tape.

## Disk Resources object

For VTL Prime servers, disk resources are the virtualized disks that have been configured as the Prime data disks, Prime index disks, and Prime folder disks on the VTL server.

---

## SAN Clients object



For VTL servers, SAN clients are the backup servers that use the VTL. VTL supports Fibre Channel and iSCSI backup servers. For each SAN client, you can add a protocol and assign/unassign tape libraries/drives. For Fibre Channel clients, you can also view performance statistics. 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
- LUN allocation
- Fibre Channel adapters configuration
- Replication status
- Virtual tape/library information
- Job status
- Deduplication status
- Deduplication tape usage

## 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

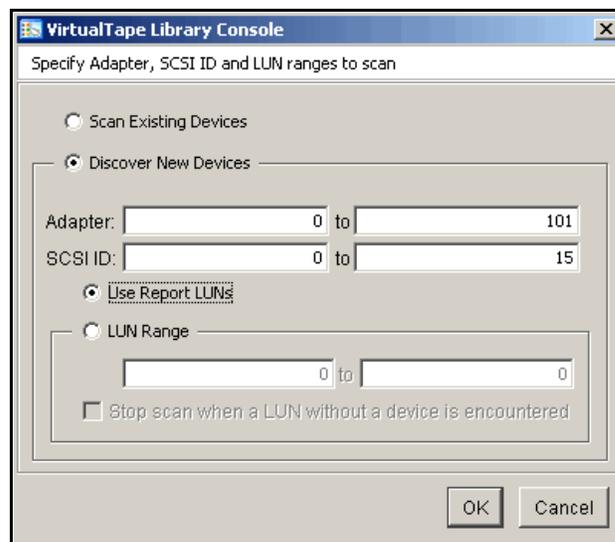
The following table describes the icons that are used to describe physical resources in the console:

Icon	Description
	The T icon indicates that this is a target port.
	The I icon indicates that this is an initiator port.
	The D icon indicates that this is a dual 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.

## Rescan physical devices

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

If you only want to scan on a specific adapter, right-click that adapter and select *Rescan*.



The adaptor must be an initiator.

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

**Note:** Discovering new devices in Solaris may take a long time. This can lead to the console becoming unresponsive. If this happens, you will need to end the process using the *Windows Task Manager*

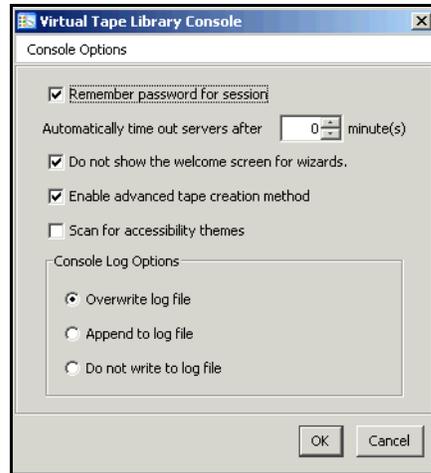
|

---

## Console options

To set options for the console:

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



2. Select the options you want to use.

*Remember password for session* - If the console is already connected to a server, when you attempt to open a subsequent server, the console will use the credentials from the last successful connection. If this option is unchecked, you will be prompted for a password for every server you try to open. You should not remember passwords when the console is being shared by different users.

*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.

---

## System maintenance

The VTL console gives you a convenient way to perform system maintenance for your VTL servers

Only the root user can access the system maintenance options.

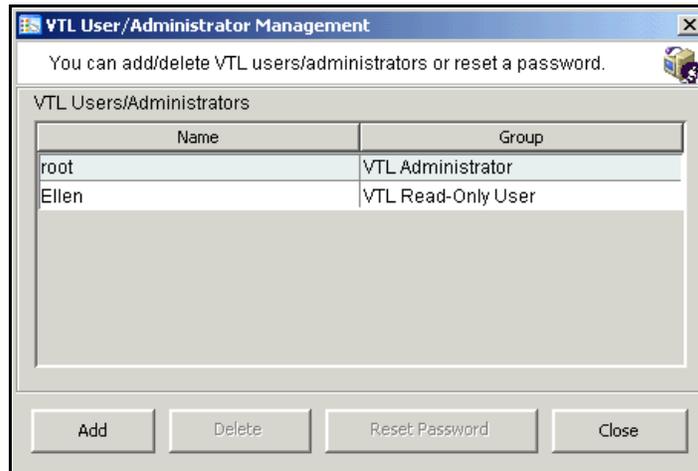
- |                       |   |
|-----------------------|---|
| Network configuration | If you need to change VTL Server IP addresses, you must make these changes using <i>Network Configuration</i> . Using any other third-party utilities will not update the information correctly. Refer to ' <a href="#">Set up network</a> ' for more information.  |
| Set hostname          | If you need to change the hostname of a VTL server, right-click a server and select <i>System Maintenance --&gt; Set Hostname</i> . The server will automatically reboot when the hostname is changed.  |
| Set date and time     | <p>You can set the date, time, and time zone for your system, as well add NTP (Network Time Protocol) servers. NTP allows you to keep the date and time of your VTL server in sync with up to five Internet NTP servers.</p> <p>You can also access these setting by double-clicking the time that appears at the bottom right of the console.</p> <p>We recommend restarting the VTL services if you change the date and time.</p> |
| Restart server        | Right-click a server and select <i>System Maintenance --&gt; Restart VTL</i> to restart the server processes.   |
| Restart network       | Right-click a server and select <i>System Maintenance --&gt; Restart Network</i> to restart your local network configuration.   |
| Reboot                | Right-click a server and select <i>System Maintenance --&gt; Reboot</i> to reboot your server.  |
| Halt                  | Right-click a server and select <i>System Maintenance --&gt; Halt</i> to turn off the server without restarting it.   |

---

## Administrators

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

1. Right-click the server (or group) and select *Administrators*.



There are three types of administrators:

- *VTL Administrators* are authorized for full console access (except that only the root user can add or delete a VTL administrator, change an administrator's password, or access the system maintenance options).
- *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.
- *VTL iSCSI Users* are used for iSCSI protocol login authentication (from iSCSI initiator machines). They do not have console access. You will be able to add this type of administrator if iSCSI is enabled

If you accessed *Administrators* from the group level, you can add an administrator, modify a password, or delete a user for all servers in the group.

2. Select the appropriate option. Note that administrator names must comply with Solaris naming conventions.

You cannot delete the root user or change the root user's password from this screen. Use the *Change Password* option instead.

---

## 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 or group 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 & Time	The date and time on which the event occurred. Events are listed in chronological order. If you have servers from different time zones in a group, the events will be sorted using coordinated universal time (UTC).
ID	This is the message number.
Event Message	This is a text description of the event describing what has occurred.

The Event Log is refreshed every three seconds, meaning that new events are added on a regular basis. If you are at the top of the Event Log when new events are added, the screen will automatically scroll down to accommodate the new events. If you are anywhere else in the Event Log, your current view will not change when new events are added. This allows you to read messages without the screen scrolling.

**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 a column heading to re-sort the information. For example, if you click the *ID* 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:

1. Click the *Filter* button.
2. Specify your search criteria.

You can search for specific message types, records that contain/do not contain specific text, category types, and/or time or date range for messages. You can also specify the number of lines to display.

**Export data from the Event Log** You can save the data from the Event Log in one of the following formats: comma delimited (.csv) or tab delimited (.txt) text. Click the *Export* button to export information.

---

Print the Event  
Log

Click the *Print* button to print the Event Log to a printer.

Clear the Event  
Log

You can purge the messages from the Event Log. You will have the option of saving the existing messages to a file before purging them. Click the *Purge* button to clear the Event Log.

## Reports

The VTL console provides you with the following pre-defined reports:

Report	Server Type	Scheduled
<b>Server Throughput Report</b> - Provides information about the overall throughput of the VTL server for a specific date or range of dates.	VTL Prime	Yes
<b>SCSI/Fibre Channel Throughput Report</b> - Displays information about data going through the selected SCSI or Fibre Channel adapter on the VTL server for a specific date or range of dates.	VTL Prime	Yes
<b>SCSI Device Throughput Report</b> - Displays information about the utilization of the selected physical SCSI storage device on the VTL server for a specific date or range of dates.	VTL Prime	Yes
<b>Physical Resources Configuration Report</b> - Lists the physical resources on the VTL server, including the physical adapters and physical devices.	VTL Prime	No
<b>Disk Space Usage Report</b> - Displays information about the amount of disk space that each SCSI adapter is currently using and how much is available.	VTL Prime	Yes
<b>Disk Space Usage History Report</b> - Displays information about the peak amount of total disk space available and being used on a specific date or range of dates. The interval shown is based on the range. For single days, disk usage is shown for each half hour. For a week, the interval is every four hours. For a 30 day period, the interval is once per day.	VTL Prime	Yes
<b>LUN Report</b> - Displays all of the virtual tapes that are allocated on one or all LUNs.	VTL Prime	Yes
<b>Physical Resources Allocation Report</b> - Shows the disk space usage and layout for each physical disk that can be allocated by the system (for virtual tapes, VTL database, etc.).	VTL Prime	Yes
<b>Physical Resource Allocation Report</b> - Shows the disk space usage and layout for a specific disk that can be allocated by the system (for virtual tapes, VTL database, etc.).	VTL Prime	Yes
<b>Fibre Channel Adapters Configuration Report</b> - Shows the World Wide Port Name (WWPN) and port information for each Fibre Channel adapter; this report is useful for matching up WWPNs with clients.	VTL Prime	No
<b>Replication Status Report</b> - Displays historical status for all virtual tapes enabled for replication. This report can be generated for the source or target server for any range of dates.	VTL Prime	Yes
<b>Virtual Library Information Report</b> - Displays information about each library being emulated, including drives, tapes and slots.	VTL Prime	No
<b>Virtual Tape Information Report</b> - Displays information about a virtual tape. You can select a specific barcode or a range of barcodes from one or more libraries. You can also specify what information you want to include in the report.	VTL Prime	Yes

Report	Server Type	Scheduled
<b>Job Report</b> - Displays information about jobs run on a specific date or range of dates. Information displayed includes job type, status, and start/end time.	VTL Prime	Yes
<b>Deduplication Status Report</b> - Summarizes all of the deduplication and replication jobs that were run on a specific date or range of dates. It includes the deduplication policy information as well as a detailed section listing the run times and associated information for each job.	VTL Prime	No
<b>Deduplication Tape Usage Report</b> - Provides statistics for all deduplication tapes and includes detailed information about each of the deduplication tapes.	VTL Prime	No
<b>Deduplication Detailed Status Report</b> - Provides detailed information for each tape in each deduplication job run on a specific date or range of dates, including start time, end time, data size, average dedupe ratio and performance, and time of replication.	VTL Prime	No
<b>Deduplication Tape Activity Report</b> - Provides detailed information about the tape activity during each deduplication job run during a specified date range. It displays the total and unique data, as well as data replication information, if applicable. It also includes a deduplication and replication summary for each job.	VTL Prime	No

Create a report    Each report can be created for a specific server or for multiple servers in a group.

1. To create a report, right-click the *Reports* object and select *New*.  
If you want to create a report at the group level, right-click the *Group Reports* object and select *New*.
2. If this is a group report, select if you want to run a *Regular Report* or a *Consolidated Report*.  
*Regular Report* - Standard reports that are generated on each server in the group. These reports contain data specific to a single server.  
*Consolidated Report* - Consolidated reports include every server in the group in one single report.
3. Select a report.  
Depending upon which report you select, additional windows appear to allow you to filter the information for the report.
4. If applicable, set the date or date range for the report and indicate which tape libraries/drives, adapters, devices, and/or SCSI devices to include 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 Virtual Resources* – Include all current and previous configurations for this server (including virtual tape libraries/drives that you may have changed or deleted).

---

*Include Current Active Virtual Resources and Clients Only* – Include only those virtual tape libraries/drives and clients that are currently configured for this server.

5. Enter a name for the report.
6. If you have configured email for reports, indicate if you want to email this report. You will have to enter the recipient(s) and a subject. You can also include text for the body of the email.
7. If this is a regular group report, select which servers should be included.
8. Confirm all information and click *Finish* to create the report.

**View a report** After a report is created, it is categorized by report type in the tree. Expand the *Reports* (or *Group Reports*) object and the report type to see the existing reports. When you select an existing report in the tree, the report is displayed in the right-hand pane.

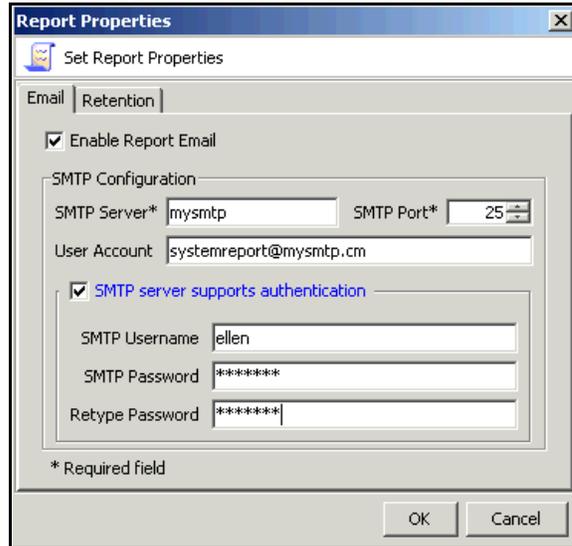
- Schedule a report** You can schedule certain reports to run at regular intervals. To do this:
1. Right-click the *Scheduled Jobs* object under *Reports* and select *New*.
  2. Select a report.  
Depending upon which report you select, additional windows appear to allow you to filter the information for the report.
  3. If applicable, set the date or date range for the report and indicate which tape libraries/drives and backup clients to include in the report.
  4. Set the schedule for how often this report should run.  
You can select to run the report on an hourly, daily, or weekly basis and you must indicate a starting time. If you select weekly, you must also select which day to run the report. If you select hourly, you must select how the frequency (in hours).
  5. Enter a name for the report.
  6. Confirm all information and click *Finish* to create the schedule.

**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 one of the following formats: comma delimited (.csv), tab delimited (.txt) text, Excel spreadsheet (.xls), PDF (.pdf), HTML (.html). To export information, right-click a report that is generated and select *Export*.

## Set report properties

You can set email and retention properties for reports. To do this:

1. Right-click the *Reports* object and select *Properties*.  
If this is a multi-node group, right-click *Group Reports* and select *Properties*.
2. If you will be emailing reports, enter information about your SMTP configuration.



The screenshot shows the 'Report Properties' dialog box with the 'Email' tab selected. The 'Retention' tab is also visible. The 'Enable Report Email' checkbox is checked. Under 'SMTP Configuration', the 'SMTP Server\*' field contains 'mysmtp', the 'SMTP Port\*' field contains '25', and the 'User Account' field contains 'systemreport@mysmtp.cm'. The 'SMTP server supports authentication' checkbox is also checked. Below this, the 'SMTP Username' field contains 'ellen', the 'SMTP Password' field contains '\*\*\*\*\*', and the 'Retype Password' field contains '\*\*\*\*\*'. A note at the bottom left states '\* Required field'. 'OK' and 'Cancel' buttons are at the bottom right.

*SMTP Server* - Specify the mail server that should be used.

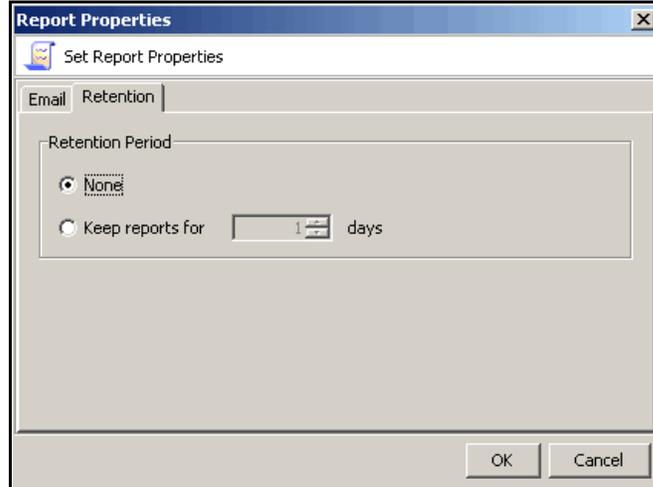
*SMTP Port* - Specify the mail server port that should be used.

*User Account* - Specify the email account that will be used in the "From" field of emails.

*SMTP server supports authentication* - Indicate if the SMTP server supports authentication.

*SMTP Username/Password* - Specify the user account that will be used to log into the mail server.

3. On the *Retention* tab, specify how long generated reports should be retained.



**Email a report** In order to be able to email a report, you must have set email properties for reports. If you have configured email, you can set a report to be emailed during the creation wizard. To email a previously created report:

1. Right-click a report that is generated and select *Email*.
2. Specify a recipient and a subject and then click *Send*.

**Refresh report display** You can refresh the list of reports that are displayed. This is useful if you have scheduled reports that have run while you are in the console. To do this, right-click *Reports (or Group Reports)* and select *Refresh*.

**Delete a report** You can delete one or more reports. To access the delete option, you can right-click a specific report, a report category, or the *Reports (or Group Reports)* object.

## Attention Required tab

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

- Hardware appliance errors
- Replication errors

Date & Time	Category	Message
06/25/2007 14:45:22 EST	Import/Export	Job 20 - An error occurred while writing to the tape [08880002]
06/25/2007 14:45:22 EST	Import/Export	Import job failed, jobID = 20, replID = 3, job status 5
06/25/2007 14:39:20 EST	Import/Export	Job 18 - An error occurred while writing to the tape [08880002]
06/25/2007 14:23:51 EST	Import/Export	Job 14 - Export Operation succeeded. The tape [08880002]
06/25/2007 14:22:13 EST	Import/Export	Job 13 - Export Operation succeeded. The tape [08880002]
06/25/2007 14:16:53 EST	Import/Export	Job 12 - Export on tape [08880002] in physical library [L7]

The *Attention Required* tab only appears for a VTL server (or at the group level) 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.

If you check the *Attention Required* tab at the group level, it will display events from all servers in the group, listed in chronological order. The server name will be included for each event to identify the source of the event.

If you have servers from different time zones in a group, the events will be sorted using coordinated universal time (UTC).

To view only a specific category of events, select the category from the *Filter* drop-down box.

Clear issues from the list

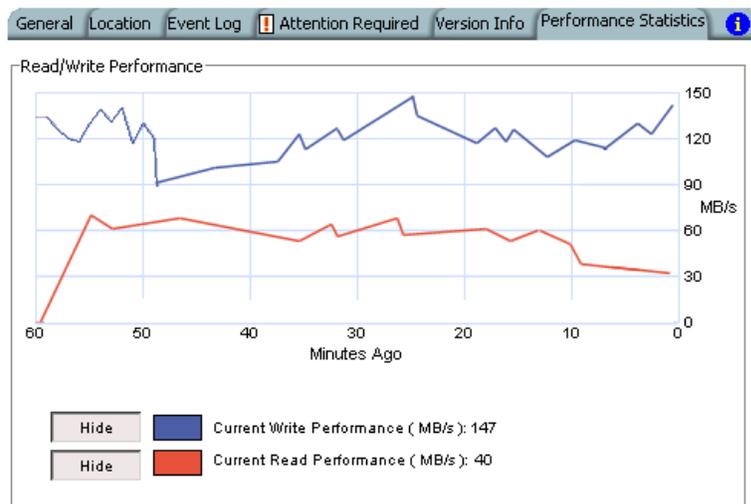
After you have resolved an issue, you can click the check box next to it and click the *Clear* button. You can clear individual issues or you can clear all listed issues by clicking *Select All* and then *Clear*.

## Performance statistics

Performance statistics are available for each virtual tape library, tape drive, tape, adapter, LUN, and Fibre Channel SAN client. They are also available at the *Virtual Tape Libraries* and *Server* levels.

At the *Virtual Tape Libraries* level, the *Performance Statistics* tab shows the aggregate throughput of all I/O activity on *all* virtual libraries. At the *Server* level, the tab shows an aggregate of *all* I/O activity.

Each *Performance Statistics* tab displays a chart showing read and write throughput for the last 60 minutes. Current performance is also displayed. All information is displayed in MB per second.



To hide a read or write performance chart, click the appropriate *Hide* button.

---

## Server properties

To set properties for a specific server or group:

1. Right-click the server/group 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, set VTL to send traps to your SNMP manager. Refer to '[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.

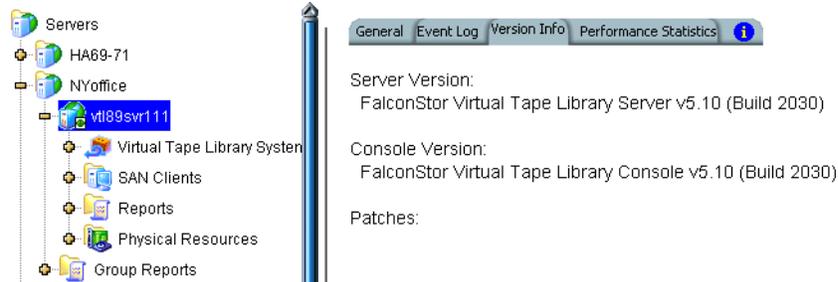
5. On the *Location* tab, enter information about the location of this server and who is responsible for maintaining it.

You can also include a .JPG/.JPEG format photograph of the appliance or its location.

---

## Software patch updates

The *Version Info* tab displays the current version of the VTL server and console.



With this information, 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 a 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 a 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*.

---

## 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 configure SNMP:

1. In the console, right-click your VTL server (or group) and select *Properties*.
2. Select the *SNMP Maintenance* tab.
3. Indicate the system information that should be available in your MIB browser.

*SysLocation* - Enter a location.

*SysContact* - Enter contact information. 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.

Refer to [SNMP Messages](#) for a complete listing of SNMP messages.

5. Click *Add* to enter the name of your SNMP server and a valid SNMP community name.
6. Compile the VTL MIBs into your SNMP manager.

The procedure to do this will vary by SNMP manager.

You will need to compile the following VTL MIB files: *falconstor.mib* and *falc-vtl.mib*

These files can be found at the following location: `$ISHOME/etc/snmp/mibs`

7. 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.

## Mirror the VTL database to protect your VTL configuration

In a typical VTL configuration, the VTL server uses one or more external storage devices to hold all of the data used by the virtual tapes as well as the VTL configuration. Even if you lose your VTL server, the data on your tapes will be maintained. **Mirroring the database is the only way to protect your configuration** if the disk storing the database is lost and is highly recommended.

When you mirror the VTL database, each time data is written to the 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.

In order to mirror the database, you must have at least two physical devices (preferably on different controllers) because the mirror cannot be on the same disk as the VTL database.

To set mirroring:

1. Right-click the *Database* object (under the *Virtual Tape Library System* object) and select *Mirror --> Add*.
2. Select which 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.

Name	Value
Vendor ID	FALCON
Product ID	IPSTOR DISK
Total Size (MB)	6,000
Status	Online
Virtual ID	3
GUID	3b2a95d2-c9e9-0710-0963-0000475afa34
Serial Number	PSTPXCHKI230
Mirror Type	Synchronous
Mirror Synchronization Status	Synchronized 31%
Instantaneous Throughput (MB/s)	60
Average Throughput (MB/s)	60
Estimated Time Remaining	1 minute 7 seconds

- *Synchronized* - Both disks are synchronized. This is the normal state.
- *Not synchronized* - 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 to the mirrored copy.

- If the synchronization is occurring, you will see a progress bar along with the percentage that is completed.

Replace a failed disk

If one of the mirrored disks has failed and needs to be replaced:

1. Right-click the database and select *Mirror --> Remove* to remove the mirroring configuration.
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.

3. Right-click the database and select *Mirror --> Add* to create a new mirroring configuration.

Fix a minor disk failure

If one of the mirrored disks has a minor failure, such as a power loss:

1. Fix the problem (turn the power back on, plug the drive in, etc.).
2. Right-click the database and select *Mirror --> Synchronize*.

This re-synchronizes the disks and re-starts the mirroring.

Replace a disk that is part of an active mirror configuration

If you need to replace a disk that is part of an active mirror configuration:

1. If you need to replace the primary database's disk, right-click the database and select *Mirror --> Swap* to reverse the roles of the disks and make it a mirrored copy.
2. Select *Mirror --> Remove* to cancel mirroring.
3. Replace the disk.
4. Right-click the database and select *Mirror --> Add* to create a new mirroring configuration.

Swap the primary disk with the mirrored copy

Right-click the database and select *Mirror --> Swap* 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.

Remove a mirror configuration

Right-click the database and select *Mirror --> Remove* to delete the mirrored copy and cancel mirroring. You will not be able to access the mirrored copy afterwards.

# Manage Tape Drives and Tapes

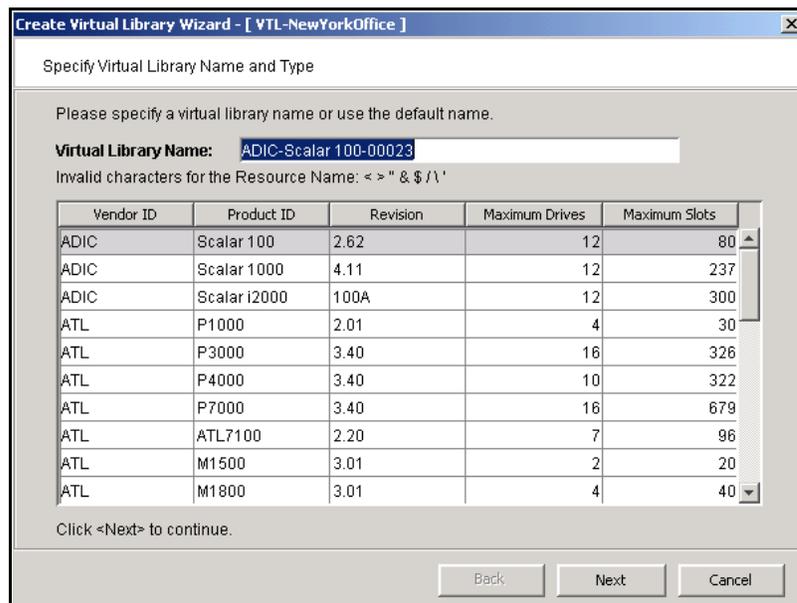
## Create virtual tape libraries

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

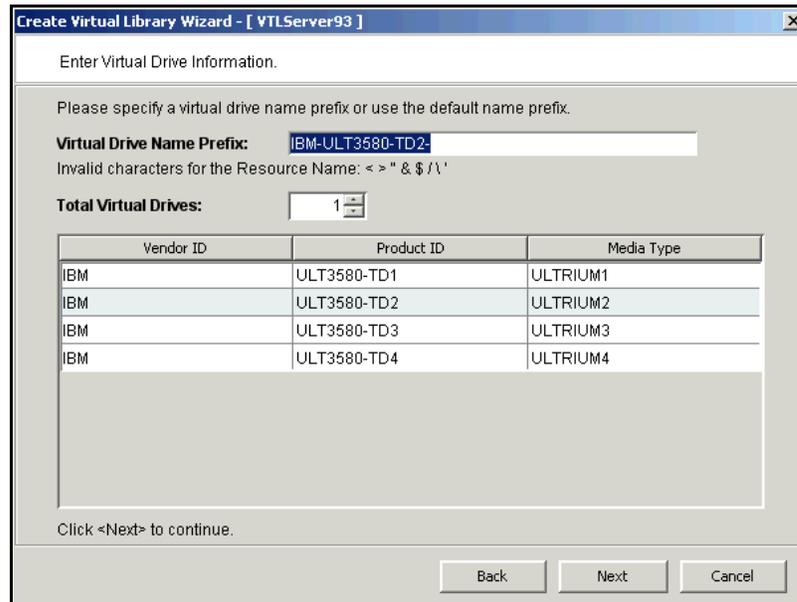
- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click the *Virtual Tape Libraries* object and select *New*.

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 *Physical Resources* and select *Prepare Devices*. Set hard drives to *Reserved for Virtual Device*. You may need to [Rescan physical devices](#) if all devices are not shown.

1. Select the tape library that you are emulating.



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



Vendor ID	Product ID	Media Type
IBM	ULT3580-TD1	ULTRIUM1
IBM	ULT3580-TD2	ULTRIUM2
IBM	ULT3580-TD3	ULTRIUM3
IBM	ULT3580-TD4	ULTRIUM4

*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. Determine if you want to use auto replication for this virtual library.

*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.

Do not enable auto-replication for libraries or tapes for which you will be defining a deduplication policy. This feature is not supported for ECO VITs. (For more information refer to ['Data Deduplication'](#).)

4. Enter barcode information for the virtual library.

The screenshot shows a dialog box titled "Create Virtual Library Wizard - [ VTLServer93 ]". The main heading is "Enter Virtual Library Information." Below this, it says "Please enter information for the virtual library." The fields are as follows:

- Name:** IBM-ULT3583-TL-00046
- Barcode Starts:** 002E00
- Barcode Ends:** 002EZZ
- Number of Slots:** 24
- Import|Export Slots:** 12

At the bottom, there is a prompt: "Click <Next> to continue." and three buttons: "Back", "Next", and "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**

5. Enter the guidelines for expanding virtual tape capacity.

The screenshot shows a dialog box titled "Create Virtual Library Wizard - [ VTLServer93 ]". The main heading is "Enter virtual tape properties." Below this, it says "Please enter virtual tape properties." The fields are as follows:

- Tape Capacity On Demand**
- Initial Tape Size:** 5 GB
- Incremental Size:** 5 GB
- Maximum Capacity:** 170 GB
- Media Type:** ULTRIUM2

At the bottom, there is a prompt: "Click <Next> to continue." and three buttons: "Back", "Next", and "Cancel".

---

You will only see this dialog if you have enabled the *Advanced Tape Creation* method (set in *Tools --> Console Options*). If *Advanced Tape Creation* is not enabled, *Tape Capacity On Demand* will automatically be set for you.

*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.

If *Tape Capacity on Demand* is used, when a tape is overwritten, all disk segments beyond the segment being written to are freed up. Space allocated for a replica resource will be adjusted to match the primary tape allocation before the replication starts, optimizing the disk space used by replica resources.

*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.

6. 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 the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click a virtual tape library or on the *Tapes* object and select *New Tape(s)*.

The *Create Virtual Tape wizard* will vary depending on whether or not you have enabled the *Advanced Tape Creation* method (set in *Tools --> Console Options*).

1. (*Advanced Tape Creation* only) 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 available device(s). If you select *Express*, you can create multiple virtual tapes at the same time.

2. (*Advanced Tape Creation* only) Specify which physical device should be used to create the virtual tapes.

Storage space is allocated from the local server even if this server is part of a multi-node group.

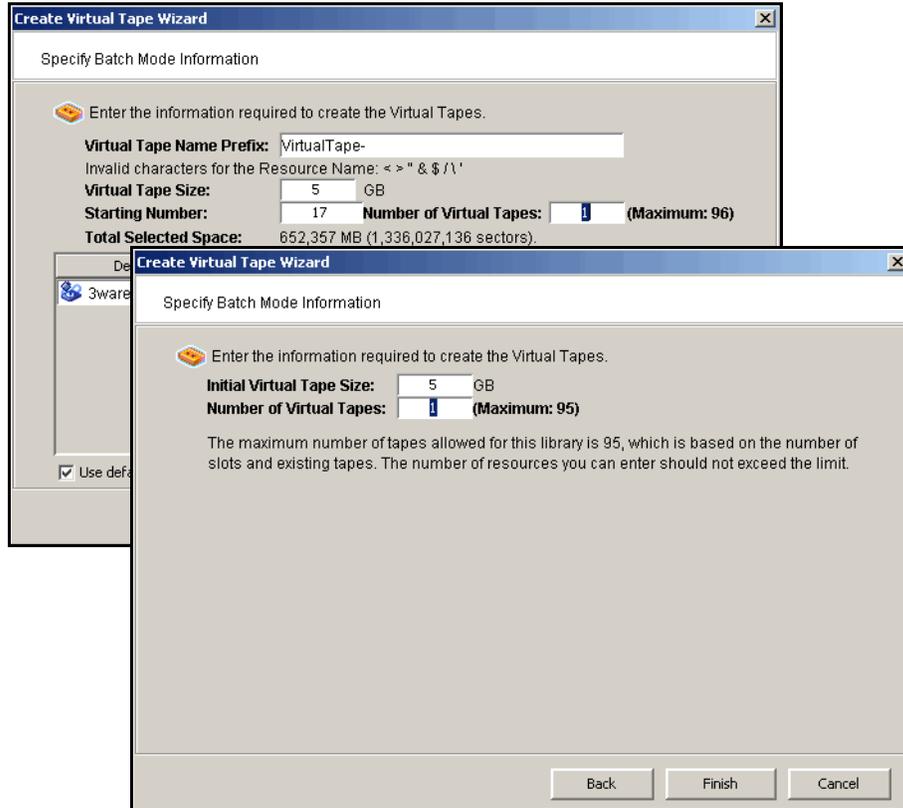
3. If *Auto Replication* is enabled for the virtual library and you want it enabled for this/these tapes, select the target server.

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.

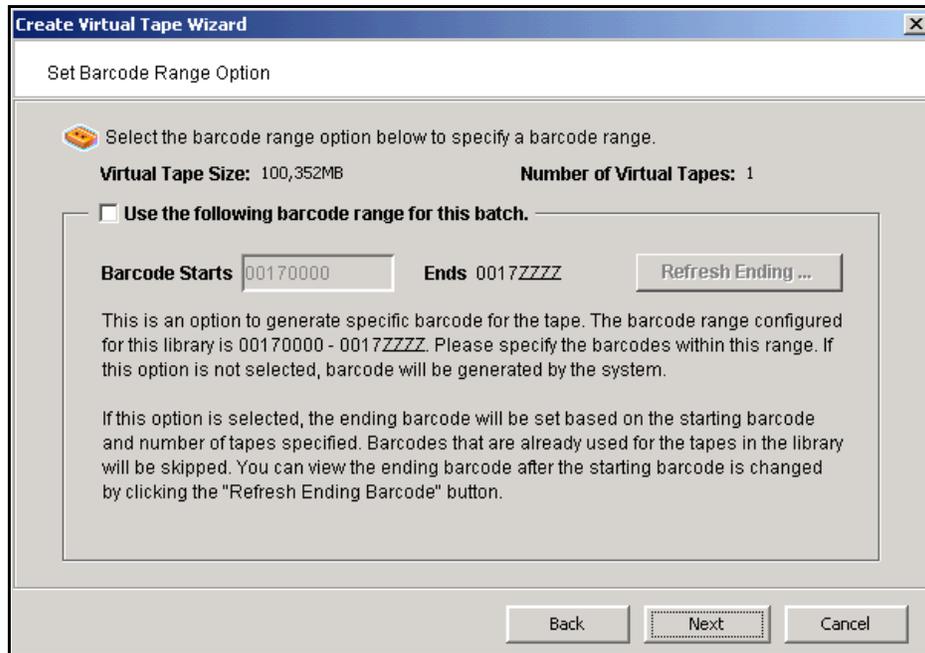
- Depending upon which method you selected, specify the size of the tape(s), name, and number of tapes to create.

You will be able to specify the tape name if the *Advanced Tape Creation* method is enabled.



You will see this dialog if the *Advanced Tape Creation* method is not enabled.

- (*Advanced Tape Creation* only) If desired, set a barcode range for the virtual tapes you are creating.



- 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.

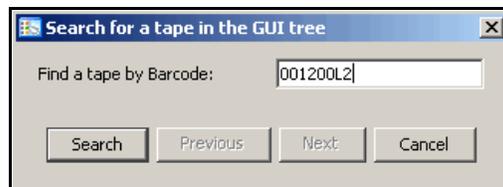
## Locate and display virtual tapes in the console

Because it is possible to have a large number of virtual tapes, we have included tools to help you locate just the tape(s) you are looking for.

### Search by barcode

To search by barcode for a specific virtual tape:

1. Highlight any object on the server where the tape resides.
2. Select *Edit* menu --> *Find*.



3. Enter the full barcode.

Note that the search is case sensitive. Once you click *Search*, you will be taken directly to that tape in the right pane.

### Display virtual tapes

When you highlight the *Tapes* object in the tree, a list of all tapes in that virtual library is displayed in the right-hand pane.

When you highlight the *Virtual Vault* object, a list of all tapes in the vault is displayed in the right-hand pane.

While the right pane is usually just for informational purposes, you can perform tape functions directly from the right pane by highlighting one or more tapes and using the right-click context menu. You can also highlight any tape to see detailed tape information.

## Sort all tapes

You can sort the tapes displayed in the right-hand pane by barcode or name. To do this:

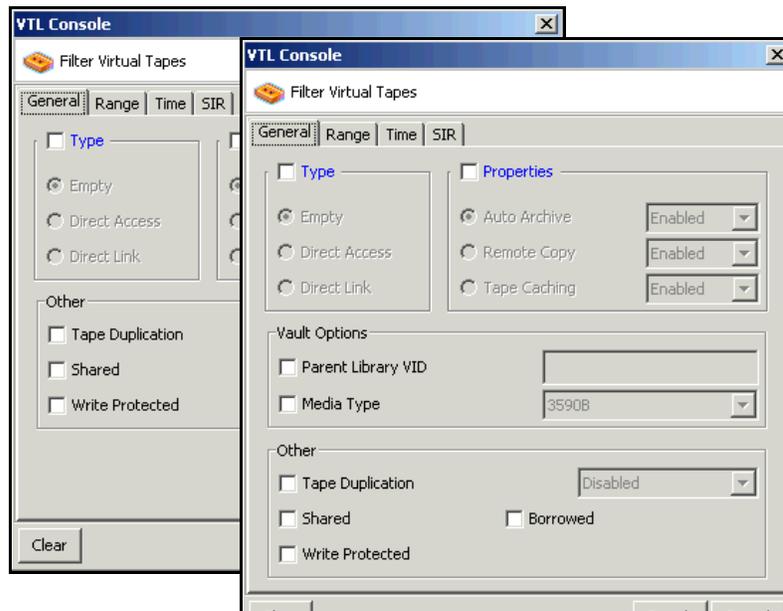
1. Select *Barcode* or *Name*.
2. Indicate whether they should be sorted in *Ascending* or *Descending* order.

## Filter the display of tapes

Because it is possible to have a large number of tapes in the right-hand pane, you may want to filter the tapes and display only specific tapes. To do this:

1. Click the *Filter* button.
2. On the *General* tab, you can indicate the type of tape(s) you are looking for.

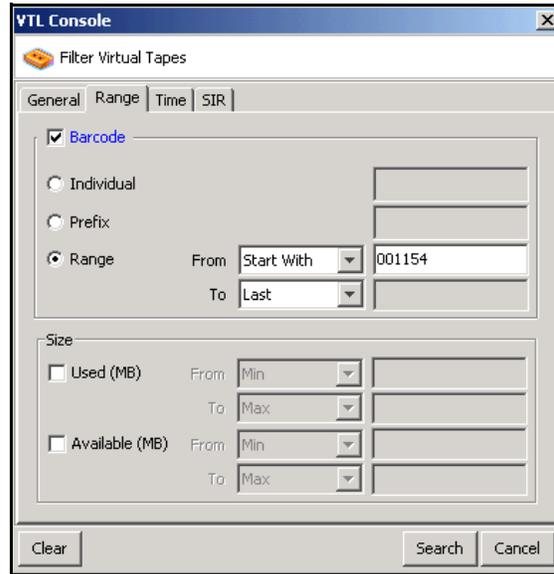
You will see this dialog if you started from the *Tapes* object.



You will see this dialog if you started from the *Virtual Vault* object.

The dialog will offer different options depending upon whether you are in the virtual vault or not.

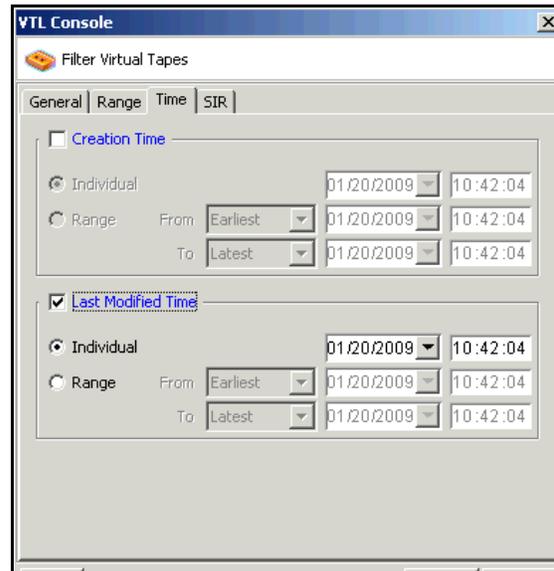
3. On the *Range* tab, you can enter a range of barcodes and/or sizes.



If you want to specify a particular number, select *Start With* or *End With* in the *From/To* fields. You can then type the number in the box to the right.

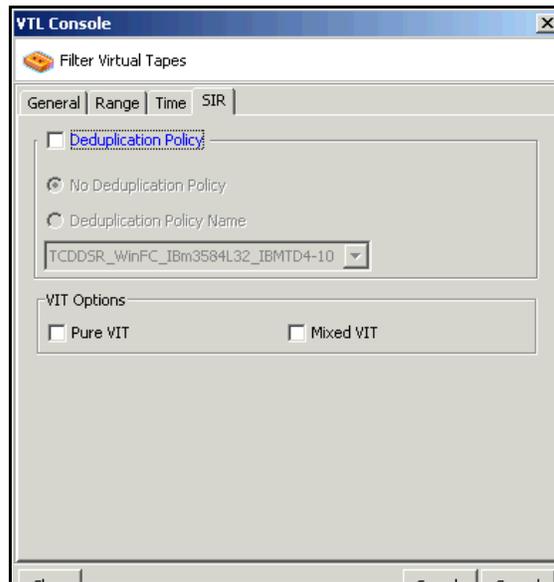
You can use multiple filters to further narrow your search. For example, you may want to locate empty tapes (select on the *General* tab) within a specific barcode range.

4. On the *Time* tab, you can enter a specific time or a range of times based on when a tape was created or modified.



If you want to specify a particular date/time, select *Start At* or *End At* in the *From/To* fields. You can then change the number in the box to the right.

5. On the *ECO* tab, you can look for tapes associated with a deduplication policy.



6. Click *Search*.

Afterwards, *just* the tapes that match the selected criteria will be displayed in the right pane. You can click the *Show All Tapes* button when you are done.

---

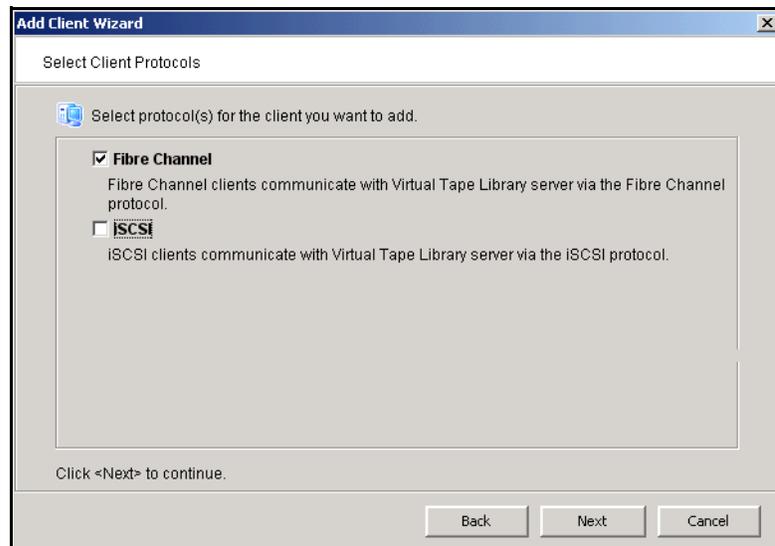
## Add SAN Clients (backup servers)

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 the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click the *SAN Clients* object and select *Add*.

After launching the wizard, follow these steps to continue:

1. Enter the client name.
2. Select the protocol(s) being used by the client.



**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.

**For iSCSI clients**, 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.

3. Click *Finish* when you are done.

## Assign virtual tape libraries to clients

You can assign a virtual tape library or drive to the target of a backup server listed in the VTL console under the *SAN Clients* object. The backup server can then access the assigned virtual tape library/drive(s).

There are three ways to assign a library to a client (backup server):

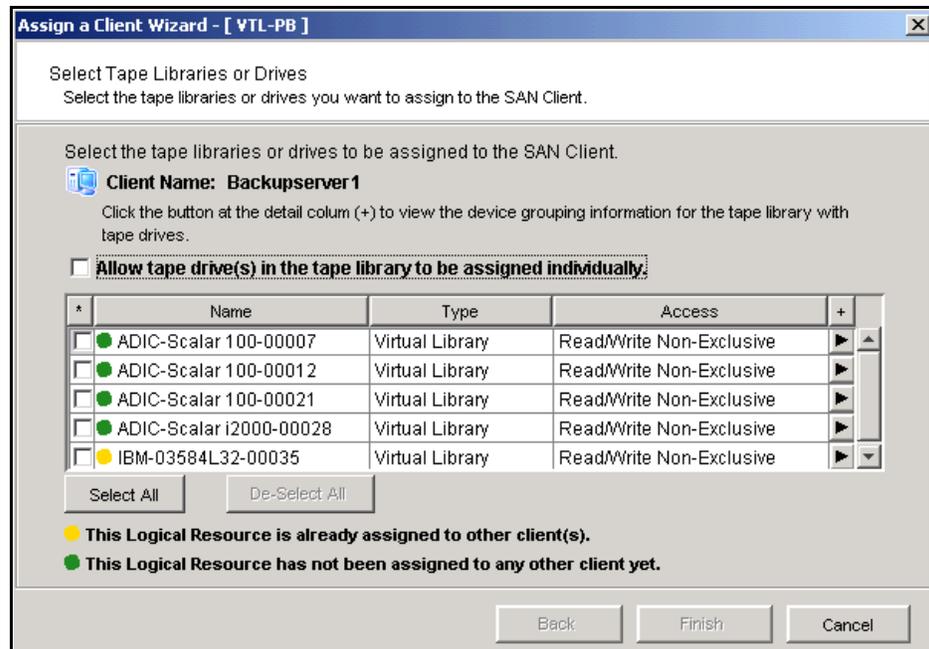
- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*. After adding a virtual tape library, you can assign it to a backup server.
- Right-click a virtual tape library, select *Assign*, and then select a backup server.
- Right-click a specific SAN Client or on the *Everyone\_FC* or *Everyone\_iSCSI* client, select *Assign*, and then select a virtual tape library. The *Everyone* clients are generic clients that you can assign to all (or some) of your virtual libraries/drives.

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. For security purposes, you should assign specific WWPNs to specific clients.

### Configuration wizard or client object:

If you started from the configuration wizard or a client object, follow these steps to continue:

1. Select a virtual tape library.



---

All tape drives in the library will be assigned to the selected client.

If you want to assign tape drives in the library individually, select the checkbox for that option. The VTL server and backup server will treat each individually assigned drive as if it were a standalone tape drive.

Do not select any "SIR-Tape-Drive" virtual drive that may appear in the list of available libraries and drives.

2. Click *Finish* when you are done.
3. Use the backup server's operating system to discover the VTL server.

The steps to do this vary according to the backup server's operating system.

For Fibre Channel environments, if your zoning has been correctly configured, and devices have been properly assigned to clients, a simple bus rescan performed on the client should show the new backup devices. Of course, this procedure varies depending on the OS.

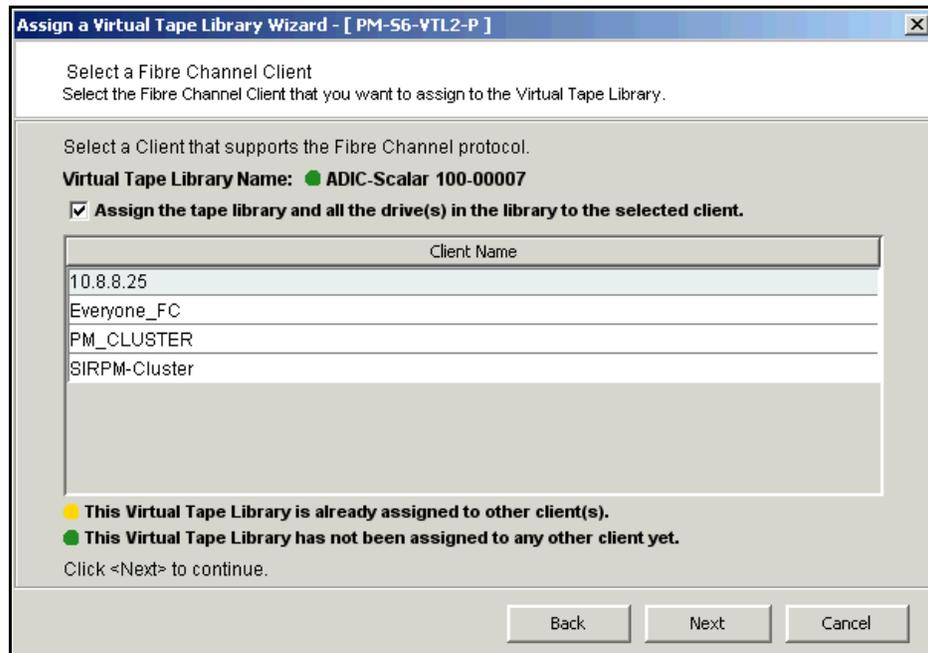
For Windows, *Control Panel --> Computer Management --> Device Manager -->* right-click the device in the right pane --> *Scan for hardware changes*.

4. Use your backup software to discover the library. The steps to do this vary according to your backup software.

### *Virtual tape library:*

If you started from a virtual tape library, follow these steps to continue:

1. Select the appropriate protocol for the backup server to which you want to assign the library.
2. Select a backup server.



3. Click *Next* and then click *Finish* when you are done.

# *Data Deduplication*

---

The data deduplication solution integrates seamlessly with VTL to eliminate redundant data without impacting your established backup window. Deduplication offers as much as a 30:1 reduction of backup data, minimizing replication time and storage requirements.

The deduplication process scans virtual tape cartridges, analyzes the data, and determines whether data is unique or has already been copied to the deduplication repository. The process then passes only single instances of unique data to the deduplication repository. The original virtual tape is replaced with a virtual index tape (VIT) pointing to deduplication storage, freeing considerable space for more data.

Deduplication occurs as a separate, off-line process. Backup and restore jobs have higher priority than deduplication. Deduplication jobs are temporarily suspended when the tape being deduplicated is needed for backup or restore; when the backup application finishes using that particular tape, the deduplication job automatically resumes from where it left off.

Deduplication is controlled by policies managed in VTL. You can set policies for all tapes in a library, groups or ranges of tapes, or just an individual tape. Deduplication is performed in the background without user intervention. During normal use, the deduplication option is transparent to the backup operation. Data duplicated across remote sites is deduplicated at the central site, enabling only globally unique data to be replicated to the disaster recovery site.

When replication is configured as part of a deduplication policy, the deduplication repository and metadata are replicated.

## Enable deduplication

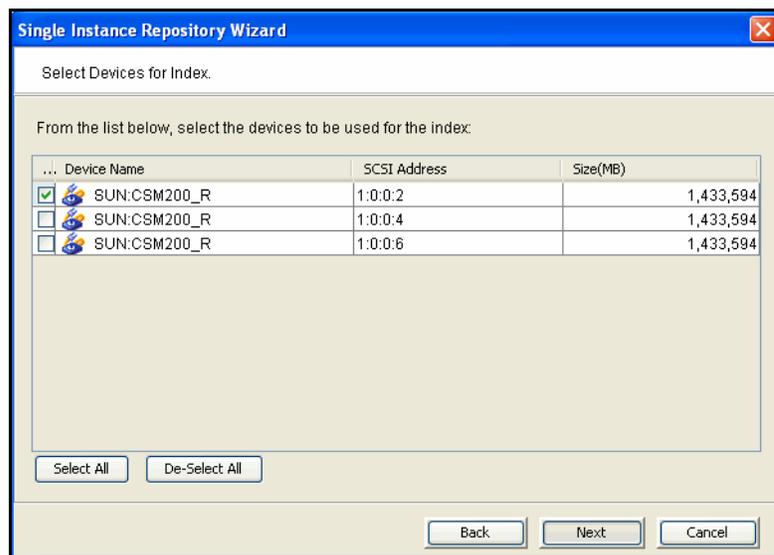
Deduplication must be enabled on the VTL server, as well as on any VTL server that will serve as a replica target for a replicated deduplication repository. To do this:

1. Right-click on the server and select *Options --> Enable Deduplication*.
2. To automate the process of preparing SIR storage, select *Physical Device*.



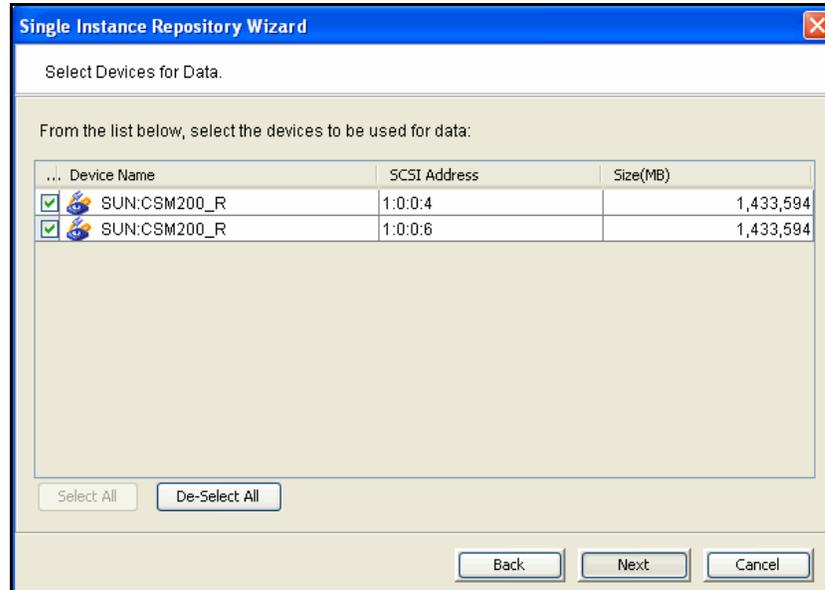
3. In the *Select Devices for Index* dialog, select the virtualized disk that will serve as the index resource, scratch resource, and configuration repository resource. The LUN must be of sufficient size to contain these resources.

The minimum size disk required for these resources is calculated in GB as *Number of CPUs on deduplication appliance x 20 + 10*.



4. In the *Select Devices for Data* dialog, select the device(s) that will be used for data storage.

Select 1, 2, 4, 8, 16, or any number of disks based on 2 to the Nth power.



5. In the confirmation dialog, select *Finish* to complete the wizard.

## Replicating the deduplication repository

When you create a deduplication policy, you have the option of configuring replication for the tapes in the policy. If you do this for all deduplication policies, you effectively replicate the entire deduplication repository.

Replication from the source server to the target server occurs via Fibre Channel or iSCSI. The target server is usually located at a remote location. If a disaster occurs and the replica is needed, the administrator can move the replicated tape from the virtual vault to its virtual tape library so that it can be accessed by backup software.

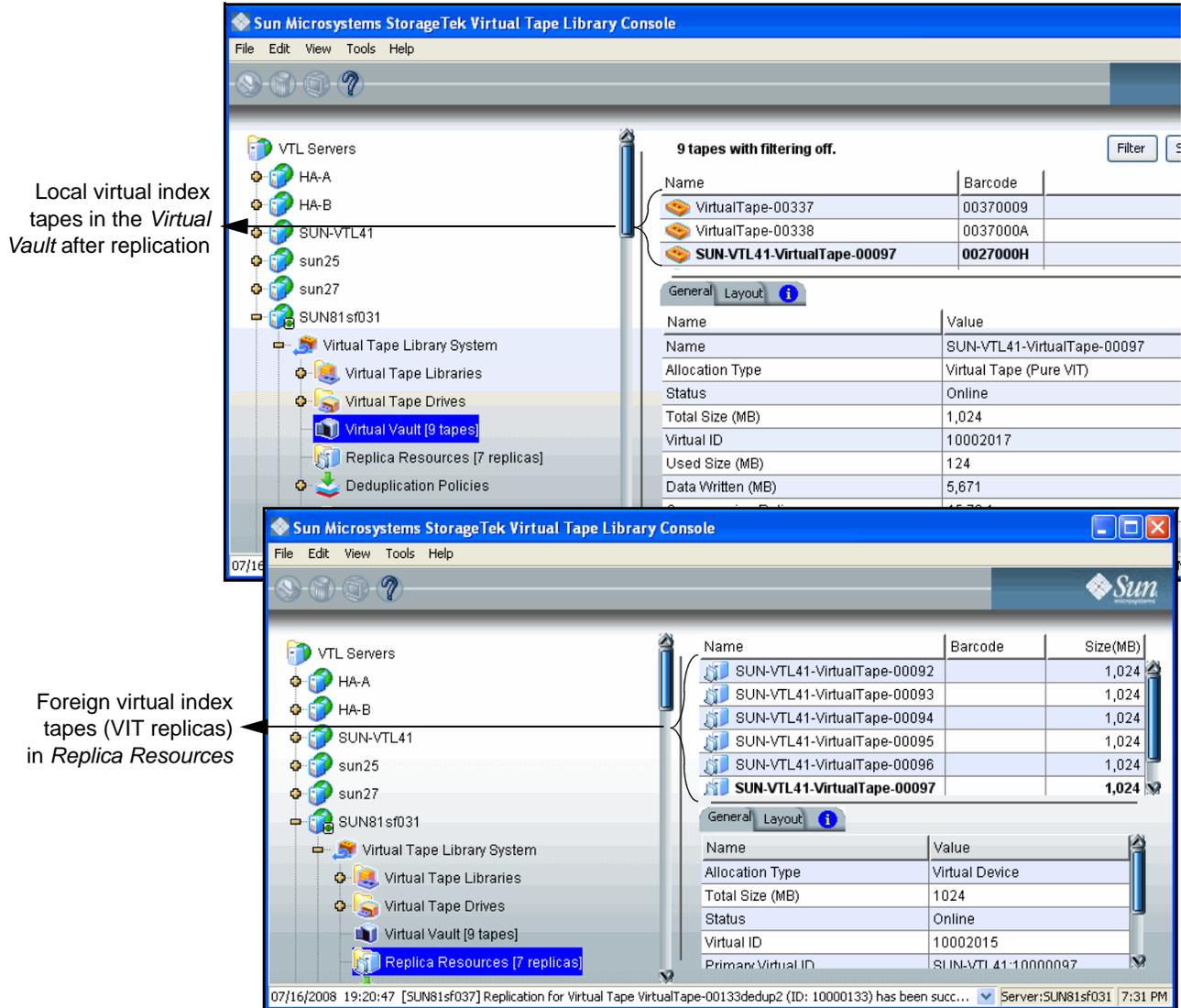
Replication of deduplicated data occurs in several stages:

- When replication occurs, the virtual index tape (VIT) from the source server is copied to the target server and becomes a foreign virtual index tape (FVIT) which you can see when you select the *Replica Resources* object.
- The FVIT is scanned to determine whether or not the data blocks it uses exist locally. Missing data blocks are replicated from the source server to the target server. After all missing data blocks are replicated, the target server has all the data blocks used by the FVIT.
- The target server automatically creates a local virtual index tape (LVIT) and puts it in the target server's virtual vault; the LVIT is now a replica of the source VIT and contains pointers to the replicated blocks of data.

Replication is complete when you see the LVIT in the target server's virtual vault. The name of the LVIT corresponds to the name of the FVIT. The

image below shows the VTL target server, with FVITs listed for the Replica Resources object and the LVITs for replicated data listed for the Virtual Vault object.

This final step may not occur immediately after the initial replication of data and can take some time to complete, depending on the availability of SIR tape drives on the target server and the amount of data on the FVIT.



## Requirements

- (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.
- You must enable replication between the two VTL servers by adding the target server to the primary server using the console on the primary server.

- You must enable deduplication on the target server using the console on the target server.
- The target server must be a 64-bit server.

## Connect appliances

In order to configure replication to another VTL server using a Fibre Channel (FC) switch, the servers must be zoned so a target port on the replica source server is zoned to an initiator port on the replica target server.

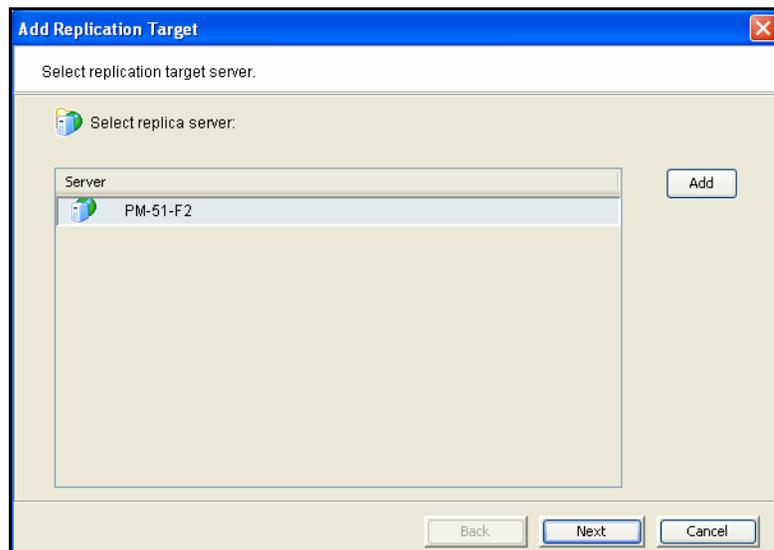
While most customers choose to use a Fibre Channel switch to connect their VTL and deduplication appliances, it is also possible to direct-connect the appliances. If you are using an iSCSI connection, the iSCSI option must be enabled on both servers. If you are direct-connecting the appliances, the source VTL server must have at least two target ports and you must connect the appliances as follows:

- Target port on the replica source server with the initiator port on the replica target server
- Initiator port on the replica source server with the target port on the replication target server
- Target port(s) on the replica source server with the initiator port(s) on the backup server

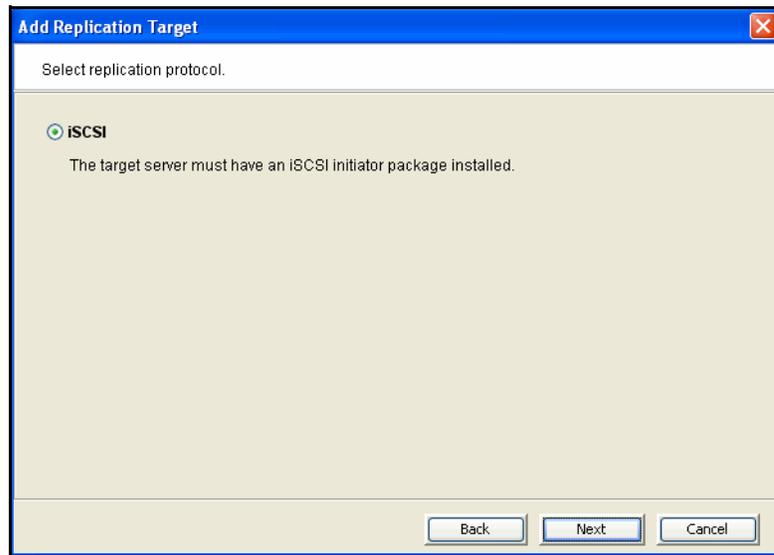
## Add the replication target server

Before you can configure replication for a tape, you must enable replication between the two VTL servers. To do this:

1. Right-click the server and select *Options --> Deduplication --> Replication --> Add Target*.
2. If the server you wish to use as a target is listed, select the server. (You must be logged into that server).



3. If the server is not listed, select *Add*.
4. Enter login information for the VTL server that will serve as the target.
5. Select *OK*. The server appears in the list. Select the server.
6. In the next screen, iSCSI is selected by default. Select the correct replication protocol.



7. In the next screen, confirm the information and click *Finish*. The target server is configured to be the replication target.

The *SIR Replication* tab appears in the right-hand pane for both servers when replication has been configured. Content identifies the replicator (the data source) and the replica (the VTL server to which data is replicated).

---

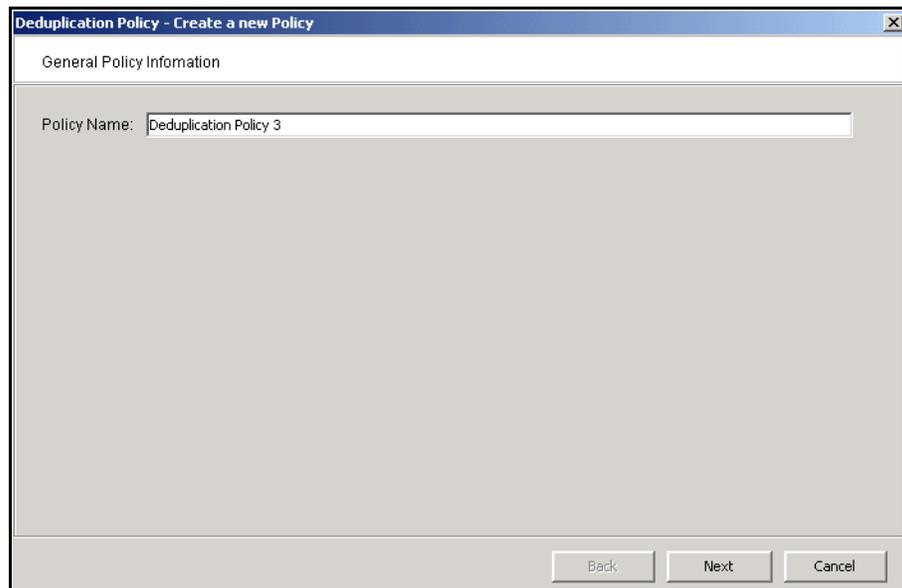
## Data deduplication policies

### *Add deduplication policies*

Deduplication policies specify which virtual tapes need to have deduplication and when deduplication should occur. You must have at least one virtual tape library and one virtual tape in order to create a policy.

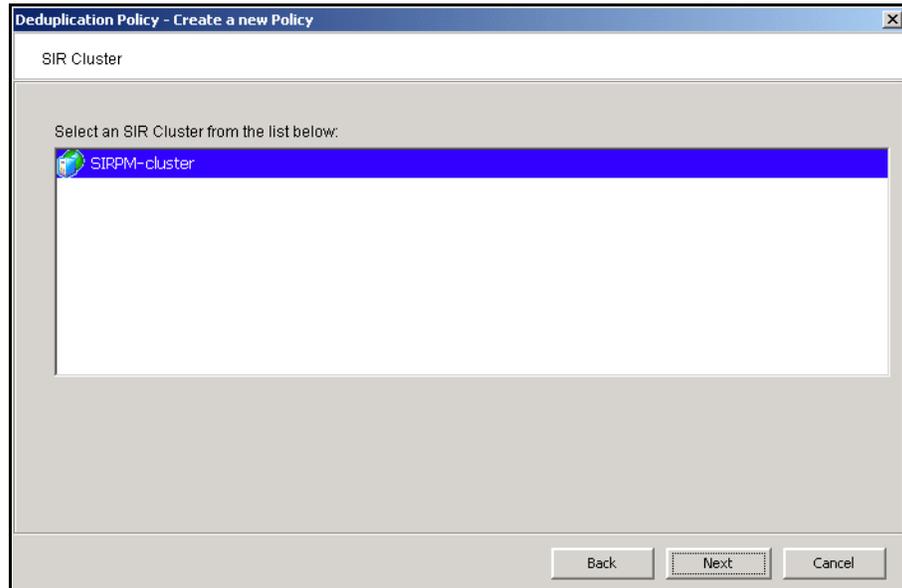
Once you set your deduplication policies, you should not change the IP address or hostname of your appliance(s). If you need to change the IP address or host name, do it **BEFORE** setting your policies.

1. On your VTL server, right-click on the *Deduplication Policies* object and select *New*.
2. For a new policy, enter a name for the policy.

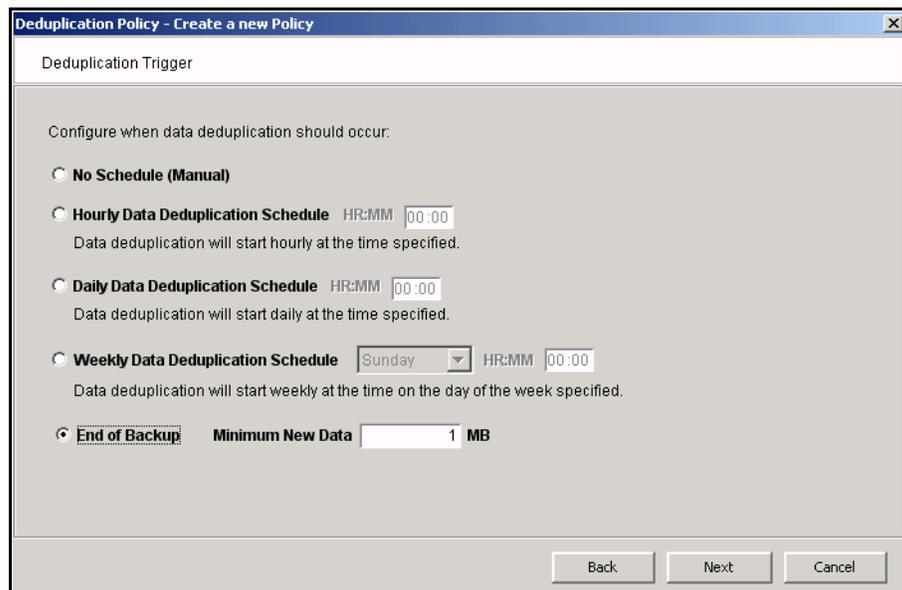


The screenshot shows a Windows-style dialog box titled "Deduplication Policy - Create a new Policy". The dialog is divided into a header section labeled "General Policy Information" and a main content area. In the main content area, there is a text input field labeled "Policy Name:" which contains the text "Deduplication Policy 3". At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

3. Select a deduplication cluster to associate with the policy.



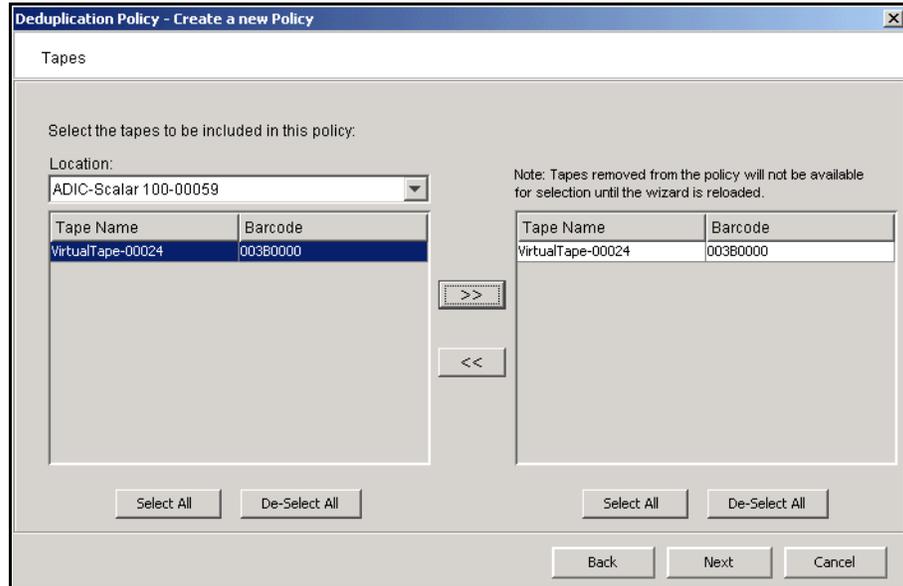
4. Indicate how often deduplication should occur.



If you are setting deduplication for a specific time, be sure to set the deduplication policy to a time after the backup job will be completed for the virtual tape associated with the policy.

If the job is not completed by the time the next deduplication job should begin, the policy will wait the selected time after the current deduplication job is complete. For example, if you choose to deduplicate every two minutes and the deduplication policy is running for more than two minutes, the policy will continue until completion and then wait two minutes before starting again.

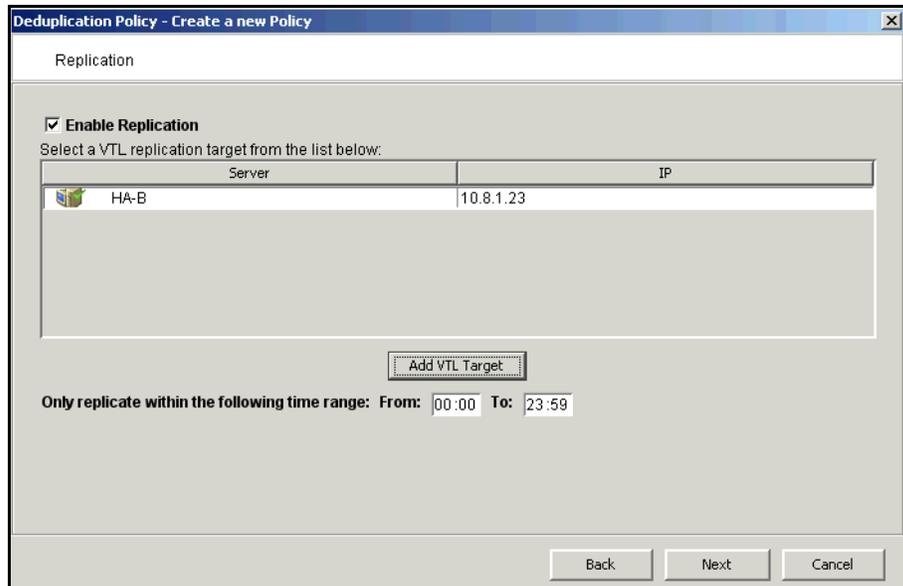
5. Select the virtual tape(s) that you want to include in this policy.



A virtual tape can be part of only one deduplication policy at a time.

Use the *Location* drop-down box to select a virtual tape library. Then, highlight one or more tapes and use the >> button to move the tape(s) to the right column.

6. Indicate whether you want to enable Replication for the tapes in this policy. If this is the first deduplication policy being created for this library, no replication targets will be listed. Add the target server. If a replication target has already been created for this VTL, be sure to add the same replication target (refer to '[Add the replication target server](#)'). Deduplication must already be enabled on the target server.



---

For information on replicating the deduplication repository, refer to [‘Replicating the deduplication repository’](#).

7. Click *Finish* to finalize the policy.

The policy is enabled and will execute at the next scheduled time.

To view statistics about running policies, refer to [‘Monitor deduplication and view statistics’](#).

## *Modify deduplication policies*

After a policy is created, you can do the following:

- To modify the properties of a policy, right-click on the policy and select *Edit*.
- To execute a policy right now, regardless of the time, right-click on the policy and select *Run*.
- If a policy is running and you want it to stop, right-click on the policy and select *Stop*.
- To completely remove a policy, right-click on the policy and select *Delete*.

## **Perform deduplication**

If your deduplication job has not started yet, you can use the console to force it to run now by right-clicking on a policy and selecting *Run*.

Before deduplication, the virtual tape’s backup data is stored on the disks of the VTL Server. When the deduplication policy runs, an intelligent “Tape Scanner“ process on the deduplication server analyzes the backup data to perform deduplication. Upon completion, the entire virtual tape will be free of any backup data, and instead, an “index” to the real data is stored. All truly unique data blocks found during the deduplication process are stored on the deduplication server disk space.

Therefore, you can describe the deduplication process as a “data block mover” that moves all blocks from VTL storage space to the deduplication storage space, except that redundant blocks are discarded. A virtual tape that has been deduplicated is called a “Virtual Index Tape” because it contains only the pointers to the data, instead of the actual data.

## Monitor deduplication and view statistics

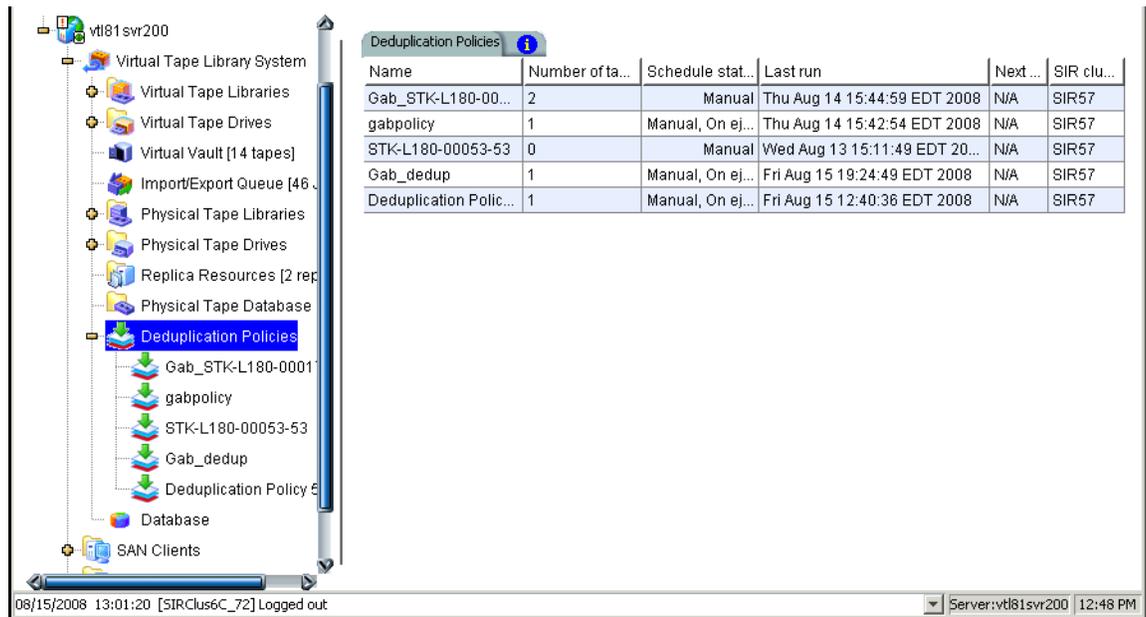
From the console, you can view the following:

- Status of running policies
- Scanner history
- Repository statistics for the cluster

### *Deduplication Policies object*

When you highlight the *Deduplication Policies* object, the right-hand pane lists all of the policies that are configured for deduplication on this server.

For each policy, you can see the number of tapes included, schedule information (such as status, history, and next run time), and the deduplication cluster to which this policy belongs.



The screenshot displays the VTL console interface. On the left, a tree view shows the hierarchy of objects, with 'Deduplication Policies' highlighted. The right pane shows a table titled 'Deduplication Policies' with the following data:

Name	Number of ta...	Schedule stat...	Last run	Next...	SIR clu...
Gab_STK-L180-00...	2	Manual	Thu Aug 14 15:44:59 EDT 2008	N/A	SIR57
gabpolicy	1	Manual, On ej...	Thu Aug 14 15:42:54 EDT 2008	N/A	SIR57
STK-L180-00053-53	0	Manual	Wed Aug 13 15:11:49 EDT 20...	N/A	SIR57
Gab_dedup	1	Manual, On ej...	Fri Aug 15 19:24:49 EDT 2008	N/A	SIR57
Deduplication Polic...	1	Manual, On ej...	Fri Aug 15 12:40:36 EDT 2008	N/A	SIR57

The status bar at the bottom indicates the date and time as 08/15/2008 13:01:20, the user as [SIRClus6C\_72] Logged out, and the server as vtl81svr200 at 12:48 PM.

## Individual deduplication policies

When you highlight a policy in the tree, you can view information about that policy.

### General Info tab

The *General Info* tab shows how many tapes are included in this policy, deduplication cluster and server information, schedule and replication information, and policy history, including when and why the policy was run, number of tapes scanned, total amount of data scanned, total amount of unique data written to the repository, and the deduplication ratio.

The screenshot shows the VTL Prime interface. On the left, a tree view shows the hierarchy: Virtual Tape Library System > Virtual Tape Libraries > Virtual Tape Drives > Virtual Vault [14 tapes] > Import/Export Queue [46] > Physical Tape Libraries > Physical Tape Drives > Replica Resources [2 rep] > Physical Tape Database > Deduplication Policies > Gab\_STK-L180-0001. The 'General Info' tab is active, showing the following table:

Name	Value
Policy name	Gab_STK-L180-00017
Number of tapes	2
SIR server name	SIR57
SIR server IP address	10.8.9.57
Schedule	Tape caching reclamation
Replication	Not Enabled

Below this is the 'Gab\_STK-L180-00017 run history' table:

Run date/ti...	Ru...	Total...	Data Deduplication Statistics				Data Replication Statistics				Stat...
			Tota...	Uniqu...	Dedu...	Du...	Tota...	Uniqu...	Dedu...	Du...	
2008/08/14 ...	ma...	1	5,000	0	> 100...	1:08	0	0	N/A	0:00	co...
2008/08/14 ...	ma...	1	5,000	0	> 100...	1:09	0	0	N/A	0:00	co...

The status bar at the bottom shows: 08/15/2008 13:02:32 [vtl81svr200] Virtual Tape Library 316 (ID: Test\_Lib) was added. Server: vtl81svr200 12:51 PM

### Tapes tab

The *Tapes* tab lists information about each virtual tape in the policy.

*Tape name* - The name of the virtual tape.

*Barcode* - The barcode assigned to the tape.

*Size* - Maximum uncompressed storage capacity of the tape. This is determined when the tape was created.

*Written* - The amount of data (before compression) that is written to tape by backup applications. This amount can be greater than the tape size if the data is compressed.

*New* - The amount of data (before compression) that has not yet been deduplicated, including newly appended data to a tape.

*In deduplication* - The amount of data (before compression) written that has now been moved to deduplication storage. This is basically the difference between the data written and the data not yet deduplicated.

*Unique data* - The actual physical storage in deduplication used to store tape data. This includes the effect of deduplication compression.

*Dedupe ratio* - The ratio between the data moved to deduplication and the unique data.

*Last run Dedupe* - The last time the tape was deduplicated.

*Last run Replicated* - The last time the tape was replicated.

*Next run* - The next time the tape will be deduplicated.

When you highlight a tape in the top section, the *Policy Tape Info* tab in the bottom section displays additional details about the tape:

Tape ...	Barco...	Maximum Capacity (MB)	Data details				Last run		Next r...	
			Write...	New (...)	In SIR ...	Uniqu...	Dedu...	Replic...		
V...	00050...	20480	5000	0	5000	0	> 100...	2008/...	N/A	N/A
V...	00050...	20480	5000	0	5000	0	> 100...	2008/...	N/A	N/A

Name	Value
Tape Name	VirtualTape-00011
Barcode	0005000J
Virtual ID	10000011
Tape Location	Library VID 4 [Vault]
Tape Size (MB)	20480

*Virtual ID* - The tape's virtual ID.

*Tape location and slot* - The tape's current location.

*Physical allocation* - The physical size of the tape.

*Last Dedupe Status* - The status of the last time this policy ran.

*Last Replication Status* - The status of the last time data for tapes in this policy was replicated.

## Active Policies tab

The *Active Policies* tab lists information about currently running policies and replication jobs. The data is automatically refreshed.

The screenshot shows the 'Active Policies' tab in a software interface. The left pane displays a tree view of the system components, with 'SIR Policy 1' selected. The main area contains two tables: 'Scanner status' and 'Replication status'.

**Scanner status**

Tape na...	Barc...	Tape d...	Dat...	Data si...	Scann...	Rate (MB/s)	Blocks ...	Status	Progress
Wolfman...	002...	8MDM...	gen...	30,653	17,360	95	278,155	scan ...	57%
Wolfman...	002...	8MDM...	gen...	30,653	19,038	91	305,087	scan ...	62%
Wolfman...	002...	8MDM...	gen...	30,653	17,830	86	285,683	scan ...	59%
Total: 3							262		

**Replication status**

Tape ...	Bar...	P...	Replicat...	Replication r...	Transmitt...	Transfer rat...	De-du...	Pro...	Time re...
Total: ...					0		0		

The status bar at the bottom shows the date and time: 11/20/2007 17:43:25 [sirclus7F\_VTL] Logged in. The server name and time are also displayed: Server: sirclus7F\_VTL | 5:59 PM.

## Tape History tab

The *Tape History* tab lists all of the deduplication and replication jobs that have run and provides statistics for each.

Tape name	Bar...	Dat...	Job started	Data Deduplication Statistics				Data Replication Statistics				Sta...
				Tot...	Uniq...	Dedu...	Du...	Tot...	Uniq...	Dedu...	Du...	
VirtualTa...	000...	gen...	2008/08/13...	5,000	0	> 100...	1:08	0	0	N/A	0:00	co...
VirtualTa...	000...	gen...	2008/08/13...	5,000	0	> 100...	1:09	0	0	N/A	0:00	co...

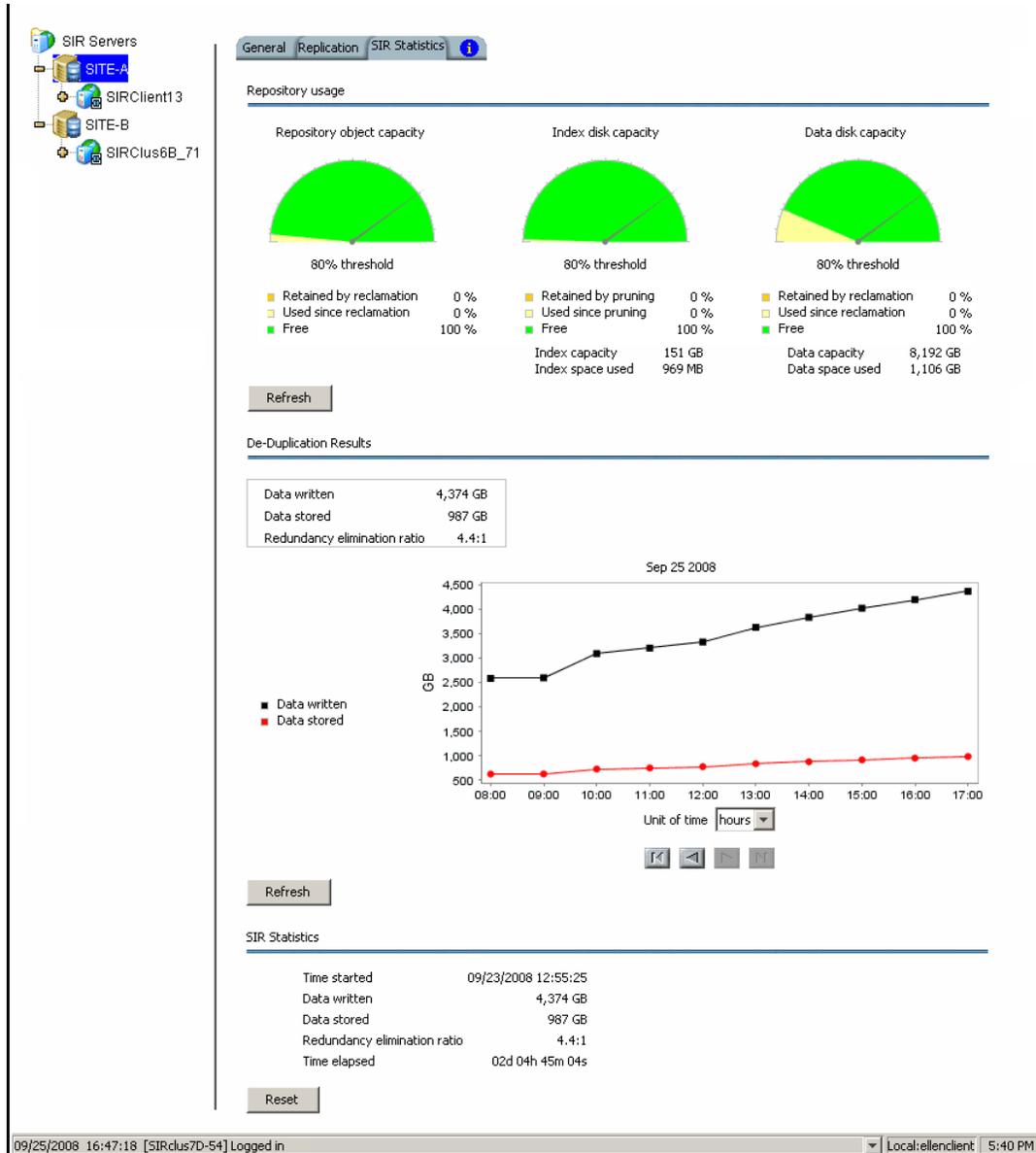
## Event Log tab

The *Event Log* tab displays informational events and errors pertaining to this policy.

Type	Date & Time	ID	Event Message
I	08/16/2008 15:07:35	50510	RDE: Policy Gab_STK-L180-00017 has completed successfully.
I	08/16/2008 15:07:34	50536	RDE: Policy Gab_STK-L180-00017 tape scan: Total tapes: 0; Tot
I	08/16/2008 15:07:32	50508	RDE: Policy Gab_STK-L180-00017 started, manual. Total tapes:
I	08/14/2008 15:44:59	50536	RDE: Policy Gab_STK-L180-00017 tape scan: Total tapes: 2; Tot
I	08/14/2008 15:44:59	50510	RDE: Policy Gab_STK-L180-00017 has completed successfully.
I	08/14/2008 15:44:57	50515	RDE: Policy Gab_STK-L180-00017 , Tape [0005000K] scan comp
I	08/14/2008 15:44:54	50515	RDE: Policy Gab_STK-L180-00017 , Tape [0005000J] scan comp
I	08/14/2008 15:43:29	50508	RDE: Policy Gab_STK-L180-00017 started, manual. Total tapes:

## Repository statistics

To view repository statistics for the entire cluster, highlight the VTL server and select the *Deduplication Statistics* tab in the right panel.



The values displayed for *Data written* represent data scanned in VTL; *Data stored* values represent the amount of unique data stored in the repository.

The *Redundancy elimination ratio* (frequently referred to in the industry as the *Deduplication Ratio*) represents this formula:  $[(\text{data scanned}) \div (\text{data stored})]$ .

The *Deduplication Statistics* display provides three ways to look at these values:

- Repository usage
- Deduplication results

- 
- Deduplication statistics

## *Repository usage*

This section of the display shows the current state of the physical disk used as the deduplication repository, which includes deduplication data and deduplication index storage. Values are based on all tape scans performed during the life span of the selected server.

*Disk Usage* values show how much disk space has been allocated to each deduplication storage component and how much space has been used.

The *Repository object capacity* graphic represents memory usage. Select *Refresh* to update the display to include activity that has occurred since the last refresh.

## *Deduplication results*

This section of the display combines *data written* and *data stored* statistics **for all accumulated data to show deduplication activity over time. Viewing data in this way allows you to calculate the redundancy elimination ratio for any period of time.**

Reviewing deduplication operations for successive weeks of full backup reveals the true redundancy ratios of week-to-week data evolution and can be used to accurately forecast repository requirements. You can identify how quickly you are using your repository disk space and when you are likely to need to add more.

Select a *Unit of time* from the drop-down list to adjust the granularity of the graph. Use the arrow buttons to scan through accumulated data. Click *Refresh* to include data for deduplication activity that has occurred since the last refresh.

## *Deduplication statistics*

This section of the display shows current statistics: a view of the redundancy elimination ratio based on tape scans performed since a user last reset the display.

For example, statistics might reflect 7 days, 1 hour, 2 minutes, and 2 seconds of deduplication processing, during which 125 GB of data was scanned by deduplication. 45 GB of data was unique and therefore stored in the repository, resulting in a redundancy elimination ratio of 2.8:1.

Statistics are automatically updated every 30 seconds. You can click the *Reset* button to reset values to zero and reset the time to the current time. Subsequent updates will reflect activity since the reset. If you view the display after a few minutes, the redundancy elimination ratio will reflect tapes currently being scanned.

It is not uncommon to see a ratio of 1000:1 for a particular tape; this simply indicates that extremely little data has changed.

---

## Reclaim disk space

During the deduplication process, only single instances of unique data are passed to the deduplication repository. The original virtual tape is replaced with a VIT pointing to deduplication storage.

Over time, VITs can be erased, formatted, or overwritten by your backup application (such as when a tape has expired). It is also possible that you may have manually deleted a VIT from the console.

When a VIT is eliminated, the pointers to deduplication storage are deleted but the actual deduplicated data is not. VTL can automatically reclaim unneeded space (the default) or you can run the process manually.

Putting a VIT in a scratch pool of a backup application does not mean that the storage used by that VIT can be reclaimed. Storage can be reclaimed only when a VIT is deleted from the console or erased/formatted/overwritten by the backup application.

At least one VIT must exist in order for data reclamation to take place.

## Reclamation thresholds

The system will run a reclamation process automatically whenever a threshold is met. There are three independent thresholds and the reclamation processes run independently for each. To see the thresholds:

1. Right-click your VTL server and select:

*Deduplication --> Reclamation --> Reclamation Parameters.*

The dialog displays the thresholds; you cannot modify these values:

- Index space reclamation
- Index pruning (removing index items related to records removed by data space reclamation)
- Data space reclamation

2. If desired, you can specify how frequently the system should check the thresholds in order to attempt to reclaim space.

You can see the status of the thresholds on the *Deduplication Statistics* tab.

---

## Manual reclamation

To manually run reclamation, right-click your VTL server and select:

*Deduplication --> Reclamation --> Start Space Reclamation (or Start Index Pruning).*

- *Start Space Reclamation* - Composed of index reclamation and storage reclamation, this option reclaims data disk space and memory.
- *Start Index Pruning* - Reclaims space on the index disk. This process is CPU intensive and does not need to be run frequently.

# Data Replication

---

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.

Keep in mind that if you intend to change the IP address or host name of your VTL appliance, you must do this before you configure replication. In order to change the IP address after you configure replication, you must remove the replication target, change the IP address, and then configure replication again.

There are four methods for replicating data in VTL; three 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).
Remote Copy	Manual	Replicates the contents of a single tape <i>on demand</i> .
Replication of virtual tapes	Automatic	Replicates <i>changed</i> data from a primary virtual tape to the same server or another server at prescribed intervals, based on user defined policies.
Replication of deduplicated tapes	Automatic	Replicates <i>changed</i> data from a primary VIT to another server at prescribed intervals, based on user-defined policies.

---

## 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 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

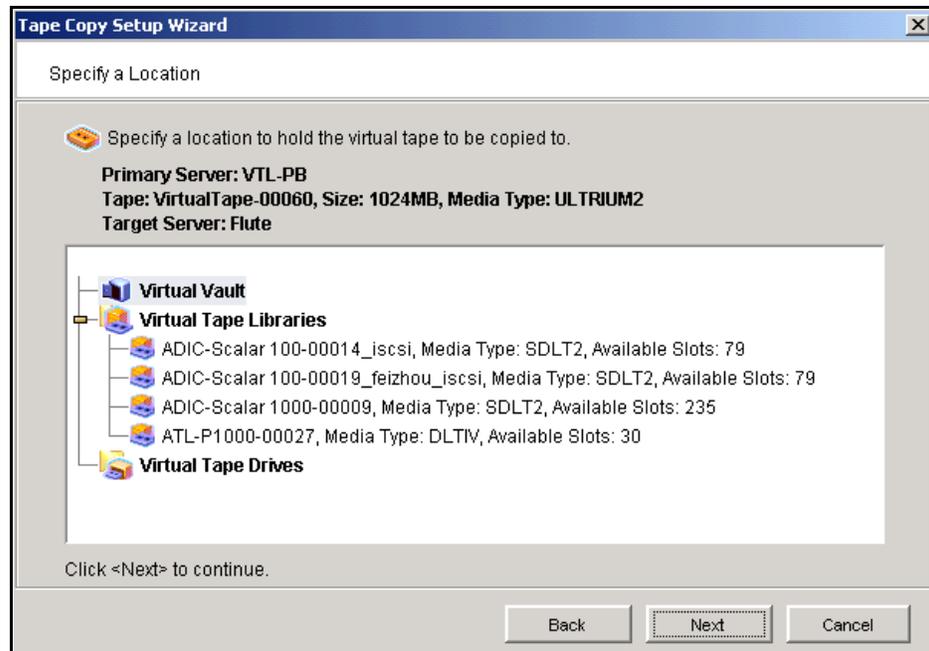
You can copy the contents of a single tape whenever you need to. Because the *Remote Copy* feature replicates the full tape rather than appending to an existing virtual tape, you can only copy a tape if there is no virtual tape on the target server with the same barcode. Therefore, if you have copied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

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

1. Right-click 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 of virtual tapes

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

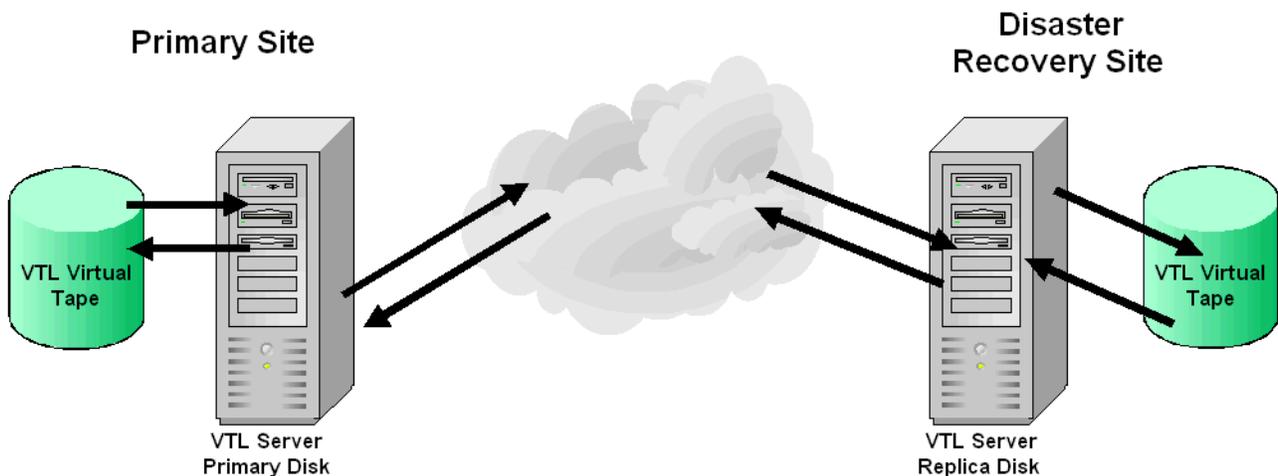
At prescribed intervals, when the tape is not in use, changed data from the *primary* virtual tape is transmitted to the *replica resource* on the target VTL server so that they are synchronized. The target VTL server is usually located at a remote location. Under normal operation, backup clients do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

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

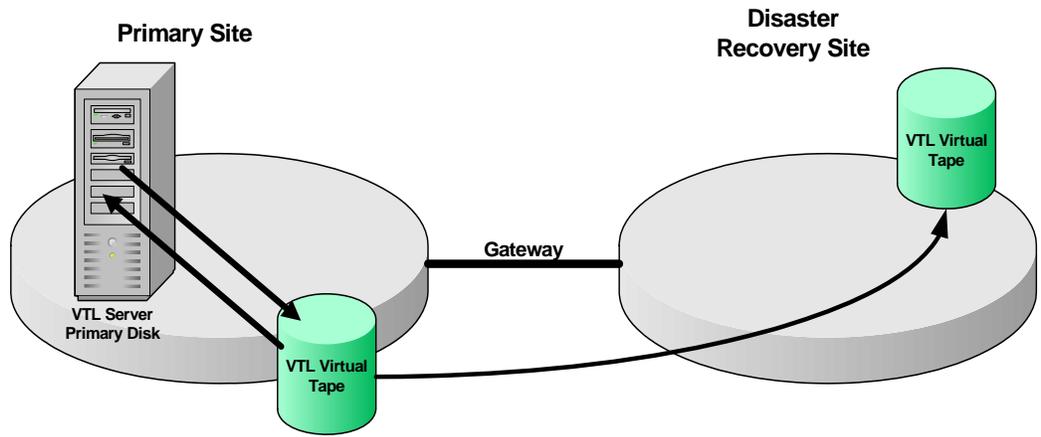
With Remote Replication, the replica disk is located on a separate target VTL server.



**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.



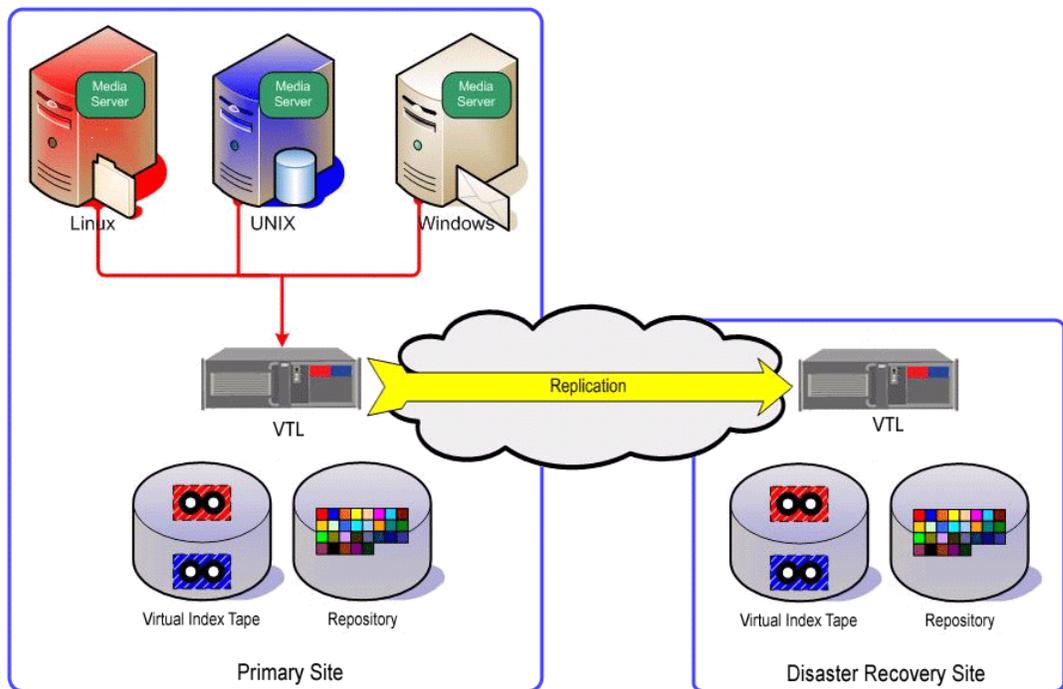
## Replication of deduplicated tapes

When you create a deduplication policy, you can configure replication for the tapes in the policy. If you do this for all tapes in all deduplication policies, you effectively replicate the entire deduplication repository.

Replication from the source server to the target server occurs via iSCSI. The target server is usually located at a remote location. If a disaster occurs and the replica is needed, the administrator can move the replicated tape from the virtual vault to its virtual tape library.

If you configure replication to a VTL cluster configuration, which incorporates separate VTL and ECO servers, deduplicated data is replicated to the ECO target server.

Because ECO replicates its virtual index tape and data, data duplicated across remote sites is deduplicated at the central site, enabling only globally unique data to be stored.

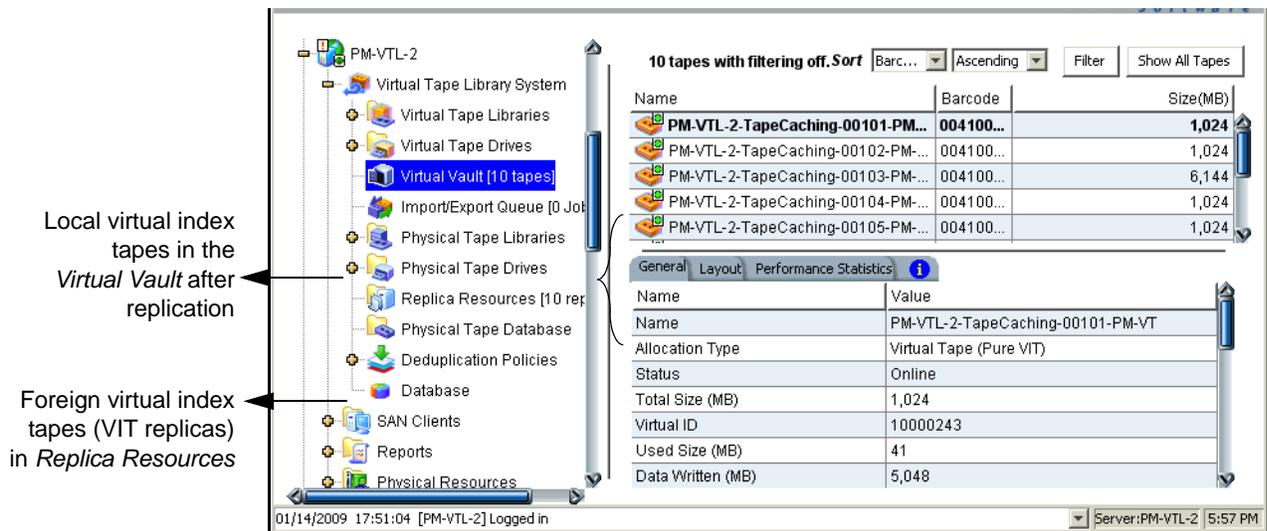


Replication of deduplicated data occurs in two phases, which you can see identified in replication status displays in the VTL console:

- During the *Index* phase of replication, the virtual index tape (VIT) from the source server is copied to the target server and becomes a foreign virtual index tape (FVIT), which you can see when you select the *Replica Resources* object in the console on the target server.
- During the *unique* phase of replication, the FVIT is scanned to determine whether or not the data blocks it uses exist locally. Missing data blocks are replicated from the source server to the target server. After all missing data blocks are replicated, the target server has all the data blocks used by the FVIT.

During the final stage, the tape is “*resolved*”: the target server automatically creates a local virtual index tape (LVIT) and puts it in the target server’s virtual vault. A red dot indicates that the tape is currently being resolved. The LVIT is now a replica of the source VIT and contains pointers to the replicated blocks of data.

Replication is complete when you see the LVIT in the target server’s virtual vault. The name of the LVIT corresponds to the name of the FVIT. The image below shows the VTL target server, with the new VITs for replicated data under the *Virtual Vault* object. A green dot indicates that the tape has been successfully resolved. The FVITs are listed when you select the *Replica Resources* object.



On the source server, you can see that replication is complete by checking the *Replication* tab for a virtual tape in a tape library. The *Resolved* field will display *true*.

Note that this final step may not occur immediately after the initial replication of data and can take some time to complete, depending on the availability of ECO tape drives on the target server and the amount of data on the FVIT.

---

## 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 administrative rights on both servers.
- (Remote Replication) You must add the target server to the management console tree on the primary server and then log into the target server.
- You must have enough space on the target server for the replica resource.
- If you will be using iSCSI protocol for replication, it must be enabled first. You must also set the default target portal. This is set on the iSCSI properties tab for the ECO server (right-click ECO server --> *Properties*).

If you are configuring replication to a VTL cluster configuration, which incorporates separate VTL and ECO servers, virtual tapes are replicated to the VTL target server and unique data is transferred to the ECO target server.

### Deduplicated tapes

The following are the additional requirements for replicating deduplicated tapes:

- Each virtual tape you want to replicate must be included in a deduplication policy.
- *At the time of configuration*, each virtual tape that will be configured for replication must be in a slot, not a virtual library tape drive.
- While you can configure replication for a virtual tape that has not been deduplicated, replication will not run until at least one deduplication has taken place.
- (Remote Replication) Just as you have to associate your ECO server with your VTL server before you can create deduplication policies, the ECO server on the target side must be associated with your local ECO server before you can configure replication.
- (Remote Replication) On the target server, you must prepare physical resources for use by ECO and enable deduplication.
- (Remote Replication) Before you can configure replication for tapes in a deduplication policy, you must associate the ECO server on the target side with your local server. If you replicating to another VTL standalone appliance, you will provide the IP address and login information for the target VTL server. If you are replicating to a VTL cluster configuration, you will provide the IP address and login information for the target ECO server.

### VTL Appliance Ports

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

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

---

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

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

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

When you set up replication, select the target server's IP addresses that are to be used for replication. Do not use the target server's main management port.

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

---

## Configure replication for virtual tapes

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

If you need to change the IP address of your VTL appliance, you must do so before configuring replication.

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

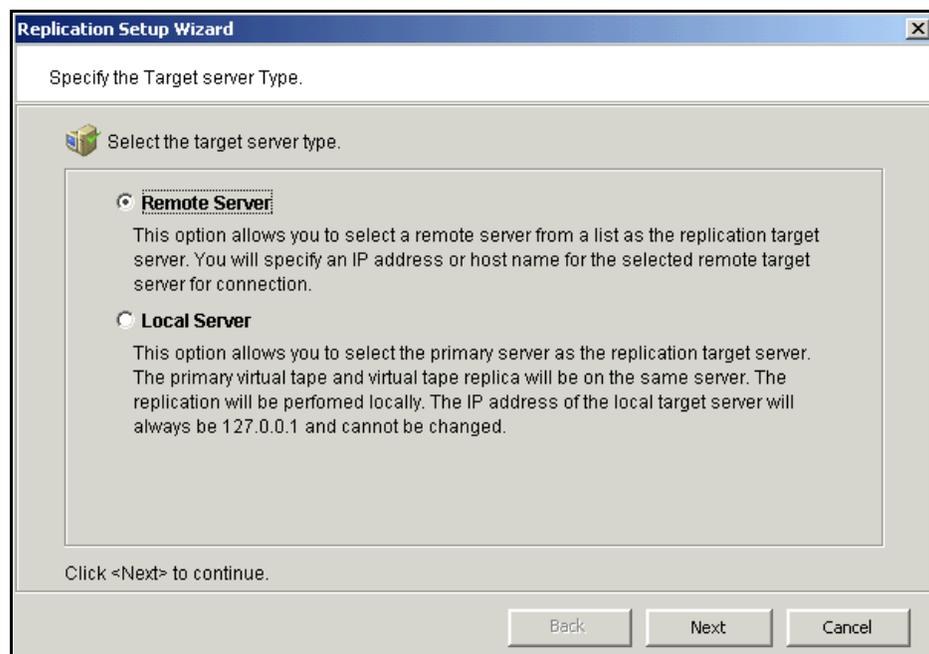
To enable replication for multiple virtual tapes in the same virtual tape library, right-click the virtual tape library and select *Replication --> Add*.

You can also right-click the virtual vault and enable replication for the virtual tapes that are in there.

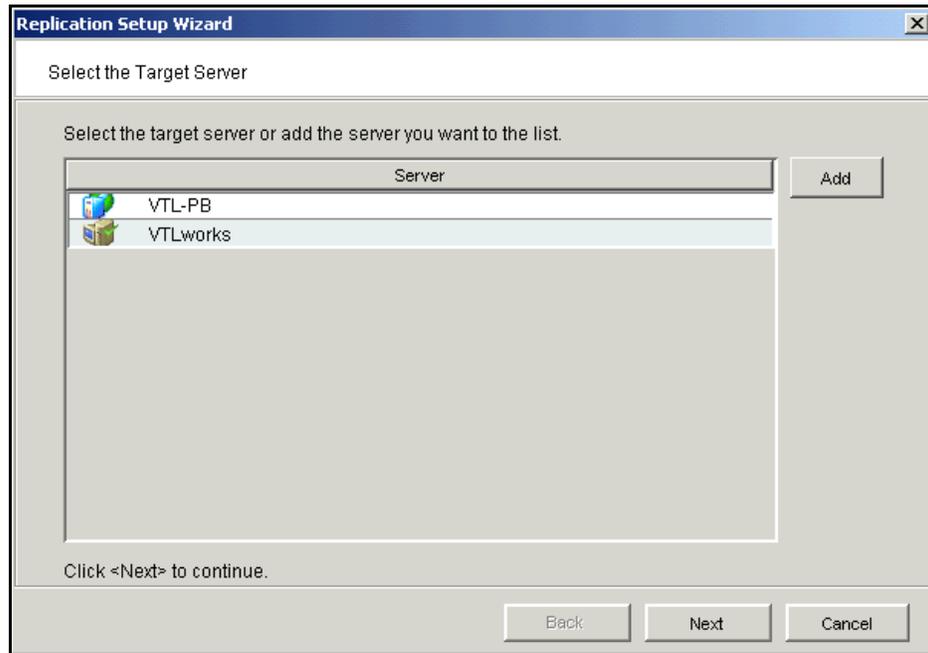
Each virtual tape can only have one replica resource.

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

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

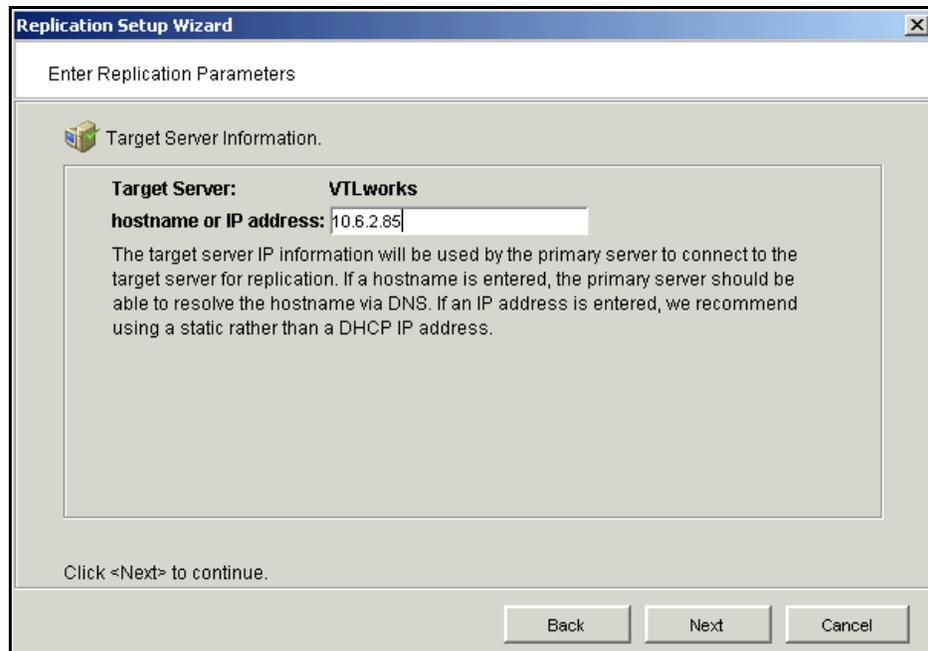


3. Select the server that will contain the replica.

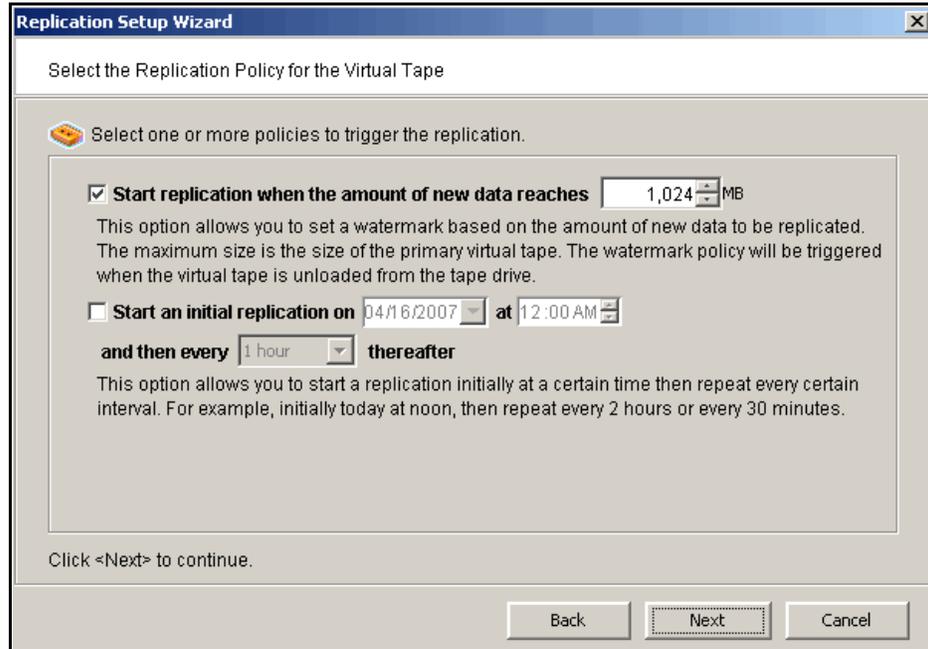


If the server you want does not appear on the list, click the *Add* button.

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



5. Configure how often, and under what circumstances, replication should occur.



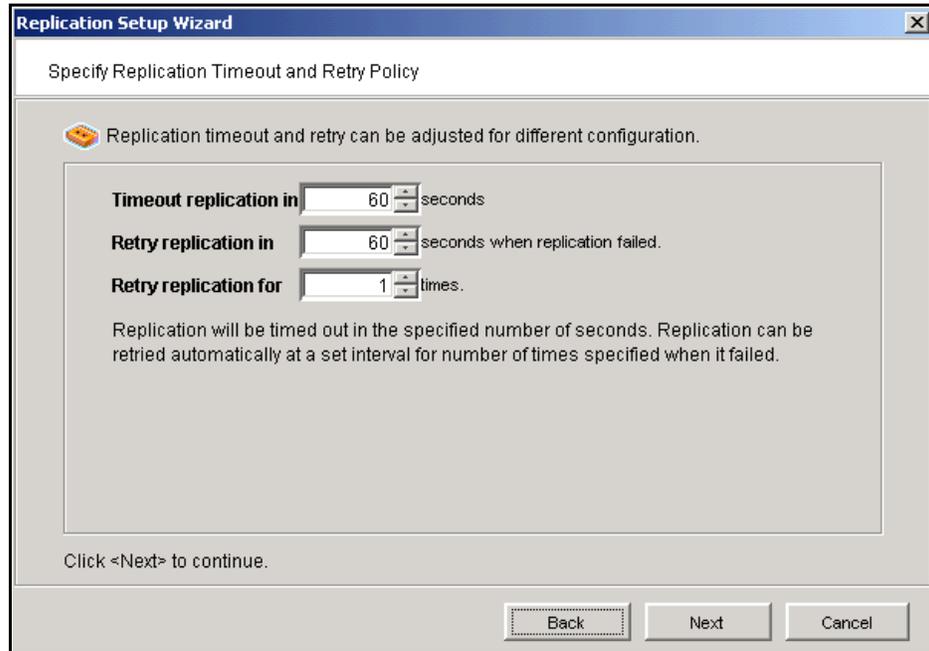
You must select at least one policy, but you can have multiple.

*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.

6. 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.

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



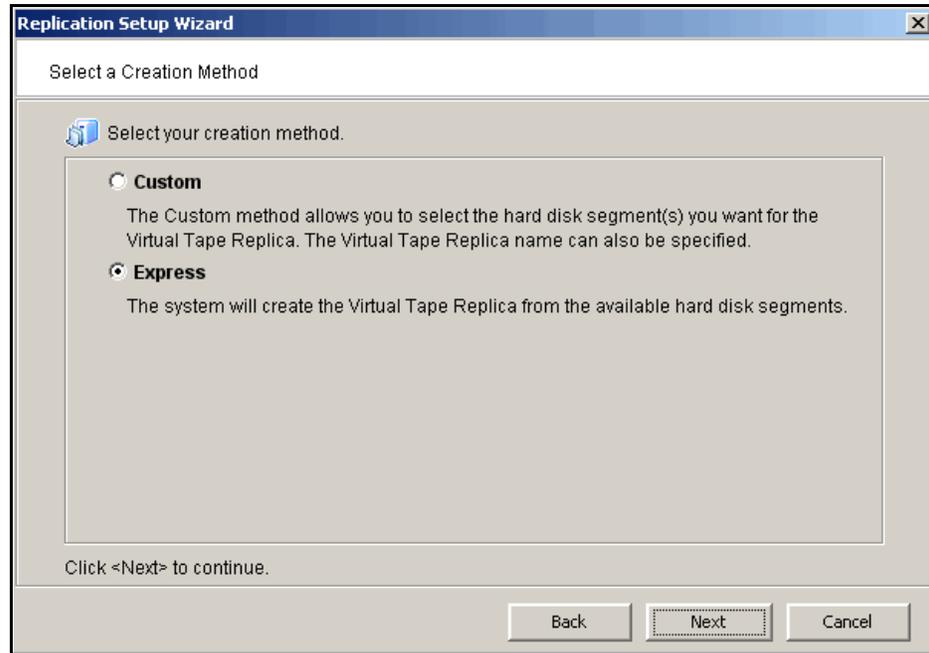
The *Compression* option provides enhanced throughput during replication by compressing the data stream.

---

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.

The *Compression* and *Encryptions* options are not recommended for replicating tapes that are or will be included in a deduplication policy.

8. Select how you want to create the replica resource.



*Custom* lets you select which physical device(s) to use.

*Express* automatically creates the resource for you using an available device(s).



---

## Configure replication for deduplicated tapes

If you need to change the IP address or hostname of your VTL appliance, you must do so before configuring replication for tapes in a deduplication policy.

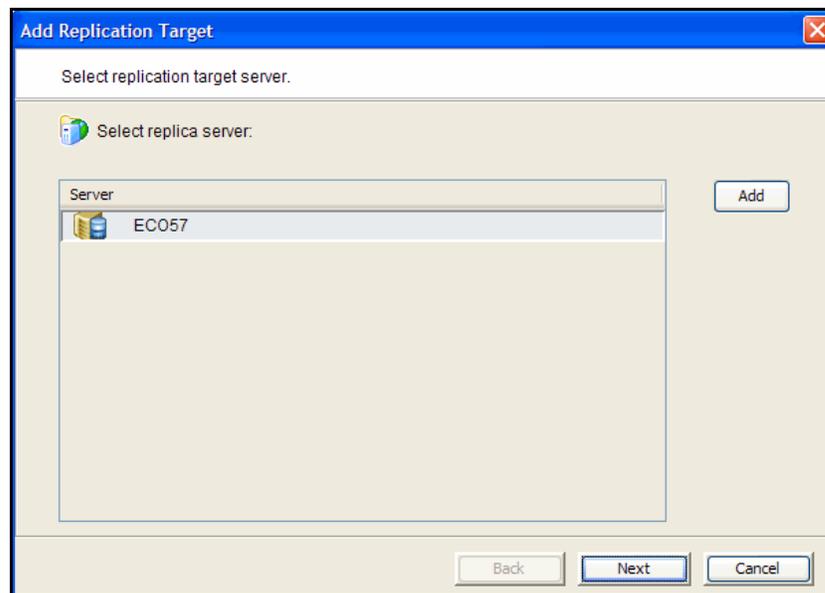
By default, replication uses eth0. If you want to replicate using eth1, you will need to configure your systems accordingly. Refer to [‘Replicating deduplicated tapes from a server using an alternate NIC’](#).

### *Add the replication target for ECO data*

If you are using ECO, before you can configure replication for tapes in a deduplication policy, you must enable replication between the source and target ECO servers. If the replica is a VTL standalone appliance, that appliance is your target.

To do this:

1. In the VTL console, add the target server and log into the target:
2. Right-click the source server and select *Options --> Deduplication --> Replication --> Add Target*.
3. Select the target server or click *Add* if the cluster is not listed.



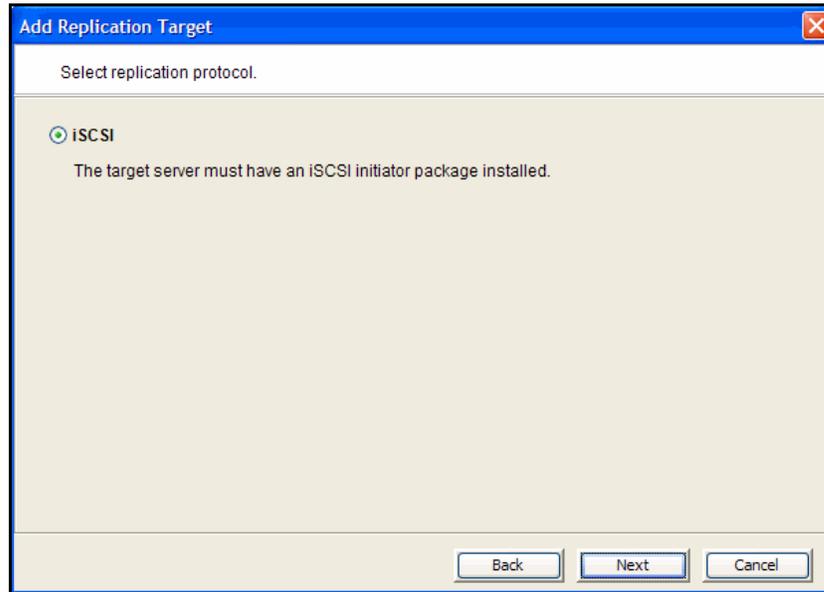
4. Enter login information for the target server.

If your target is another VTL standalone system, enter login information for the target VTL server.

---

If your target is in a VTL Cluster configuration, enter login information for the target ECO server.

5. Select *OK*. The server appears in the list and is selected for you. Select *Next* to continue.
6. In the next screen, iSCSI protocol is already selected. Select *Next* to continue.



7. In the next screen, confirm the information and click *Finish*. The target server is configured to be the replication target.

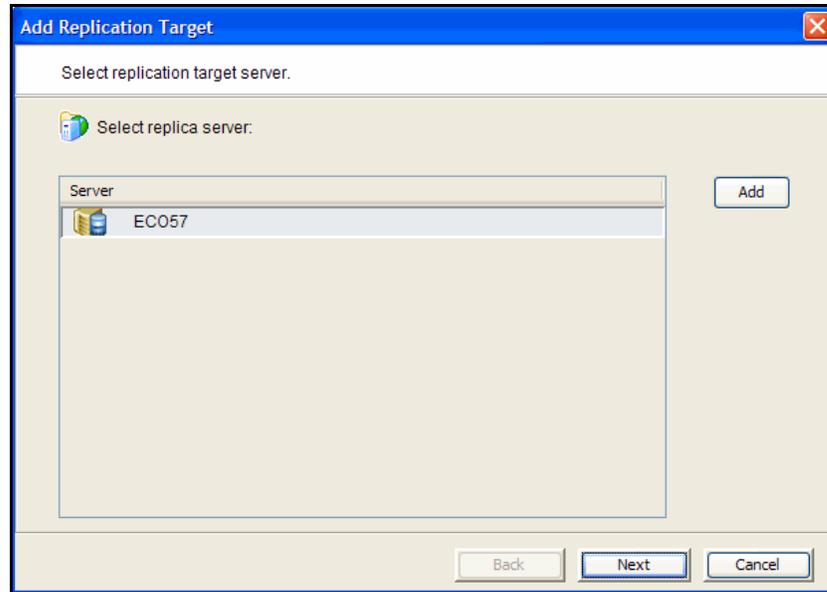
The *Replication* tab appears in the right-hand pane for both servers when replication has been configured. Content identifies the replicator (the data source) and the replica (the VTL server to which data is replicated).

You can now configure replication for tapes included in a deduplication policy (refer to '[Add deduplication policies](#)' for details).

---

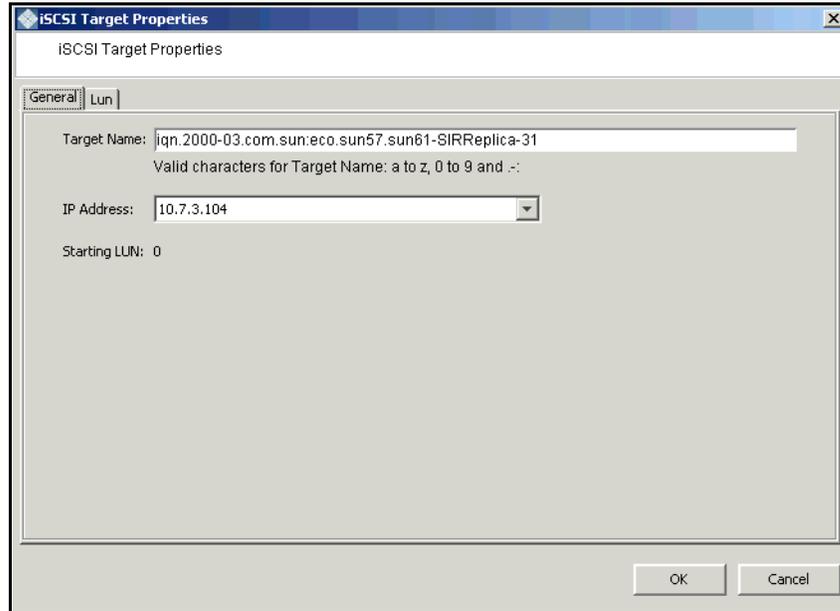
## Replicating deduplicated tapes from a server using an alternate NIC

1. Enable iSCSI protocol on the source server by choosing *RC --> Options --> Enable iSCSI*.
2. Configure replication by right-clicking on the cluster name of your source server and choose *Options --> Deduplication --> Replication --> Add Target*.
3. Select the target server or click *Add* if the cluster is not listed.



4. Enter login information for the target server.  
If your target is another VTL standalone system, enter login information for the target VTL server.  
If your target is in a VTL Cluster configuration, enter login information for the target ECO server.  
Select *OK*. The server appears in the list and is selected for you. Select *Next* to continue.
5. Once replication is configured, look under the *SAN clients* object, right-click on the target name and click on *Properties*.

6. Change the IP address from the default to the alternate IP address you want to use.



7. On the target server, replace the discovery address of the source server's previous iSCSI target IP address with the alternate IP address. To do this:

- Display the discovery address of your server:

```
iscsiadm list discovery-address
```

```
-bash-3.00# iscsiadm list discovery-address
Discovery Address: 10.8.1.41:3260
Discovery Address: 10.8.1.61:3260
Discovery Address: 10.8.13.24:3260
-bash-3.00# █
```

- Once you identify the discovery address, you need to remove it:

```
iscsiadm remove discovery-address <IP address>
```

- Add the alternate IP address as the discovery address:

```
iscsiadm add discovery-address <IP address>
```

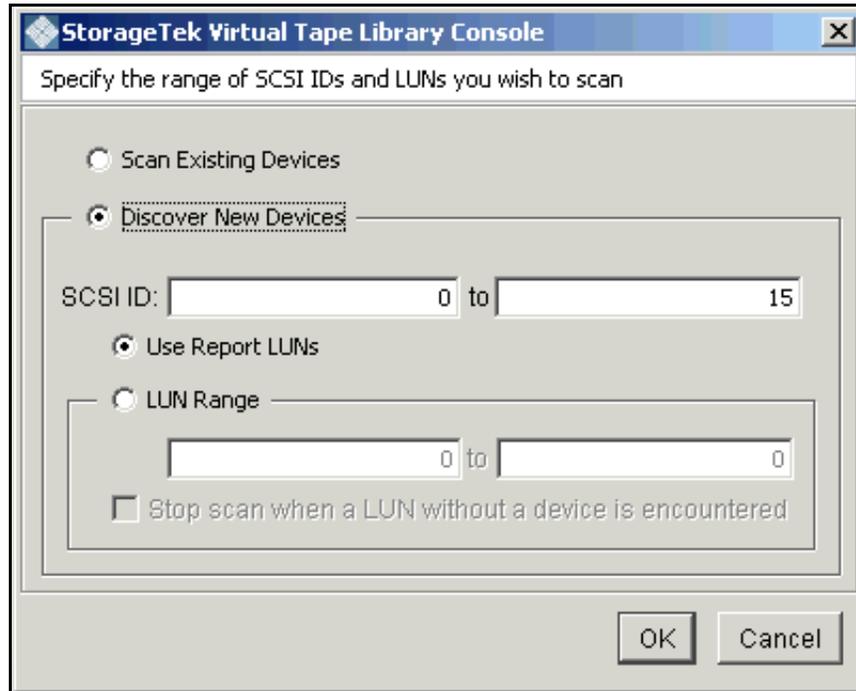
- Confirm your change by displaying the new discover address (which should be the alternate IP address):

```
iscsiadm list discovery-address
```

```
-bash-3.00# iscsiadm list discovery-address
Discovery Address: 10.8.1.41:3260
Discovery Address: 10.8.1.61:3260
Discovery Address: 192.168.130.24:3260
-bash-3.00# █
```

- Edit the /etc/iscsi/iscsi.conf file and replace the original IP address with the alternate IP address.

8. At the console, right-click and select Physical Resources to perform a rescan on the target server to rediscover the *Processor* resource over the new iSCSI target IP path.



9. On the replication target server, type the following to display the data disks from your source server.

```
dumpPDguid
```

For example, your output might look like the following:

```
-bash-3.00# dumpPDguid
GUIDs discovered on /dev/issg/c0t2d0:
    FA1C0503-3714-49FD-950B-99A6D654299C
    FA1C0504-51A7-4D26-B70C-F9E1D5587F7F
    FA1C050A-BEC1-43D7-B98F-44955A1FFB2F

GUIDs discovered on /dev/issg/c0t6d0:
    FA1C050D-8EC6-4E56-A35A-034507E85871
    FA1C050A-DABE-4578-A647-D54917EFBF78
    FA1C0504-5894-4D6C-8952-34BB2765250A
    FA1C050A-5321-438D-B79B-DA0D885BC779
    FA1C050B-2F6D-418F-86A8-BCA73BC3E58E
    FA1C050E-263E-4FEA-A348-E3C08393424D
    FA1C0500-9EB6-489F-8E93-7FAA20E1D5C5
    FA1C0507-F94F-456A-A871-A9BAFF63BD82

-bash-3.00#
```

# 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.
- *Active Policies* tab of a deduplication policy - displays information about currently running replication jobs. While replication is occurring, you will see status displays related to the Index and unique replication phases.
- 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 virtual 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: throgneck2, 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: throgneck2 (10.3.3.161)  
Primary Disk: VirtualTape-00160 (ID: 160)  
Target Server: VTLworks (10.6.2.85)  
Target Disk: throgneck2-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

- Deduplication Status Report - can be run from the *Reports* object. It provides a centralized view for displaying real-time replication status for all deduplication policies. The following is a sample *Deduplication Status Report*.

vlt59sw113		<b>Deduplication Status Report</b>						10/22/08 4:57:24 PM	
		10/2/08 12:00:00 AM - 10/2/08 11:59:59 PM							
Policy Name:		TCTDDD\$R_Sol_FalconVTL_IBMTD2-410							
Total Tapes:		0							
SR Cluster:		vlt5r67 10.8.9.67							
Schedule:		7							
Replication:		Enabled (N/A/N/A)							
Date/Time	Type	# of Tapes	Total Data(MB)	Unique Data(MB)	Dedupe Ratio	Duration	Performance (MB/sec)	Status	
10/2/08 7:18 PM	end of backup	1	1981	0	-	0:00:39	50	complete	
	replicated		1981	0	-	0:01:37	20		
10/2/08 4:25 PM	end of backup	1	3961	0	-	0:00:53	74	complete	
	replicated		3961	0	-	0:01:24	47		
10/2/08 4:16 PM	end of backup	1	1981	0	-	0:00:52	38	complete	
	replicated		1981	0	-	0:01:10	28		
10/2/08 1:11 PM	end of backup	1	1981	0	-	0:00:36	55	complete	
	replicated		1981	0	-	0:01:21	24		
10/2/08 10:17 AM	end of backup	1	7921	0	-	0:01:27	91	complete	
	replicated		7921	0	-	0:02:31	52		
10/2/08 10:09 AM	end of backup	1	1981	0	-	0:01:37	20	complete	
	replicated		1981	0	-	0:03:25	9		
10/2/08 7:01 AM	end of backup	1	1981	0	-	0:00:38	52	complete	
	replicated		1981	0	-	0:01:32	21		
10/2/08 3:57 AM	end of backup	1	1981	0	-	0:00:51	38	complete	
	replicated		1981	0	-	0:01:05	30		
10/2/08 12:51 AM	end of backup	1	1981	0	-	0:00:34	58	complete	
	replicated		1981	0	-	0:01:21	24		

---

## Promote a replica resource

Promoting a replica resource is only valid for virtual tapes, not VITs.

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 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.

## Promote a replica resource without breaking the replication configuration

Under normal circumstances, when replica storage is needed, the administrator promotes the replica to become a usable virtual tape, thereby breaking the replication configuration.

However, there may be times, such as for disaster recovery testing, when you want to promote replica storage *without* breaking the replication configuration.

When you promote a replica without breaking the replication configuration, you will have a *read-only* version of the tape on the replica server. This tape can then be used for testing or for file recovery.

You must have a valid replica storage in order to promote it. For example, if a problem occurred (such as a transmission problem or the replica storage 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 replica storage while a replication is in progress.

1. In the VTL console, locate the target server, right-click the appropriate Replica Storage and select *Replication --> Test Mode Promote*.
2. Confirm the promotion and click *OK*.

---

## Access data on a replicated virtual tape

If a replicated virtual tape is needed (due to a failure at the primary site), the administrator can do one of the following so that the data can be accessed by backup software:

- Move the virtual tape from the virtual vault to a virtual library on the target server.
- If the primary cluster has been repaired, you can replicate the virtual tape back to that server. This replicates the entire tape, which can be time consuming.
- If you move a local VIT out of the vault, replication of this VIT will be discontinued until the tape is moved back to the vault. **It is important to note** that any new data added to the tape while it is not in the vault will be overwritten when the tape is returned to the vault and replication proceeds.

## Change your replication configuration options

**Note:** This is only valid for virtual tapes, not VIT replication.

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

## Suspend/resume replication schedule

This is only valid for virtual tapes, not VIT replication.

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 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

This is only valid for virtual tapes, not VIT replication.

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

To stop replication of a VIT, right-click the policy and select *Stop*.

Note that you do not need to stop an active replication job so that a backup can occur. When a virtual tape is mounted in a virtual tape drive, the active replication job will automatically be cancelled so that the backup application can write to the tape. Replication will continue when the next replication trigger occurs.

## Manually start the replication process

This is only valid for virtual tapes, not VIT replication.

To force a replication that is not scheduled, right-click a primary virtual tape and select *Replication --> Synchronize*.

## Remove a replication configuration

**Virtual tapes** This procedure allows you to remove the replication configuration on the source server and either delete or promote the replica resource on the target server at the same time.

If you need to change the IP address of a VTL appliance that has replication configured for virtual tapes, you must complete this procedure before changing the IP address, and then reconfigure replication afterward.

1. Right-click 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.
2. Select the replication target server, the option to remove or promote, and select the virtual tape replicas.
3. Select *OK*.
4. In the confirmation message box, type *Yes* to confirm that you want to remove replication configuration from the selected tapes.

A success message is displayed when the process is complete.

**Deduplicated tapes** To remove replication for tapes included in a deduplication policy, including replica resources for FVITs on the target server, edit the policy and uncheck the *Enable Replication* option. If you need to change the IP address or a hostname of a VTL appliance that has replication configured for deduplicated tapes, you must complete this procedure before changing either the IP address or hostname, and then reconfigure replication afterward.

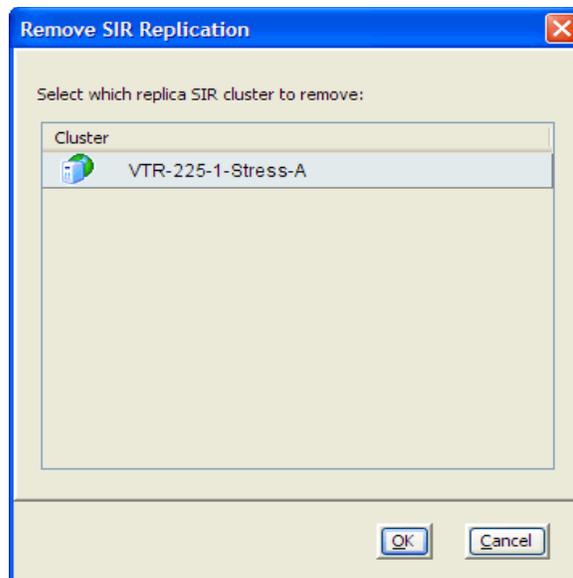
---

To remove replication of deduplicated tapes from the VTL server entirely, do the following:

1. To remove the target server, right-click the source server and select *Options --> Deduplication --> Replication --> Remove Target*.
2. Select the deduplication cluster (target server) you want to remove and click *OK*.

A series of dialogs is displayed while replication configuration is removed from the source and target servers. The *ECO Replication* tab is also removed. The *Remove Deduplication Replication* dialog closes when the process is complete.

If replication processes are running on the target (including creating the LVIT from the FVIT), target removal will fail. Re-try at a later time.



If you are removing replication to another VTL server, the procedure is now complete. If you are removing replication to a VTL cluster, do the following on the target (ECO) server:

1. Open an SSH session on the target server and execute `iscsiadmin2` to bring up the menu.

```
iscsiadm Utility v1.13
Main Menu
=====
    1) Discover a Target
    2) Delete a Target
    3) Edit a Target
    4) Show known Targets
    5) Show Active Targets
    6) Rescan a Target
    7) Login to a Target
    8) Login to all Targets
    9) Log off a Target
   10) Log off all Targets
Selection (leave blank to quit):
```

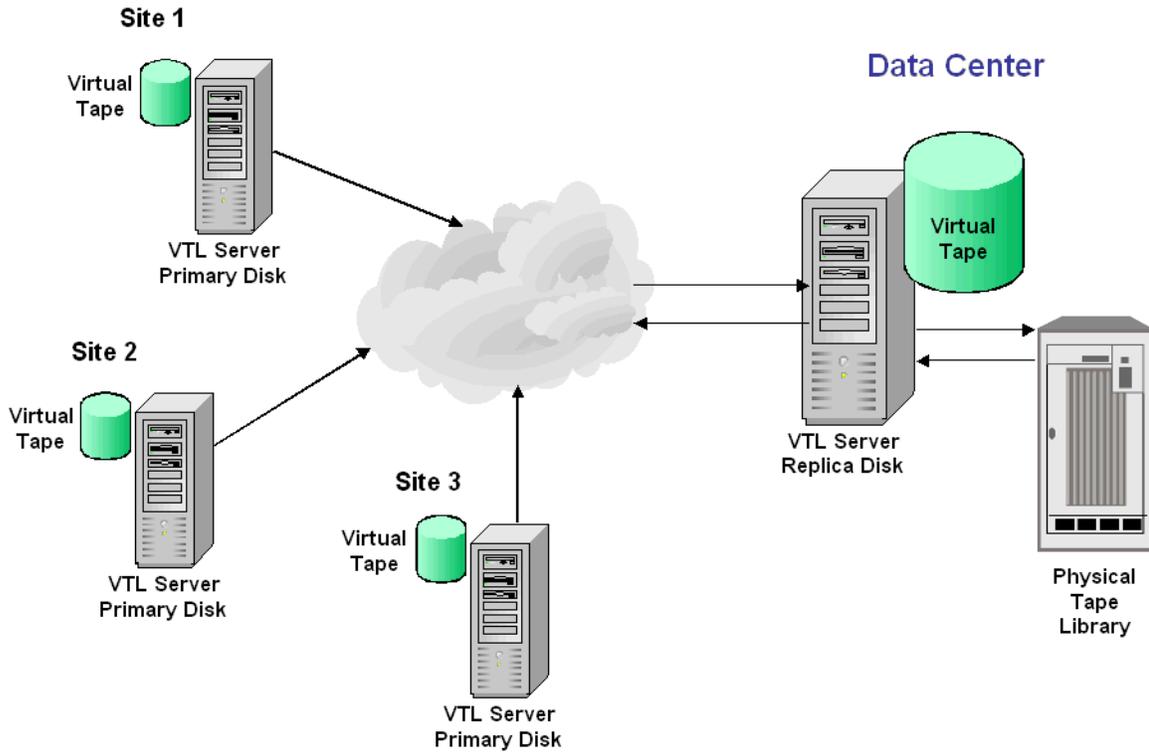
2. Enter 9 to log off the iSCSI target or 10 to log off all iSCSI targets, then follow the onscreen instructions to get back to the main menu.
3. Enter 2 and follow the onscreen instructions to delete the iSCSI target, then follow the onscreen instructions to get back to the main menu. Press *Enter* to quit.
4. Locate the file `$ISHOME/etc/hostname/ecocluster.conf`.

Search for ECOREplicator tags that match the replication source name.

Delete any line that contains this tag. For example, if the replication source server `h124-128` is to be removed, delete this line:

```
<ECOREplicator guid="ac1e8037-0000-47db-5a50-4229cd56cde8"
name="guigroup_h124-182"/>
```

## Consolidate 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.

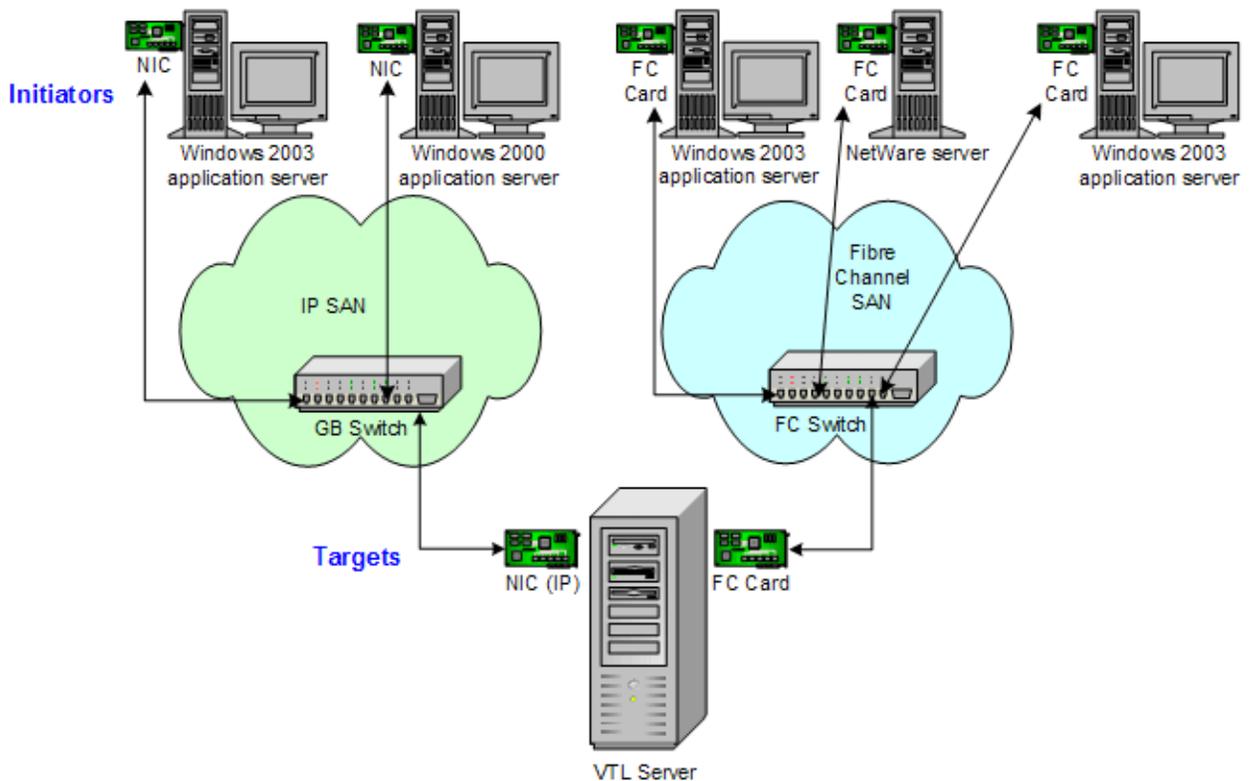
In this environment, if you will be exporting tapes from the remote VTL server to the physical tape library, you want to make sure that when you create tapes on the primary servers (at the multiple VTL locations *without* physical tape libraries), you match the barcodes of the tapes on the physical library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

# Fibre Channel Configuration

## 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.

## 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 the Server and select *Options --> Enable Fibre Channel*. 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*.

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. For security purposes, you should assign specific WWPNs to specific clients.

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 the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard*.
- Right-click the *SAN Clients* object and select *Add*. Refer to '[Add SAN Clients \(backup servers\)](#)' for more information.

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

8. Assign virtual tape libraries to clients.

For security purposes, you can assign specific tape libraries/drives to specific clients. For the rest, you can use the *Everyone* client. Refer to '[Assign virtual tape libraries to clients](#)' for more information.

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. For security purposes, you should assign specific WWPNs to specific clients.

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, 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*.

### Zoning

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 backup server 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.

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.

## 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. Check the certification matrix on our website to see a complete list of certified cards.

- |   |  |
|---|--|
| Storage array                           | <p>Connect an FC cable from a port on the storage array to an FC port on the FC switch.</p> <p>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.</p>   |
| Backup servers                          | <p>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.</p>  |
| Configure a FC switch using soft zoning | <p>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.</p> <ol style="list-style-type: none"><li>1. Access the FC switch via its web interface and log in if necessary.</li><li>2. Access the Name Server Table.</li><li>3. Access the zoning configuration and log in if necessary.</li><li>4. Using previously recorded FC HBA information, look for the WWPNs for the adapters from the VTL appliance, storage array, and backup servers.</li><li>5. Create aliases for each WWPN.</li></ol> <p>Note that some switches (i.e. McData) do not use aliasing.</p> |

- 
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.

### *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. For Solaris systems, you should reboot 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).

---

## 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*.

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

### *NetWare clients*

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 = no
  - 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, we support using the miniport drivers. 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. For any platforms that are not listed, please refer to the certification matrix on our website.

### 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 *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.

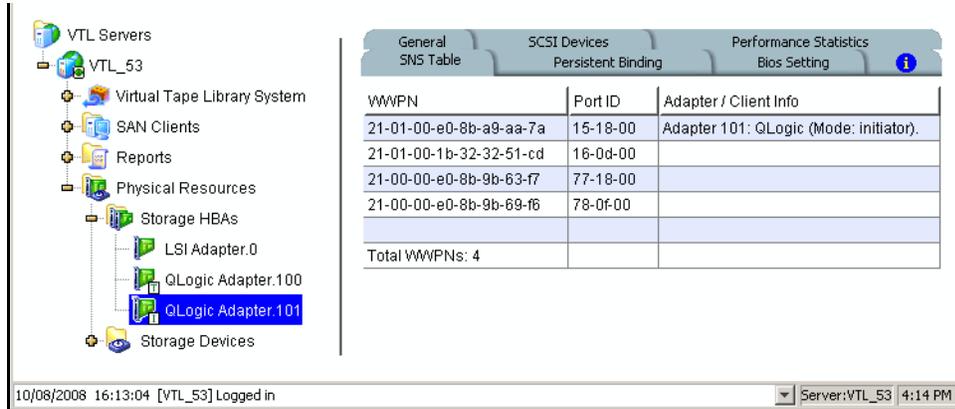
Name	Value
Adapter No	101
Adapter Info	QLogic
Mode	initiator
WWPN	21-01-00-e0-8b-a9-aa-7a
Port Status	Link Up

**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 the adapter and select *Rescan*.

Vend...	Product ID	SCSI Ad...	Size ...	Used ...	Unconfigure...	Available...
F...	IPSTOR DI...	101:0:10:0	199,...	62,431		137,561
F...	IPSTOR DI...	101:0:10:1	399,...	63,461		336,531
F...	IPSTOR DI...	101:0:10:2	507,...	74,953		432,190
F...	IPSTOR DI...	101:0:11:0				
Total: 4			1,10,...	200,845	0	906,282

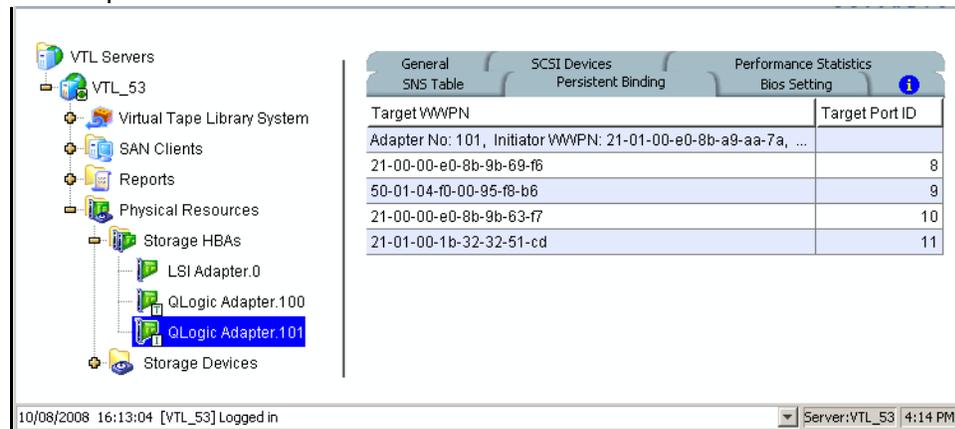
SNS Table tab

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 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.

Name	Current Value	Default Value	Valid Values
Frame Size	512	2048	512, 1024, 2048
Loop Reset...	0	5	0 - 60
Enable Har...	Disable	Disable	Disable, Enable
Loop ID	0	0	0 - 125
Execution T...	255	255	0 - 256
FC Topology	Point to Point only	Loop only	Loop only, Point to...
Fast Post	Disable	Enable	Disable, Enable
LUNs per T...	256	8	0 - 256
Enable LIP ...	Enable	Disable	Disable, Enable
Enable LIP ...	Disable	Enable	Disable, Enable
Enable Tar...	Enable	Disable	Disable, Enable
Login Retry ...	8	8	0 - 255
Port Down ...	8	8	0 - 255
Driver Load ...	Disable	Enable	Disable, Enable
IOCB Alloca...	512	512	0 - 512
FC Tape Su...	Enable	Disable	Disable, Enable
FC Confirm	Enable	Disable	Disable, Enable
Data Rate	Auto	Auto	1 Gb, 2 Gb, Auto

**Performance Statistics tab**

The *Performance Statistics* tab displays a chart showing read and write throughput for the last 60 minutes. Current performance is also displayed. All information is displayed in MB per second.

Read/Write Performance

60 50 40 30 20 10 0 MB/s

60 50 40 30 20 10 0 Minutes Ago

Hide Current Write Performance (MB/s): 0

Hide Current Read Performance (MB/s): 0

# 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.

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

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 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.

Name	Value
Server Name	VTL_53
Login Machine Name	10.6.2.53
Login User Name	root
O.S. Version	Red Hat Enterprise Linux Server release 5.1 (Tikanga)
Kernel Version	Linux 2.6.18-53.1.19.el5 #1 SMP Tue Apr 22 03:01:10 EDT 2008 x86_64
Processor 1 - 2	Intel(R) Xeon(R) CPU 5148 @ 2.33GHz 2327 MHz
Memory	3953 MB
Swap	4094 MB
Network Interface	eth0 - mtu 1500 inet 10.6.2.53 mac 0:19:b9:de:62:d4
Protocol(s)	Fibre Channel, iSCSI
Admin Mode	Read/Write
Server Status	Online
System Up Time	1 day 46 minutes 48 seconds
VTL Up Time	1 day 40 minutes 1 second
Fibre Channel WWPN	21-00-00-e0-8b-89-aa-7a [target]
Fibre Channel WWPN	21-01-00-e0-8b-a9-aa-7a [initiator]

---

## 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.

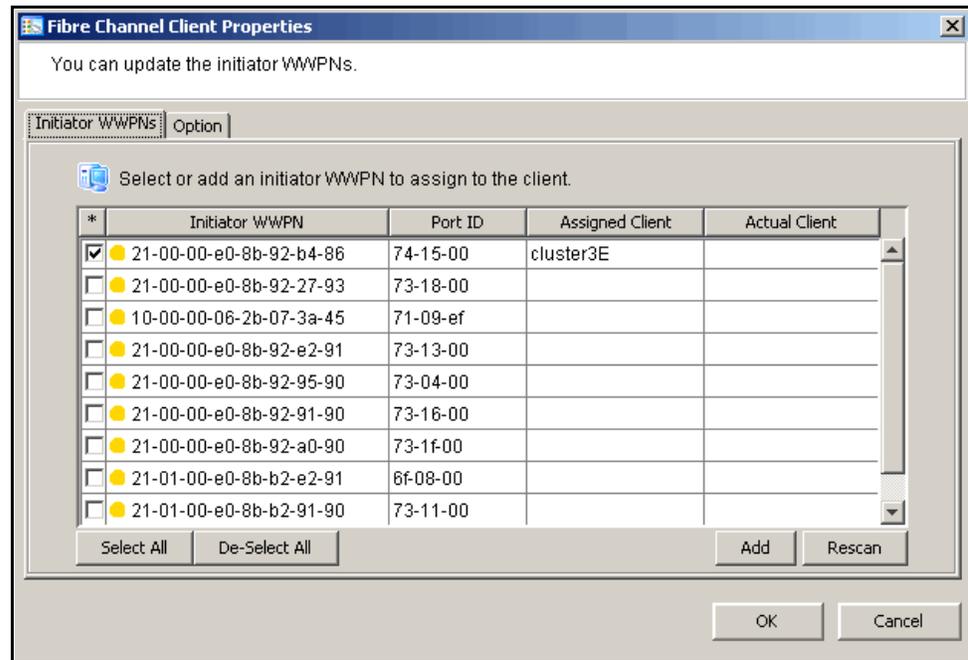
To simplify this process, when you enabled Fibre Channel, an *Everyone\_FC* client was created under *SAN Clients*. This is a generic client that you can assign to all (or some) of your tape libraries/drives. It allows any WWPN not already associated with a Fibre Channel client to have read/write non-exclusive access to any tape libraries/drives assigned to *Everyone\_FC*.

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. For security purposes, you should assign specific WWPNs to specific clients.

Do the following for each client:

1. Highlight the Fibre Channel Client in the console.

- Right-click the protocol under the client and select *Properties*.



- 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

- 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

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](#)

## iSCSI users

*VTL iSCSI Users* are used for iSCSI protocol login authentication from iSCSI backup servers. When you configure secured access for backup servers, you designate users who can authenticate for the client.

There are several ways to create iSCSI users:

- Use the *VTL User/Administrator Management* function in the VTL console and select *VTL iSCSI User* from the *Group* list. Create at least one unique user for each client.
- Add users when the *Add SAN Client* function requires you to add/select users who can authenticate for the client.
- Add users to an existing client in *iSCSI Client Properties*.

---

## Windows configuration

### Requirements

- A VTL server with an Ethernet adapter installed.
- A Windows client machine.
- iSCSI software initiator installed on each backup server. iSCSI initiator software/hardware is available from many sources. You can download the Microsoft iSCSI initiator from Microsoft's website:  
<http://www.microsoft.com/windowsserversystem/storage/iscsi.mspx>

### Prepare client initiators to access your VTL server

Before a backup server (the client initiator) can communicate with a VTL server, the two entities need to mutually recognize each other. Use an iSCSI initiator on every backup server that will access the VTL server using iSCSI. This will let you add the VTL server as a target portal and log the client onto the iSCSI target you create on the VTL server.

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.

1. Run *Microsoft iSCSI Initiator* on the backup server.

You can find the program in the Control Panel or on your desktop (if you are the user that installed it).

2. Click the *Discovery* tab, then click *Add* under the *Target Portals* group box.

3. Enter the VTL server's IP address or name (if resolvable).

To determine the IP address, go to the VTL console. Select the VTL server object. The IP address is on the *Login Machine Name* line in the right-hand pane of the console.

Use the default port (3260) and then click OK to add the client.

### Enable iSCSI

In order to add a client using the iSCSI protocol, you must enable iSCSI for your VTL server.

If you haven't already done so, right-click your VTL server in the VTL console and 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.

---

In this “open access” scheme, access is controlled purely by zoning. Any backup server that is zoned with any of the target WWPNs of the VTL server can access the virtual tape library and drives that are assigned to the iSCSI target.

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. For security purposes, you should use the “Secured Access” scheme outlined below.

In a “Secured Access” scheme, access is dictated by creating specific clients to represent specific backup servers instead of using the built-in *Everyone\_iSCSI* client. In this mode, each backup server can access *only* its own designated virtual tape library or drives.

The following sections take you through the process of configuring iSCSI clients to work with the VTL server.

## Add an iSCSI client

1. In the VTL console, right-click *SAN Clients* and select *Add*.
2. Enter the client name.
3. Select *iSCSI*.
4. Select the initiator that this client uses.

iSCSI clients correspond to specific iSCSI client initiators, and consequently, the client machines that own the specific initiator names. When a client connects to the VTL server, it can access only the resources assigned to a specific initiator name.

By default, when a backup server 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. If you already added the VTL server as a Target Portal using the iSCSI initiator on your backup server, the initiator name and backup server IP address appear in the dialog.

Otherwise, click *Add* and add the initiator name manually. (The IP address will not display.)

An available initiator shows a green dot; select the initiator name that is associated with the backup server’s IP address.

5. Add/select users who can authenticate for this client.

To define authenticated access (using CHAP), select *Select or add users who can authenticate for the client*. iSCSI users you have already created in the VTL console are displayed. You can select one of these users or select *Add* to create a new user.

More than one username/password pair can be assigned to the client, but they will be useful only when coming from the machine with an authorized initiator name.

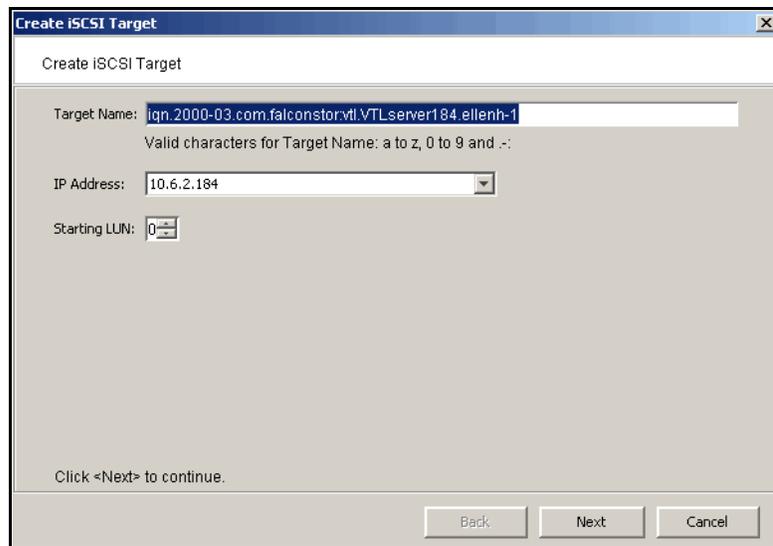
---

For unauthenticated access, select *Allow unauthenticated access*. The VTL server will recognize the client as long as it has 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. Expand the *SAN Clients* object until you see the *iSCSI* object.
3. Right-click the *iSCSI* object and select *Create Target*.



4. Enter a name for the target or accept the default and select the IP address of the adapter on the VTL server.

The list includes all Ethernet adapters you have configured on the server.

Network adapter(s) on the backup server need to be on the same subnet(s) as the selected adapter(s) on 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 (virtual tape library) to the new target.

---

## Assign a virtual tape library to the iSCSI target

1. Select the virtual library to be assigned to the client.  
You can also select *Allow tape drives in the tape library to be assigned individually* to display the virtual drives in the library.  
You can only assign a device to a client once even if the client has multiple targets.
2. On the next screen, change the LUN for the resource if you need to resolve a conflict.
3. 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 provided by the vendor.

1. To see the iSCSI targets from the client machine, run *Microsoft iSCSI Initiator* again.
2. Select the added target and click *Log On*.  
If it is desirable to have a persistent target, select *Automatically restore this connection when the system boots*.
3. Click *Advanced* and select *CHAP logon information* in the *Advanced Settings* dialog. Replace the initiator name with any of the usernames you selected as an iSCSI user for this client.  
In *Target Secret*, enter the password associated with that username.  
Click *OK*.
4. Click *OK* to log on to the target.

The status for the target will change from *Inactive* to *Connected*.

The *Targets* tab lists all iSCSI targets, whether or not they are connected. To log off a backup server from its connection, select the target, click *Details*, select the *Target Identifier*, and then click *Log Off*.

If you selected the option to *Automatically restore this connection*, the iSCSI target is listed in the *Persistent Targets* tab.

## Disable iSCSI

To disable iSCSI for a VTL server, right-click 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
```

### Enable iSCSI

Refer to [‘Enable iSCSI’](#) for more informations.

### Add an iSCSI client

Refer to [‘Add an iSCSI client’](#).

---

## Create targets for the iSCSI client to log onto

Refer to ['Create targets for the iSCSI client to log onto'](#).

## Assign a virtual tape library to the iSCSI target

1. Select the virtual library to be assigned to the client.  
You can also select *Allow tape drives in the tape library to be assigned individually* to display the virtual drives in the library.  
You can only assign a device to a client once even if the client has multiple targets.
2. On the next screen, change the LUN for the resource if you need to resolve a conflict.
3. 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
```

# 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 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.

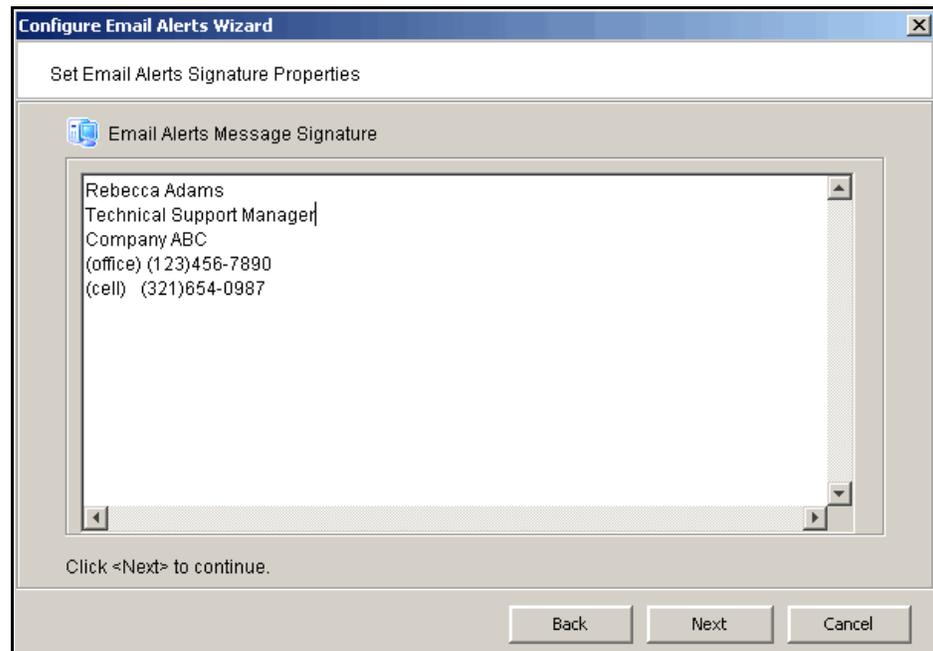
*CC* - Specify any other email accounts that should receive emails from Email Alerts.

*Subject* - Specify the text that should appear on the subject line.

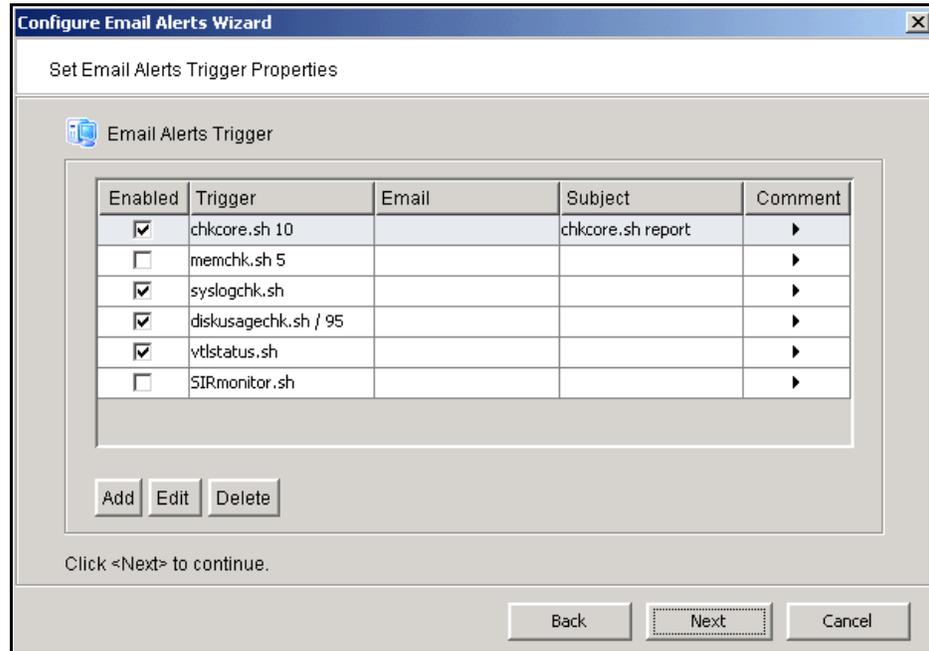
*Interval* - Specify how frequently the Email Alerts triggers and the System Log should be checked.

*Test* - Click the *Test* button to send a test Email Alerts email.

3. In the *Signature* dialog, enter the contact information that should appear in each Email Alerts email.



- In 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, we include scripts/programs 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 in 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.

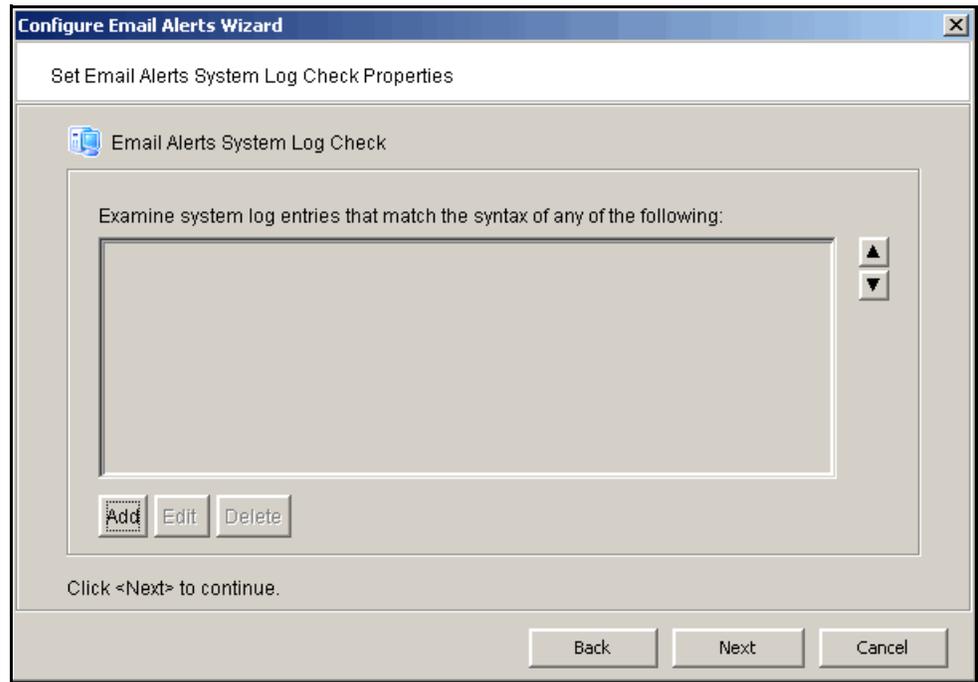
---

**SIRmonitor.sh** (ECO status check) - This script checks usage of the index repository and data repository. If the current usage is above the following levels, Email Alerts sends an email report.

- # default data repository storage usage triggering level=90%
- # default index space usage triggering level =90%

If you need to modify an existing script or create a new script/program, refer to [‘Script/program trigger information’](#) for more information. You cannot delete the predefined triggers.

5. In the *System Log Check* dialog, indicate the terms that should be tracked in the system log by Email Alerts.



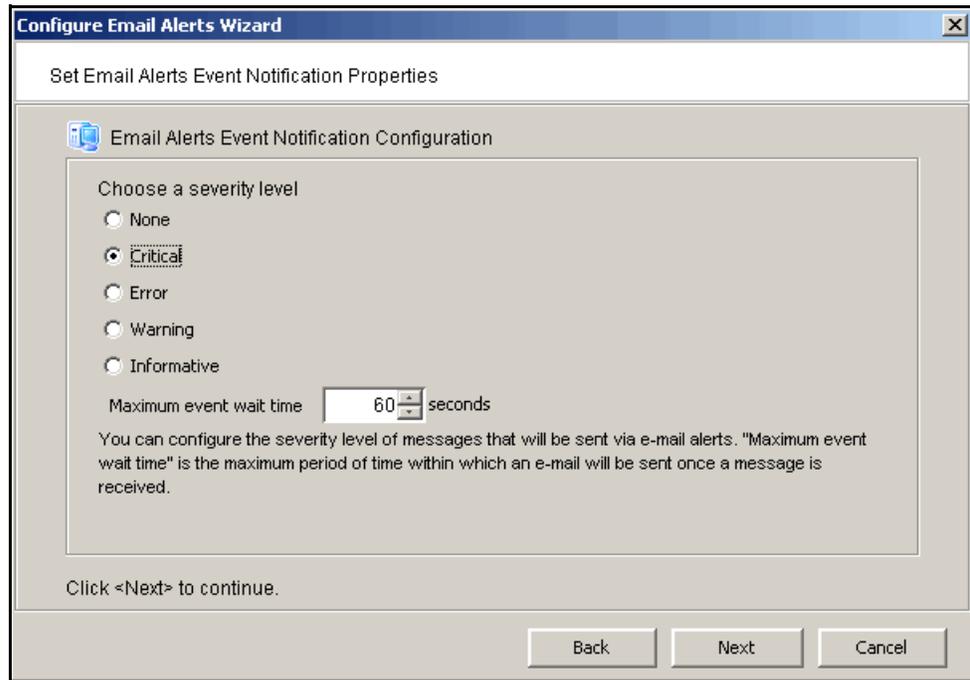
The system log records important events or errors that occur in the system, including those generated by VTL.

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. In 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 an event occurs.

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 your VTL server and selecting *Email Alerts*.

Click 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, we include several scripts/programs 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 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 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 >> $IPSTORCLHMLOG
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.

# VTL Server

---

The VTL Server is designed to require little or no maintenance.

All day-to-day VTL administrative functions can be performed through the VTL console. However, there may be situations when direct access to the server is required, particularly during initial setup and configuration of physical storage devices attached to the server or for troubleshooting purposes.

If access to the server's operating system is required, it can be done either directly or remotely from computers on the network.

All VTL commands are run from the `/usr/local/vtl/bin` directory.

The following commands are available:

- `vtl start` - Starts the VTL server processes
- `vtl restart` - Stops and then starts the VTL server processes
- `vtl status` - Checks the status of the VTL server processes
- `vtl stop` - Stops the VTL server processes

**Note:** For memory purposes, any time you stop the VTL server processes, we recommend that you reboot the machine before restarting the processes.

---

## Start the VTL server

Execute the following commands to start the VTL server processes.

```
cd /usr/local/vtl/bin
vtl start
```

When you start the server, you will see the processes start. It will look similar to the following, depending upon which VTL options you are using:

Starting VTL Configuration Module	[OK]
Starting VTL Base Module	[OK]
Starting VTL HBA Module	[OK]
Starting VTL SNMPD Module	[ OK ]
Starting VTL Authentication Module	[ OK ]
Starting VTL Server (Compression) Module	[ OK ]
Starting VTL Server (HiFn HW Compression) Module	[ OK ]
Starting VTL Server (FSNBase) Module	[ OK ]
Starting VTL Server (Upcall) Module	[ OK ]
Starting VTL Server (Transport)	[ OK ]
Starting VTL Server (Event) Module	[ OK ]
Starting VTL Server (Path Manager) Module	[ OK ]
Starting VTL Server (Application)	[ OK ]
Starting VTL Server VTL Module	[ OK ]
Starting VTL Server VTL Upcall Module	[ OK ]
Starting VTL Server VTL Upcall Daemon	[ OK ]
Starting VTL Server VTL Upcall (32 bit) Daemon	[ OK ]
Starting VTL Target Module	[ OK ]
Starting VTL iSCSI Target Module	[ OK ]
Starting VTL iSCSI (Daemon)	[ OK ]
Loading VTL Resources	[ OK ]
Starting VTL Server IMA Daemon	[ OK ]
Starting VTL Server RDE Daemon	[ OK ]
Starting VTL Communication Module	[ OK ]
Starting VTL CLI Proxy Module	[ OK ]
Starting VTL Logger Module	[ OK ]
Starting VTL Self Monitor Module	[ OK ]

You will only see these processes if *iSCSI Target Mode* is enabled.

## Restart the VTL server

Execute the following commands to stop and then start the VTL server processes.

```
cd /usr/local/vtl/bin
vtl restart
```

---

## Check the VTL Server processes

Execute the following commands to check the VTL Server processes.

```
cd /usr/local/vtl/bin
vtl status
```

You should see something similar to the following, depending upon which VTL options you are using:

Status of VTL SNMPD Module	[RUNNING]
Status of VTL Configuration Module	[RUNNING]
Status of VTL Base Module	[RUNNING]
Status of VTL HBA Module	[RUNNING]
Status of VTL Authentication Module	[RUNNING]
Status of VTL Server (Compression) Module	[RUNNING]
Status of VTL Server (HiFn HW Compression) Module	[RUNNING]
Status of VTL Server (FSNBase) Module	[RUNNING]
Status of VTL Server (Upcall) Module	[RUNNING]
Status of VTL Server (Transport)	[RUNNING]
Status of VTL Server (Event) Module	[RUNNING]
Status of VTL Server (Path Manager) Module	[RUNNING]
Status of VTL Server (Application)	[RUNNING]
Status of VTL Server VTL Upcall Module	[RUNNING]
Status of VTL Server VTL Upcall Daemon	[RUNNING]
Status of VTL Server VTL Module	[RUNNING]
Status of VTL Target Module	[RUNNING]
Status of VTL iSCSI Target Module	[RUNNING]
Status of VTL iSCSI (Daemon)	[RUNNING]
Status of VTL Server IMA Daemon	[RUNNING]
Status of VTL Server RDE Daemon	[RUNNING]
Status of VTL Communication Module	[RUNNING]
Status of VTL CLI Proxy Module	[RUNNING]
Status of VTL Logger Module	[RUNNING]
Status of VTL Self Monitor Module	[RUNNING]

You will only see these processes if *iSCSI Target Mode* is enabled.

---

## Stop the VTL Server



*Warning: Stopping the VTL Server processes will detach all virtual devices. To prevent data loss, we recommend stopping all VTL client services prior to shutdown.*

If you are using the Hosted Backup option, you must make sure to stop the backup application before stopping VTL.

Execute the following commands to shut down the VTL Server processes:

```
cd /usr/local/vtl/bin  
vtl stop
```

You should see the processes stopped.

# Command Line

---

Virtual Tape Library (VTL) provides a simple utility that allows you to perform some of the more common VTL functions at a command line instead of through the VTL console. You can use this command line utility to automate many tasks, as well as integrate VTL with your existing management tools.

## 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	--vdev	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.

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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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: *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 seconds for the RPC timeout. 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>] | [-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-Celerra=<on|off>]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command allows you to add a client to the specified server. -c (--client-name) is a unique client name for the client to be created. The maximum length of the client name is 64. The following characters are invalid for a client name: <>"&\${\`

-I (--initiator-wwpns) is the option to set the initiator WWPNs. An initiator WWPN is a 16-byte Hex value. Separate initiator WWPNs with commas if more than one initiator WWPN is specified. For example:  
13af35d2f4ea6fbc,13af35d2f4ea6fad

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

-C (--enable-Celerra) is an option to support Celerra with the following values: *on* or *off* (default).

Enabling Celerra will automatically disable VSA, and vice versa.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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|*> | -t <adapter-no>] [-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|*> |
--adapter-no=<adapter-no>] [--lun=<lun>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command prepares and assigns 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Delete virtual device

```
iscon deletevdev -s <server-name> [-u <username> -p <password>]  
[-v <vdevid> ] | [-B <barcode> -l <library/standalone drive ID| 0 (Vault)>] [-d] [-f] [-X  
<rpc-timeout>]]
```

```
iscon deletevdev --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
[--vdevid=<vdevid>] | [--barcode=<barcode> --from-location-id=<library/standalone drive  
ID| 0 (Vault)>]  
[--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.

If you want to delete a virtual tape drive from a virtual tape library, the virtual tape drive must have the highest element number in the library. You can see the element number in the console when you highlight the *Drives* object for the library.

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.

To delete a virtual tape library, virtual tape drive, or standalone virtual tape drive, specify the -v (--vdevid). You can also use the -d (--delete-virtual-tapes) option.

To delete a virtual tape, specify either the -v (--vdevid) or the -B (--barcode) of the tape, as they are mutually exclusive. You can also specify the -l (--from-location-id) option.

-v (--vdevid) is an option to specify a device's virtual ID.

-B (--barcode) is an option to specify the barcode of the virtual tape. By default, the command queries all libraries, drives, and the vault. The barcode must be unique. If you have duplicate barcodes, use l (--from-location-id) to narrow the search. If the tape's -v (--vdevid) is provided, the barcode and location ID options are ignored.

-l (--from-location-id) is an option to specify the virtual ID of the library or standalone drive where the virtual tape is located when you use the -B (--barcode) option. If the tape is located in the vault, use 0 for the location ID.

-d (--delete-virtual-tapes) is an option to delete all of the existing virtual tapes from a virtual tape library, a loaded virtual tape drive, or a standalone virtual tape drive selected for deletion. If not specified, 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 default RPC timeout is 30 seconds.

---

## Get supported virtual libraries

```
iscon getsupportedvlibs -s <server-name> [-u <username> -p <password>]
[-l [-t <vlib-type>] [-c][ -M <output-delimiter>] ] [-X <rpc-timeout>]
```

```
iscon getsupportedvlibs --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--longlist [--vlib-type=<vlib-type>] [--compatible-drive-list]
[--output-delimiter=<output-delimiter>] ] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command retrieves information about all supported virtual tape libraries.

-l (--longlist) can be specified to get the supported library information in a long format. The default is to display the information in a list format.

-t (--vlib-type) is an option with the -l (--longlist) option to get the detail library information for a specific library. The format for the <vlib-type> is: <vendorID>:<productID>. For example, ADIC:Scalar 100

-c (--compatible-drive-list) is an option to display the compatible drives in a tabular format instead of the default long format.

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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>] [-f] [-k <key-name> -W <key-password>]  
[-X <rpc-timeout>]
```

```
iscon createvirtuallibrary --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--vlib-type=<vlib-type> [--vlib-name=<vlib-name>] --vdrive-type=<vdrive-type>  
[--vdrive-name-prefix=<vdrive-name-prefix>] [--num-of-drives=<num-of-drives>]  
[--auto-archive-mode=<auto-archive-mode> [--delay-delete-days=<days>]  
[--auto-eject-to-ie] | --auto-replication=<auto-repl-mode> --target-name=<target-name>  
[--delay-delete-time=<#[D|H|M]>] ] [--barcode-range=<barcode-range>]  
[--num-of-slots=<num-of-slots>] [--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>] [--force]  
[--key-name=<key-name> --key-password=<key-password>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a virtual tape library.

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

-n (--vlib-name) is optional. 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: “<vendorID>:<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-vendorID>-<drive-productID>-<vid>.

-R (--num-of-drives) is an option to create the specified number of drives (up to the maximum allowed by the library). By default, the library will be created with 1 drive. Use -f (--force) to override the default maximum value for the specified library in order to create up to 256 drives.

-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. The default value 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

-B (--barcode-range) 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.

The (--num-of-slots) can exceed the maximum number of slots supported by the specified library type, but it is limited to 64000.

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 set the maximum capacity of the virtual tapes (up to the maximum value allowed by the library). Use -f (--force) to override the default maximum value for the specified library in order to set the value up to 1800 GB.

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*.

-f (--force) is an option to override the maximum default values for the specified library and allow up to a maximum of 256 drives and 1800 GB of tape capacity.

-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 seconds for the RPC timeout. 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-vendorID>-<drive-productID>-<vid>.

---

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## Create standalone tape drive

```
iscon createstandalone drive -s <server-name> [-u <username> -p <password>]
-d <vdrive-type> [-r <vdrive-name-prefix>] [-R <num-of-drives>]
[-D -I <initial-size> -C <increment-size>] [-m <max-capacity>] [-X <rpc-timeout>]
```

```
iscon createstandalone drive --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdrive-type=<vdrive-type> [--vdrive-name-prefix=<vdrive-name-prefix>]
[--num-of-drives=<num-of-drives>] [--capacity-on-demand --initial-size=<initial-size>
--increment-size=<increment-size>] [--max-capacity=<max-capacity>]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a standalone virtual tape drive.

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

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

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

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

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

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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.

-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 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 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

---

## Move virtual tape

```
iscon movevirtualtape -s <server-name> [-u <username> -p <password>] -v <vdev>
[-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>] --vdev=<vdev>
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid> |
--slot-no=<slot-no>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command moves a virtual tape to a different location.

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

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

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

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

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

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

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

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

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

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

- Standalone Tape Drive -> Vault

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

**Note:** If you are moving virtual tapes from within a script, be sure to include the appropriate delays, as it can take several seconds to complete the move. During this time, the tape is still considered as being in its original slot.

---

## Tape copy

```
iscon tapecopy -s <server-name> [-u <username> -p <password>]  
-v <source-vdevvid> -S <target-name> [-U <target-username> -P <target-password>]  
[-L <tape-library-vid> | -D <tape-drive-vid>] [-n <vdevname>] [-f]  
[-X <rpc-timeout>]
```

```
iscon tapecopy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--source-vdevvid=<source-vdevvid> --target-name=<target-name>  
[--target-username=<target-username> --target-password=<target-password>]  
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid>]  
[--vdevname=<vdevname>] [--force] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command copies a tape.

-v (--source-vdevvid) is required to specify the ID of the virtual tape to be copied from.

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

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

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

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

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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-replication-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]
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command configures tape properties for the specified virtual tape. The virtual tape must be located in a virtual tape library slot. If the specified virtual tape is in the vault, only the write protect property can be configured.

-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 in the 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* (enable) or *off* (disable).

-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 the auto-archive option.
- "inherited" can only be specified when the parent library is enabled with the auto-archive option.

-Y (--delay-delete-days) is an option for auto-archive *move* mode to specify up to 365 days to wait before the deletion. The default value is 365 days.

-J (--auto-eject-to-ie) is an option for auto-archive mode to eject the physical tape to the IE slot after a successful archive job: *on* (enable) or *off* (disable).

-N (--auto-replication) is an option in one of the following values: *localcopy*, *localmove*, *remotecopy*, *remotemove*, or *none*.

-S (--target-name) is the remote server name for auto-replication. It is required for auto-replication.

-U (--target-username) and -P (--target-password) are options to specify a different user ID and password to log in to the remote server.

---

-M (--delay-delete-time) is an option for auto-replication move mode to specify up to 30 days to wait 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 physical tape. Specify -d (--disable-key) if you wish to disable tape encryption for this tape.

At least one of the above properties has to be specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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>]] | [-h]
[-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>]] | [--local]
[--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 tape 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 where the tape replica will be created and replicated to.

-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.

-h (--local) is an option to create a local replica. Target server information and credentials are not required when using this option and are ignored if they are specified.

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 in order 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).

For virtual tapes with tape caching enabled, replication is triggered based on the tape caching policy:

-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 for remote replication only to enable or disable compression with one of the values: *on* or *off*.

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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.

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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.

Either the primary server with the source virtual tape or the target server with the tape replica can be specified to remove the replication configuration, but not both.

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 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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-vdev) is the ID of the source virtual tape on the primary server to be resumed.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

## Set replication properties

```
iscon setreplicationproperties -s <server-name> [-u <username> -p <password>]
-v <source-vdev> [-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-vdev=<source-vdev> [--watermark=<watermark(MB)>
[--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-vdev) 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, the 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 to enable or disable encryption with one of the values: *on* or *off*.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

## ***Start replication***

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

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

### **Description:**

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

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

---

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

## ***Stop replication***

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

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

### **Description:**

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

## ***Promote replica in test mode***

```
iscon testmodepromotereplica -S <replica-server-name> -V <replicaid>
[-U <replica-server-username> -P <replica-server-password>]
[-u <primary-server-username> -p <primary-server-password>] [-X <rpc-timeout>]
```

```
iscon testmodepromotereplica
--target-name=<replica-server-name> --replicaid=<replicaid>
[--target-username=<replica-server-username>
--target-password=<replica-server-password>]
[--server-username=<primary-server-username>
--server-password=<primary-server-password>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command promotes a tape replica in test mode and suspends the replication property for its virtual tape source.

Both, tape replica and its virtual tape source must be valid and available. The information identifying the virtual source tape is automatically retrieved from the tape replica properties. If not already logged in, the user name and password must be specified for both replica and source servers.

-V (--replicaid) is the ID of the tape replica.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

---

## ***Demote replica in test mode***

```
iscon testmodedemotetape -S <testmode-server-name> -V <testmode-tape-id>
[-U <testmode-server-username> -P <testmode-server-password>]
[-u <primary-server-username> -p <primary-server-password>] [-X <rpc-timeout>]
```

```
iscon testmodedemotetape --target-name=<testmode-server-name>
--testmode-tape-id=<testmode-tape-id> [--target-username=<testmode-server-username> --
target-password=<testmode-server-password> [--server-username=<primary-server-username>
--server-password=<primary-server-password>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command demotes a test mode virtual tape to a replica and resumes the replication property for its virtual tape source. The test mode virtual tape must be in the virtual vault.

Both the test mode virtual tape and its source virtual tape must be valid and available. The information identifying the source virtual tape is automatically retrieved from the test mode virtual tape properties. If not already logged in, the user name and password must be specified for both servers holding the virtual tapes.

-V (--testmode-tape-id) is the test mode virtual tape ID.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

---

## Physical devices

### *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:**

This command displays a list of allocated physical devices.

-F (--config) is an option to get the physical device configuration information. The default is to exclude the system device information.

-M (--include-system-info) is an option to include the system device information.

-C (--category) is an option to be used as a filter to get the configuration information for the specified category with one of the values: *virtual* (default) or *service-enabled* or *direct*.

The -M (--include-system-info) and -C (--category) options are mutually exclusive.

-o (--output-format) is the option to specify the output format. The <output-format> for the -F (--config) option is one of the following values: *list* or *detail* or *guid* or *scsi*.

-a (--allocated-list) is an option to get the allocated physical device information.

-A (--available-list) is an option to get the available physical device information.

-I (--scsiaddress) is an option to specify the SCSI address as a device filter in the following format:  
<ACSL>=#:#:# (adapter:channel:id:lun)

The <output-format> for the -a (--allocated-list) and the -A (--available-list) options is one of the following values: *list* or *detail* or *size-only*.

-F (--config), and -a (--allocated-list) and/or -A (--available-list) are mutually exclusive. You can either get the configuration information or get the allocation information. When getting the allocation information, you can specify either -a (--allocated-list), or -A (--available-list) or both. The default is to display both the device allocation and availability information if none of the options is specified.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 the adapters if it is not specified. For example, e.g. -a 5 or -a 5-10

-i (--scsi-range) is the starting SCSI ID and ending SCSI ID to be rescanned. The default is to rescan all the SCSI IDs if the range is not specified. For example, e.g. -i 0-5

-l (--lun-range) is the starting LUN and ending LUN to be rescanned. The default is not to rescan any LUN if it is not specified. For example, e.g. -l 0-10

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. 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 imports a physical disk.

<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 for the disk to be imported.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Prepare disk

```
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>]  
--scsiaddress=<ACSL> | --guid=<guid> --category=<category> [--new-guid=<new-guid>]  
[--rpc-timeout=<rpc-timeout>]
```

### Description:

This command prepares a physical disk.

<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 for the disk to be prepared.

`-C` (`--category`) is required to specify the new category for the physical device with one of the following values: *unassigned*, *virtual*, *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".

`-X` (`--rpc-timeout`) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## Show storage allocation

```
iscon showstorageallocation -s <server-name> [-u <username> -p <password>]  
[-o <csv|list>] [-X <rpc-timeout>]
```

```
iscon showstorageallocation --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
[--output-format=<csv|list>][--rpc-timeout=<rpc-timeout>]
```

### Description:

This command displays information about how your storage is allocated.

`-o` (`--output-format`) is an option to choose one of the following formats for the output: *csv* (default) or *list*.

`-X` (`--rpc-timeout`) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 30 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 the output filename is not specified, the default filename is: eventlogYYYY-MM-DD-hh-mm-<servername>[.#]

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

-f (--force) is an option 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 seconds for the RPC timeout. The default RPC timeout is 30 seconds.

---

## Reports

### *Server throughput report*

```
iscon createserverthroughputreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-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>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: ServerThroughput-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>]
[-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>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: SCSIChannelThroughput-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***SCSI device throughput report***

```
iscon createdevicethroughputreport -s <server-name> [-u <username> -p <password>]
-I <ACSL> [-z <report period>] | [-D <date-range>] [-o <filename>]
[-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>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: SCSIDeviceThroughput-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>] [-X <rpc-timeout>]
```

```
iscon createphyresourcesconfreport --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]  
[--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [.#] will be appended to the report name. If the output file name is not specified, the default file name is: PhysicalResourcesConfiguration-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>]  
[-X <rpc-timeout>]
```

```
iscon creatediskusagereport --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]  
[--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [.#] will be appended to the report name. If the output file name is not specified, the default file name is: DiskSpaceUsage-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>] [-X <rpc-timeout>]
```

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

### **Description:**

This command creates a report that displays the physical resource allocation for a specific server.

-o (--output-file) is an option to specify an output file name for the report. If a report with the same name already exists, a suffix [.#] will be appended to the report name. If the output file name is not specified, the default file name is: PhysicalResourcesAllocation-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>] [-X <rpc-timeout>]
```

```
iscon createphyresourceallocreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--scsiaddress=<ACSL>]
[--output-file=<filename>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: PhysicalResourceAllocation-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>]
[-X <rpc-timeout>]
```

```
iscon createfcaconfreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]
[--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: FCAdaptersConfig-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>]
[-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>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: ReplicationStatus-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>] [-X <rpc-timeout>]
```

```
iscon createvirlibinfo report --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]
[--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: VirtualLibraryInfo-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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>] [-i] [-X <rpc-timeout>]
```

```
iscon createvirtapeinfo report --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]
[--include-filter] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: VirtualTapeInfo-server-MM-DD-YYYY-hh-mm-ss

-i (--include-filter) is an optional filter to include only the virtual tapes with selected properties. This option can be any combination of one of the following values from each filter groups, separated by comma:

Barcode group:

- BARCODEPREFIX=barcodePrefix,
- BARCODECONTAINS=pattern,
- BARCODERANGE=barcodeStart-barcodeEnd,

Location group:

- LOCATION=virtualLibraryID, for Vault use LOCATION=Vault,
- LIBNAMEPREFIX=virtualLibraryNamePrefix.

e.g.: -i LOCATION=Vault,BARCODERANGE=0000000A-0000000H

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## ***LUN report***

```
iscon createlunreport -s <server-name> [-u <username> -p <password>]  
[-I <ACSL>] [-o <filename>] [-X <rpc-timeout>]
```

```
iscon createlunreport --server-name=<server-name>  
[--server-username=<username> --server-password=<password>] [--scsiaddress=<ACSL>]  
[--output-file=<filename>] [--rpc-timeout=<rpc-timeout>]
```

### **Description:**

This command creates a report that displays information about the resources allocated per LUN.

-I <ACSL> (--scsiaddress) is an option to specify a single LUN address to be reported.

-o (--output-file) is an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: lun-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Job report

```
iscon createjobreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-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>] [--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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: JobReport-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## Disk space usage history report

```
iscon creatediskspaceusagehistoryreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-X <rpc-timeout>]
```

```
iscon creatediskspaceusagehistoryreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--output-file=<filename>] [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command creates a report that displays information about the peak amount of total disk space available and being used for up to 30 days.

-z (--report-period) is the period of choice. 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 an option to specify an output file name for the report. If a report with the same name already exists, a suffix [#] will be appended to the report name. If the output file name is not specified, the default file name is: DiskSpaceUsageHistory-server-MM-DD-YYYY-hh-mm-ss

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 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 of the log messages
- YYMMDDhhmm-YYMMDDhhmm = log messages in date/time range

The default is to get all of 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

-f (--force) is an option 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 seconds for the RPC timeout. 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 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Deduplication

### *Start deduplication policy*

```
iscon dedupstartpolicy -s <server-name> [-u <username> -p <password>]  
-I <"policyname"> [-X <rpc-timeout>]
```

```
iscon dedupstartpolicy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--policyname=<"policyname"> [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command starts the execution of the specified policy.

-I (--policyname) is required to specify the policy name. Enclose the policy name in double quotes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

### *Stop deduplication policy*

```
iscon dedupstoppolicy -s <server-name> [-u <username> -p <password>]  
-I <"policyname"> [-X <rpc-timeout>]
```

```
iscon dedupstoppolicy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--policyname=<"policyname">] [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command stops the execution of the specified policy.

-I (--policyname) is required to specify the policy name. Enclose the policy name in double quotes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

### *Add tape to deduplication policy*

```
iscon dedupaddtapetopolicy -s <server-name> [-u <username> -p <password>]  
-T <tapevidlist> -I <"policyname"> [-X <rpc-timeout>]
```

```
iscon dedupaddtapetopolicy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--tape-vid-list=<tapevidlist> --policyname=<"policyname"> [--rpc-timeout=<rpc-timeout>]
```

#### **Description:**

This command adds virtual tapes to an existing policy.

-T (--tape-vid-list) is required to specify the ID of the virtual tapes to be added to the policy as a list of numbers separated by commas.

-I (--policyname) is required to specify an existing name. Enclose the policy name in double quotes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

---

## Remove tape from deduplication policy

```
iscon dedupremovetapefrompolicy -s <server-name> [-u <username> -p <password>]  
-T <tapevidlist> -I <"policyname"> [-X <rpc-timeout>]
```

```
iscon dedupremovetapefrompolicy --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
--tape-vid-list=<tapevidlist> --policyname=<"policyname"> [--rpc-timeout=<rpc-timeout>]
```

### Description:

This command removes virtual tapes from an existing policy.

-T (--tape-vid-list) is required to specify the ID of the virtual tapes to be removed from the policy as a list of numbers separated by commas.

-I (--policyname) is required to specify the policy name. Enclose the policy name in double quotes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

## Get deduplication tape activity

```
iscon deduptapeactivityinfo -s <server-name> [-u <username> -p <password>]  
[-I <"policynamelist">] [-T <tapevidlist>] [-S <job-status>] [-D <date-range>]  
[-w <hh:mm-hh:mm>] [-x] [-d] [-l] [-M <delim>] [-X <rpc-timeout>]
```

```
iscon deduptapeactivityinfo --server-name=<server-name>  
[--server-username=<username> --server-password=<password>]  
[--policyname=<"policyname">] [--tape-vid-list=<tapevidlist>]  
[--job-status=<OK | FAILED>] [-date-range<YYYYMMDD-YYYYMMDD | YYYYMMDD>]  
[--backup-window=<hh:mm-hh:mm>] [--last-run] [--skip-delete][--longlist]  
[--output-delimiter=<delim>][--rpc-timeout=<rpc-timeout>]
```

### Description:

This command reports the deduplication history for tapes on the specified server. The optional arguments can be combined in order to perform advanced queries. The default relationship for any optional argument combination is "and".

-I (--policyname) is an option to report the activity of the specified policy only. Multiple names must be separated by commas and the whole argument must be enclosed in double quotes: e.g. "Policy 1,Policy 2,Policy 3".

-T (--tape-vid-list) is an option to report the activity of the specified virtual tapes only. The format for this argument must be a list of numbers separated by commas.

-S (job-status) is an option to report the activity based on the job status. The accepted values for this argument are: *OK*, *FAILED*, *CANCELED*, or *NEW*.

-D (--date-range) is an option to report the activity for the specified date range. The format for this argument must be: *YYYYMMDD-YYYYMMDD* or *YYYYMMDD* for a single day.

-w (--backup-window) is an option to report the activity for the specified time interval only.

-x (--last-run) is an option to report the last execution for each tape per policy.

-d (--skip-deleted) is an option to filter out the records for the tapes that were deleted or moved from policies.

---

-l (--longlist) is an option to display the detailed report in the format "Label=Value".

-M (--out-delimiter) is an option to display the detailed report using the specified string as the field delimiter. The delimiter can be up to 8 characters long.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 300 seconds.

# Appendix

This appendix contains information about system security and LUN migration.

## 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
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)*
UDP port 6666	Areca Raid Controller #1 (Appliances with built in storage)
TCP port 6666	Areca Raid Controller #1 (Appliances with built in storage)

Port	Purpose
UDP port 6667	Areca Raid Controller #2 (Appliances with built in storage)
TCP port 6667	Areca Raid Controller #2 (Appliances with built in storage)
UDP port 6668	Areca Raid Controller #3 (Appliances with built in storage)
TCP port 6668	Areca Raid Controller #3 (Appliances with built in storage)
TCP 11576	SAN Client
TCP 11582	SAN Client
TCP 11762	SAN Client

\* 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.

## LUN migration

VTL offers a command line tool to migrate data on a LUN to one or more other LUNs. With this tool, you can specify the target LUN(s) or let the system auto-select the target LUN(s). With its built-in restart capability, incomplete/failed migration jobs can be restarted from where they left off.

After the data is moved to the target LUN, the source LUN will be unassigned.

**Requirements** The following requirements must be met before running a LUN migration job:

- The source LUN must have data on it. You cannot migrate an empty LUN. You will get an error if you try and the job will fail.
- You need to move all of the tapes on the LUN to be migrated to the virtual vault before you run a migration job or your job will fail.
- The target LUN must have enough space or you will get an error and the job will fail. Because data is copied over sector by sector, you must have enough space for each sector on the target LUN. For example, the source LUN is 10 GB and there are two target LUNs that are 5 GB each. Even though the total of the two target LUNs is 10 GB, the job will fail if the first sector on the source LUN is 6 GB (since each target LUN is only 5 GB and neither is large enough to accept the 10 GB segment).
- Database LUNs (LUNs with VTL database segments on it) can be selected as the source but the database segment will not be moved. Database LUNs cannot be selected as the target. You will get an error if you try and the job will fail. If you run automatic migration when there are only DB LUNs, you will get a *createmigratedummytape fail* error and the job will fail.

- 
- **It is very important** that there is no I/O occurring on the source or target LUN while LUN migration is in progress.

**Manual migration** Manual migration lets you specify the target LUN(s). To run a manual migration job, go to \$ISHOME/bin and run the following command.

```
lunmigration.sh <source LUN ACSL> <target LUN ACSL>
```

The format for specifying the ACSL is a:c:s:l

For multiple target LUNs, you must separate each target LUN with a comma:

```
lunmigration.sh <source LUN ACSL> <target LUN ACSL 1>, ..., <target LUN ACSL n>
```

**For example:** `lunmigration.sh 1:0:0:6 1:0:0:7,1:0:0:8`

**Automatic migration** Automatic migration lets the system auto-select the target LUN(s). To run an automatic migration job, go to \$ISHOME/bin and run:

```
lunmigration.sh <source LUN ACSL> AUTO
```

AUTO must be in uppercase.

**For example:** `lunmigration.sh 1:0:0:6 AUTO`

**Restart a job** To restart an incomplete/failed migration job from where it left off, run the following before re-running the migration job:

```
lmclean.sh
```

---

## SNMP Messages

VTL provides Simple Network Management Protocol (SNMP) support to integrate VTL management into an existing enterprise management solution. By default, event log messages are not be sent, but you may want to configure VTL to send certain types of messages. The four classificaion of messages are:

- **Critical Messages** - Only critical errors that stop the system from operating properly will be sent.
- **Error Messages** - Errors (failure such as a resource is not available or an operation has failed) and also critical errors will be sent.
- **Warning Messages** - Warnings (something occurred that may require maintenance or corrective action) and also errors and critical errors will be sent.
- **Information Messages** - Informational messages and also errors, warnings, and critical error messages will be sent.

All of the available log messages that can be generated and correspondingly configured to be sent to the SNMP trap manager are listed here.

### Critical Messages

13800	Primary server %1 failure detected. Failure condition: %2
13817	Primary server failback was unsuccessful. Failed to update the primary configuration.
13863	Primary server is commanded to resume. %1 ID %4 LUN %5.
13864	Primary server operation will terminate. %1
13879	Secondary server detect kernel module failure reboot machine may need.
14017	Failed to save the configuration to configuration repository. Please check the storage connectivity.

---

## Error Messages

- 1000 Socket connection could not be terminated properly --%1.
- 1001 Socket connection could not be terminated properly due to error during shutdown --%1.
- 1002 Unexpected interrupt occurred.
- 1005 Out of kernel resources. Failed to get major number for IPStor SCSI device.
- 1006 Failed to allocate memory.
- 1007 Failed to set up the network connection due to an error in SANRPC\_Init --%1.
- 1008 Failed to set up the network connection due to an error in SANRPCListen --%1.
- 1011 Error while writing --write(%1) result = 0x%2 cmd = 0x%3.
- 1012 Error while reading --read(%1) result = 0x%2 cmd = 0x%3.
- 1023 Failed to connect to physical device %1. Switching alias to %2.
- 1030 Failed to start replication --replication is already in progress for virtual tape %1.
- 1031 Failed to start replication --replication control area not present on virtual tape %1.
- 1032 Failed to start replication --replication control area has failed for virtual tape %1.
- 1033 Failed to start replication --a snapshot is in progress for virtual device %1.
- 1034 Replication failed for virtual device %1 --the network transport returned error %2.
- 1035 Replication failed for virtual device %1 --the local disk failed with error %2.
- 1036 Replication failed for virtual device %1 --the local snapshot used up all of the reserved area.
- 1037 Replication failed for virtual device %1 --the replica snapshot used up all of the reserved area.
- 1038 Replication failed for virtual device %1 --the local server could not allocate memory.
- 1039 Replication failed for virtual device %1 --the replica failed with error %2.
- 1040 Replication failed for virtual device %1 --failed to set the replication time.
- 1043 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 A SCSI command terminated with a non-recoverable hardware failure (for example controller failure)
- 1046 Rescan replica has failed for virtual device %1 --the local device failed with error %2.
- 1047 Rescan replica has failed for virtual device %1 --the replica device failed with error %2.
- 1048 Rescan replica has failed for virtual device %1 --the network transport returned error %2.
- 1049 Rescan replica cannot proceed --replication control area not present on virtual device %1
- 1050 Rescan replica cannot proceed --replication control area has failed for virtual device %1
- 1051 Rescan replica cannot proceed --a merge is in progress for virtual device %1
- 1052 Rescan replica failed for virtual device %1 --replica status returned %2
- 1053 Rescan replica cannot proceed --replication is already in progress for virtual device %1

- 
- 1054 Replication cannot proceed --a merge is in progress for virtual device %1
- 1055 Replication failed for virtual tape %1 --replica status returned %2
- 1056 Replication control area exchange failed for virtual tape %1 --the error code is %2
- 1059 Replication failed for virtual tape %1 --start replication returned %2
- 1060 Rescan replica failed for virtual device %1 --start scan returned %2
- 1066 Replication cannot proceed --snapshot resource area does not exist for remote virtual device %1.
- 1067 Replication cannot proceed --unable to connect to replica server %1. device failure parity error etc.). Please check the system log for additional information.
- 1068 Replication cannot proceed --group %1 is corrupt.
- 1069 Replication cannot proceed --virtual tape %1 no longer has a replica or the virtual tape replica does not exist.
- 1070 Replication cannot proceed --replication is already in progress for group %1.
- 1071 Replication cannot proceed --virtual tape %1 no longer has a replica or the virtual tape replica does not exist.
- 
- 1072 Replication cannot proceed --missing a remote replica device in group %1.
- 1073 Replication cannot proceed --unable to open configuration file.
- 1074 Replication cannot proceed --unable to allocate memory.
- 1075 Replication cannot proceed --unexpected error %1.
- 1078 Replication cannot proceed --mismatch between our snapshot group %1 and replica server.
- 1079 Replication for group %1 has failed due to error on virtual device %2
- 1080 Replication cannot proceed --failed to create timemark on virtual device %1
- 1081 Replication cannot proceed --failed to create common timemark for group %1
- 1084 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 HotZone for virtual device %1 has been auto-disabled due to an error.
- 1086 Replication cannot proceed --failed to load the virtual tape %1.
- 1087 Replication cannot proceed --virtual tape %1 is in the drive.
- 1088 Replication cannot proceed --failed to set initialization status in Virtual Library System for virtual tape %1.
- 1099 Replication cannot proceed --virtual tape replica %1 ( virtual tape %2 ) cannot be expanded/shrunk; The allowed capacity on the target server is exceeded.
- 
- 1203 Path failed to trespass to %1.
- 1204 Failed to add path group. ACSL: %1.
- 1206 Failed to activate path: %1.
- 1207 Critical path failure detected. Path %1 will be removed.

- 
- 1214 Failed to add path: %1.
  - 7001 Patch %1 failed --environment profile is missing in /etc.
  - 7002 Patch %1 failed --it applies only to build %2.
  - 7003 Patch %1 failed --you must be the root user to apply the patch.
  - 7005 Patch %1 installation failed --prerequisite patch %2 has not been applied.
  - 7006 Patch %1 installation failed --cannot copy new binaries.
  - 7009 Patch %1 rollback failed --cannot copy back previous binaries.
  - 7010 Patch %1 failed --the file %2 has the patch level %3 higher than this patch. You must rollback first %4.
  - 7011 Patch %1 failed --it applies only to kernel %2.
  - 7012 Patch %1 failed --The available free space is %2 bytes; you need at least %3 bytes to apply the patch.
  - 10001 Insufficient privilege (uid: %1).
  - 10002 IPStor Server environment is corrupt.
  - 10003 Failed to initialize configuration %1.
  - 10004 Failed to get SCSI device information.
  - 10005 A physical device will not be available because we cannot create a Global Unique Identifier for it.
  - 10006 Failed to write configuration %1.
  - 10054 IPStor Server FSID update error.
  - 10059 Server Persistent Binding update error.
  - 10100 Failed to scan new SCSI devices.
  - 10101 Failed to update configuration %1.
  - 10102 Failed to add new SCSI devices.
  - 10204 Failed to parse configuration %1.
  - 10207 Add Adapter %1 failed not enough memory.
  - 10209 Add Physical Device %1 failed not enough memory.
  - 10240 Missing SCSI Alias %1.
  - 10241 Physical Adapter %1 could not be located in /proc/scsi/.
  - 10242 Duplicate Physical Adapter number %1 in /proc/scsi/.
  
  - 10243 Physical Device data structure is null.
  - 10244 Invalid FSID device %1 -the LUN byte (4th byte) in FSID %2 does not match actual LUN.
  - 10245 Invalid FSID Generate FSID %1 does not match device acsl:%2 GUID %3.
  - 10246 Fail to generate FSID for device acsl:%1 can't validate FSID.
  - 10247 Device (acsl:%1) GUID is blank can't validate FSID.
  - 10496 Failed to attach tle repository.

- 
- 11000 Failed to create socket.
  - 11001 Failed to set socket to re-use address.
  - 11002 Failed to bind socket to port %1.
  - 11003 Failed to create TCP service.
  - 11004 Failed to register TCP service (program: %1 version: %2).
  - 11006 IPStor communication module failed to start.
  - 11030 Auto save configuration: cannot setup crontab.
  - 11031 Auto save configuration: cannot create the running script %1.
  - 11032 Auto save configuration: cannot connect to FTP server %1 port %2.
  - 11033 Auto save configuration: cannot login user %1.
  - 11034 Auto save configuration: directory %1 does not exist.
  - 11035 Auto save configuration: failed to copy %1 to FTP server.
  - 11036 Auto save configuration: failed to delete old file %1 from FTP server.
  - 11101 SAN Client (%1): Failed to add SAN Client.
  - 11103 SAN Client (%1): Authentication failed.
  - 11104 There are too many SAN Client connections.
  - 11106 SAN Client (%1): Failed to log in.
  - 11107 SAN Client (%1): Illegal access.
  - 11109 SAN Client (%1): Failed to open file %2.
  - 11110 SAN Client (%1): Failed to get hostname.
  - 11111 SAN Client (%1): Failed to resolve hostname %2.
  - 11112 SAN Client (%1): Failed to parse configuration file %2.
  - 11113 SAN Client (%1): Failed to restart authentication module.
  - 11114 SAN Client (%1): Failed to allocate memory.
  - 11115 SAN Client (%1): License conflict --Number of CPUs approved: %2 number of CPUs used: %3.
  - 11170 Failed to virtualize LUN %1 because of mismatching size between configuration file and disk. Please do a rescan and try it again.
  - 11200 Buffer overflow.
  - 11201 There are too many Console connections.
  - 11202 Console (%1): Illegal access.
  - 11203 Console (%1): SCSI device re-scanning has failed.
  - 11204 Console (%1): SCSI device checking has failed.
  - 11205 Console (%1): Failed to get information for file %2.
  - 11206 Console (%1): Failed to allocate memory.
  - 11207 Console (%1): Failed to open file %2.
  - 11208 Console (%1): Failed to read file %2.
  - 11209 Console (%1): Insufficient privilege access.

- 
- 11211 Console (%1): Failed to save file %2.
  - 11212 Console (%1): Failed to create index file %2 for Event Log.
  - 11213 Console (%1): Illegal time range (%2 -%3) for Event Log.
  - 11214 Console (%1): Failed to get Event Log (%2 -%3).
  - 11215 Console (%1): Failed to open directory %2.
  - 11216 Console (%1): Out of system resources. Failed to fork process. pdev sect %3 from %4 to %5.
  - 11217 Console (%1): Failed to execute program %2. s:%3 l:%4 from %5 to %6.
  
  - 11218 Console (%1): Failed to remove file %2.
  - 11219 Console (%1): Failed to add device %2.
  - 11220 Console (%1): Failed to remove device %2.
  - 11221 Console (%1): Failed to add SAN Client (%2) to virtual device %3.
  - 11222 Console (%1): Failed to remove SAN Client (%2) from virtual device %3.
  - 11231 Console (%1): Failed to get CPU status.
  - 11232 Console (%1): Failed to get memory status.
  - 11233 Console (%1): Failed to map the SCSI device name for [%2 %3 %4 %5].
  - 11234 Console (%1): Failed to execute "hdparm" for %2.
  - 11235 Console (%1): Failed to get the IPStor Server module status.
  - 11236 Console (%1): Failed to get the version information for the message file.
  - 11237 Console (%1): Failed to get file %2.
  - 11238 Console (%1): Failed to restart the authentication module.
  - 11240 Console (%1): Failed to start the IPStor Server module.
  - 11242 Console (%1): Failed to stop the IPStor Server module.
  - 11244 Console (%1): Failed to access the IPStor administrator list.
  - 11245 Console (%1): Failed to add user %2.
  - 11247 Console (%1): Failed to delete user %2.
  - 11249 Console (%1): Failed to reset password for user %2.
  - 11251 Console (%1): Failed to update password for user %2.
  - 11253 Console (%1): Failed to modify virtual device %2.
  - 11255 Console (%1): Failed to modify virtual device %3 for SAN Client (%2).
  - 11257 Console (%1): Failed to add SAN Client (%2).
  - 11259 Console (%1): Failed to delete SAN Client (%2).
  - 11261 Console (%1): Failed to get SAN Client connection status for virtual device %2.
  - 11262 Console (%1): Failed to parse configuration file %2.
  - 11263 Console (%1): Failed to restore configuration file %2.
  - 11265 Console (%1): Failed to restart IOCore module.

- 
- 11266 Console (%1): Failed to erase partition of virtual device %2.
- 11268 Console (%1): Failed to update meta information of virtual device %2.
- 11269 Console (%1): Failed to get ID for SAN Client (%2).
- 11270 Console (%1): Failed to add mirror for virtual device %2.
- 11272 Console (%1): Failed to remove mirror for virtual device %2.
- 11274 Console (%1): Failed to stop mirroring for virtual device %2.
- 11276 Console (%1): Failed to start mirror synchronization for virtual device %2.
- 11278 Console (%1): Failed to swap mirror for virtual device %2.
- 11280 Console (%1): Failed to create shared secret for IPStor Server %2.
- 11282 Console (%1): Failed to change device category for physical device %2 to %3.
- 11284 Console (%1): Failed to get raw device name for physical device %2.
- 11285 Console (%1): Failed to execute failover command (%2).
- 11287 Console (%1): Failed to set failover mode (%2).
- 11289 Console (%1): Failed to restart IPStor Server module.
- 11291 Console (%1): Failed to update meta information of physical device %2.
- 11292 Console (%1): Failed to swap IP address from %2 to %3.
- 11294 Console (%1): Failed to get host name.
- 11295 Console (%1): Invalid configuration format.
- 11296 Console (%1): Failed to resolve host name --%2.
- 11298 Console (%1): Failed to reset cache on target device %2 (ID: %3) for %4 copy.
- 11306 The IPStor Administrator group does not exist.
- 11307 User %1 at IP address %2 is not a member of the IPStor Administrator's group.
- 11308 The IPStor Client group does not exist.
- 11309 User ID %1 at IP address %2 is invalid.
- 
- 11310 IPStor Client User name %1 does not match with the client name %2.
- 11311 Client agent %1 failed to request license.
- 11313 Client agent %1 failed to release license.
- 11315 You have no license for %1 protocol.
- 11316 You have exceeded the storage capacity allowed by your license used space=%1MB
- 11400 Failed to communicate with the Self-Monitor module.
- 11401 Failed to release IP address %1.
- 11402 Failed to read %1.
- 11403 Failed to retrieve authentication information.
- 11404 Failed to merge authentication information.
- 11405 Failed to obtain IP address %1.
- 11406 Failed to prepare the failover configuration package --%1.

- 
- 11407 Failed to extract the failover configuration package --%1.
  - 11500 Failed to expand virtual tape %1: not enough disk space.
  - 11501 Failed to expand virtual tape %1: maximum segment exceeded (error code %2).
  - 11502 Failed to expand virtual tape %1 (segment allocation error code %2).
  - 11504 Failed to expand virtual tape id %1 by %2 MBytes.
  - 11505 Failed to change virtual tape %1 to direct link mode.
  - 11507 Console (%1): Failed to create X-Ray file.
  - 11508 Console (%1): Failed to set the properties for the IPStor Server.
  - 11510 Console (%1): Failed to save report --%2.
  - 11511 Console (%1): Failed to get the information for the NIC.
  - 11512 Console (%1): Failed to add a replica for virtual tape %2 to IPStor Server %3 (watermark: %4 MB time: %5
  - 11514 Console (%1): Failed to remove the replica for virtual tape %2 from IPStor Server %3 (watermark: %4 MB time: %5
  - 11516 Console (%1): Failed to create the virtual tape replica %2.
  - 11518 Console (%1): Failed to start replication for virtual tape %2.
  - 11520 Console (%1): Failed to stop replication for virtual tape %2.
  - 11522 Console (%1): Failed to promote virtual tape replica %2 to a virtual tape.
  - 11524 Console (%1): Failed to run IPStor Server X-Ray.
  - 11526 Console (%1): Failed to add Copy Manager %2.
  - 11528 Console (%1): Failed to remove Copy Manager %2.
  - 11530 Console (%1): Failed to back up configuration files.
  - 11532 Console (%1): Failed to restore configuration files.
  - 11534 Console (%1): Failed to reset the umap for virtual device %2.
  - 11535 Console (%1): Failed to update the replication parameters for virtual tape %2 to IPStor Server %3 (watermark: %4 MB time: %5
  - 11537 Console (%1): Failed to claim physical device %2.
  - 11539 Console (%1): Failed to import physical device %2.
  - 11540 Console (%1): Host name mismatch (old: %2 new: %3).
  - 11541 Console (%1): Failed to save event message (ID: %2).
  - 11542 Console (%1): Failed to remove virtual tape replica %2.
  - 11544 Console (%1): Failed to modify virtual tape replica %2.
  - 11546 Console (%1): Failed to mark the replication for virtual tape %2.
  - 11548 Console (%1): Failed to determine if data was written to virtual device %2.
  - 11549 Console (%1): Failed to set option "%2 %3."
  - 11551 Console (%1): Failed to set Snapshot option %3 for virtual device %2.
  - 11553 Console (%1): Failed to get login user list.
  - 11554 Console (%1): Failed to set failover option <selfCheckInterval: %d sec>.

- 
- 11556 Console (%1): Failed to start initializing snapshot copy from virtual device %2 to virtual device %3.
- 11558 Console (%1): Failed to stop initializing snapshot copy from virtual device %2 to virtual device %3.
- 11560 Console (%1): Failed to get licenses.
- 11561 Console (%1): Failed to add license %2.
- 11563 Console (%1): Failed to remove license %2.
- 11565 Console (%1): Failed to check licenses --option mask %2.
- 11566 Console (%1): License conflict --Number of CPU's available: %2 number of CPU's used: %3.
- 11567 Console (%1): Failed to clean up failover server directory %2.
- 11568 Console (%1): Failed to set (%2) I/O Core for failover --Failed to create failover configuration.
- 11569 Console (%1): Failed to set %2 to Fibre Channel mode %3.
- 11571 Console (%1): Failed to assign Fibre Channel device %2 to %3 (rolled back).
- 11572 Console (%1): Failed to assign Fibre Channel device %2 to %3 (not rolled back).
- 11574 Console (%1): Failed to unassign Fibre Channel device %2 from %3 (rolled back) and returns %4.
- 11575 Console (%1): Failed to unassign Fibre Channel device %2 from %3 (not rolled back) and returns %4.
- 11577 Console (%1): Failed to get Fibre Channel target information.
- 11578 Console (%1): Failed to get Fibre Channel initiator information.
- 11579 Console (%1): Failed to set %2 to Fibre Channel authentication mode %3.
- 11581 Console (%1): Failed to set NAS option %2.
- 11585 Console (%1): Failed to set Fibre Channel option %2.
- 11587 Console (%1): Failed to demote virtual device %2 to a replica.
- 11589 Authentication failed to connect to client %1 and returned %2.
- 11590 Out of disk space to expand snapshot storage for virtual device %1.
- 11591 Failed to expand snapshot storage for virtual device %1: maximum segment exceeded (error code %2).
- 11592 Console (%1): Failed to sync replication status for virtual tape %2 to the new target server.
- 11593 Failed to expand snapshot storage for virtual device %1 (segment allocation error code %2).
- 11594 Console (%1): Failed to set Email Alerts option %2.
- 11596 Console (%1): Failed to set hostedbackup option %2.
- 11605 Failed to create character device to map timemark %1 for virtual device %2.
- 11608 Console (%1): Failed to proceed copy/rollback timemark operation with client attached on the target virtual device %2.

- 
- 11609 [Task %1] Failed to create timemark for virtual device %2 while the last creation/client notification is in progress.
- 11610 Console (%1): Failed to create timeview for virtual device %2 timemark %3.
- 11613 Console (%1): Failed to enable timemark for device %2.
- 11615 Console (%1): Failed to disable timemark for device %2.
- 11618 Failed to select timemark %1 for virtual device %2: timemark %3 has already been selected.
- 11619 Failed to select timemark %1 character device for virtual device %2.
- 11621 Failed to create timemark %1 for virtual device %2.
- 11623 Failed to delete timemark %1 for virtual device %2.
- 11625 Failed to copy timemark %1 of virtual device %2 as virtual device %3.
- 11627 Failed to rollback timemark to timestamp %1 for virtual device %2.
- 11629 Failed to auto delete group member timemark %1 for virtual device %2.
- 11631 Failed to expand snapshot storage for virtual device %1.
- 11632 Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec autoRecoveryInterval: %3 sec>.
- 11633 Console (%1): Failed to set failover option on secondary server <heartbeatInterval: %2 sec autoRecoveryInterval: disabled>.
- 11645 Console (%1): Failed to create timeview: virtual device %2 already have a timeview.
- 11648 Failed to get inquiry string on SCSI device %1.
- 11649 Failed to convert inquiry string on SCSI device %1.
- 11650 Failed to get capacity size for SCSI device %1.
- 11651 Medium Test failed for SCSI device %1.
- 11652 Could not get type for SCSI device %1 because of inquiry string failure.
- 11653 Discarded scsi device %1 unsupported type "%2".
- 11654 Discarded scsi device %1 missing MTI vendor in inquiry string.
- 11655 Discarded scsi device %1 bad capacity size.
- 11656 Discarded scsi device %1 unsupported Cabinet ID.
- 11657 Discarded scsi device %1 missing "%2" vendor in inquiry string.
- 11665 Console (%1): Failed to enable backup for virtual device %2.
- 11667 Console (%1): Failed to disable backup for virtual device %2.
- 11668 Console (%1): Failed to stop backup sessions for virtual device %2.
- 11672 Console (%1): Virtual device %2 cannot join snapshot group %3 group id %4.
- 11673 Console (%1): Virtual device %2 cannot leave snapshot group %3 group id %4.
- 11676 Console (%1): Failed to resize NAS filesystem on virtual device %2.
- 11681 Console (%1): Failed to resume cache resource %2 (ID: %3).
- 11683 Console (%1): Failed to suspend cache resource %2 (ID: %3).

- 
- 11684 Console (%1): Failed to reset cache on target device %2 (ID: %3) for %4 copy.
  - 11686 Console (%1): Failed to add %2 Resource %3 (ID: %4).
  - 11688 Console (%1): Failed to delete %2 Resource %3 (ID: %4).
  - 11690 Console (%1): Failed to resume HotZone resource %2 (ID: %3).
  - 11692 Console (%1): Failed to suspend HotZone resource %2 (ID: %3).
  - 11693 Console (%1): HotZone policy for resource %2 (ID: %3) updated successfully.
  - 11694 Console (%1): Failed to update policy for HotZone resource %2 (ID: %3).
  - 11695 Console (%1): Failed to get HotZone statistic information.
  - 11696 Console (%1): Failed to get HotZone status.
  - 11698 Console (%1): Failed to update policy for snapshot/timemark resource (ID: %2).
  - 11699 Console (%1): Failed to get port mapping for adapter no %2 persistent binding.
  - 11701 Console (%1): Failed to reinitialize snapshot resource (ID: %2) for virtual device (ID: %3).
  - 11704 Console (%1): The configuration file update for %2 %3(s) was rolled back.
  - 11705 Console (%1): The disk partition update for %2 %3(s) was rolled back.
  - 11706 Console (%1): The device creation for %2 %3(s) was rolled back.
  - 11707 Console (%1): Failed to create %2 %3(s). Error: %4.
  - 11709 Console (%1): The configuration file update for replication setup for %2 %3(s) was rolled back.
  - 11710 Console (%1): The disk partition update for replication setup for %2 %3(s) was rolled back.
  - 11711 Console (%1): The replication setup for %2 %3(s) was rolled back.
  - 11712 Console (%1): Failed to configure replication for %2 %3(s). Error: %4.
  - 11714 Console (%1): The configuration file update for replication removal for %2 %3(s) was rolled back.
  - 11715 Console (%1): The disk partition update for replication removal for %2 %3(s) was rolled back.
  - 11716 Console (%1): The replication removal for %2 %3(s) was rolled back.
  - 11717 Console (%1): Failed to remove replication for %2 %3(s). Error: %4.
  - 11719 Console (%1): The configuration file update for deleting %2 %3(s) was rolled back.
  - 11720 Console (%1): The disk partition update for deleting %2 %3(s) was rolled back.
  - 11721 Console (%1): The deletion of %2 %3(s) was rolled back.
  
  - 11722 Console (%1): Failed to delete %2 %3(s). Error: %4.
  - 11724 Console (%1): The configuration file update for promoting %2 %3(s) was rolled back.
  - 11725 Console (%1): The disk partition update for promoting %2 %3(s) was rolled back.
  - 11726 Console (%1): The promotion of %2 %3(s) was rolled back.
  - 11727 Console (%1): Failed to promote %2 %3(s). Error: %4.

- 
- 11729 Console (%1): Failed to update replication properties for %2 %3(s). Error: %4.
- 11731 Console (%1): Failed to update replica properties for %2 %3(s). Error: %4. needed space=%2MB licensed capacity=%3MB.
- 11734 Console (%1): The configuration file update for virtual library creation was rolled back.
- 11735 Console (%1): Adding virtual library to the system was rolled back.
- 11736 Console (%1): Failed to create virtual library. Error: %2.
- 11738 Console (%1): The configuration file update for virtual drive creation was rolled back.
- 11739 Console (%1): Adding virtual tape drives to the system was rolled back.
- 11740 Console (%1): Failed to create virtual tape drives. Error: %2.
- 11741 Console (%1): Failed to create virtual library with %2 slots due to only %3 slots available.
- 11742 Console (%1): Create only %2 out of %3 virtual drives requested due to memory allocation failure.
- 11744 Console (%1): The configuration file update for testmode promoting %2 %3(s) was rolled back.
- 11745 Console (%1): The disk partition update for testmode promoting %2 %3(s) was rolled back.
- 11746 Console (%1): The testmode promotion of %2 %3(s) was rolled back.
- 11747 Console (%1): Failed to testmode promote %2 %3(s). Error: %4.
- 11760 Console (%1): Failed to get information for license activation.
- 11761 Console (%1): Failed to activate license (%2).
- 11782 Barcode [%1] of the source tape id %2 already exist on target server %3. Auto-replication cannot be configured.
- 11783 Failed to setup auto-replication for tape id %1 on target server %2. Error: %3.
- 11788 Appliance Hardware Problem: %1.
- 11791 Failed to shrink virtual tape %1 to %2 MB. Error: %3.
- 11796 Failed to set the migration disk threshold.
- 11797 Failed to set the reclamation disk threshold error = %1. interval: %6 watermark retry: %7 suspended: %8).
- 11900 Failed to import report request. interval: %6 watermark retry: %7 suspended: %8).
- 11901 Failed to parse report request %1 %2. interval: %6 watermark retry: %7 suspended: %8).
- 11902 Undefined report type %1. interval: %6 watermark retry: %7 suspended: %8).
- 11903 Failed to allocate memory.
- 11904 Failed to create directory %1.
- 11906 Failed to open file %1.
- 11907 Failed to write file %1.
- 11909 Failed to parse log file %1 %2.
- 11910 Failed to create report file %2 (type %1).
- 12002 Failed to open directory %1.

- 
- 12003 Failed to open file %1.
  - 12004 Failed to create directory %1.
  - 12005 Failed to allocate memory.
  - 12007 Failed to delete file %1.
  - 12008 Wrong file format %1.
  - 12009 Missing parameter %1.
  - 12010 Invalid parameter %1.
  - 12011 Wrong status for file %1.
  - 12501 Failed to set virtual library properties cannot find virtual library %1.
  
  - 12502 Failed to set virtual library properties no tape library properties for virtual library %1.
  - 12503 Failed to set virtual library properties cannot find encryption key %1.
  - 12504 Failed to set virtual library properties no tape properties for virtual library %1.
  - 12505 Failed to set virtual library properties cannot get library export key info vid %1. interval: %6 watermark retry: %7 suspended: %8).
  - 12506 Failed to set virtual library properties failed to set tape caching policy for virtual library %1. interval: %6 watermark retry: %7 suspended: %8).
  - 12508 Failed to set virtual library %1 properties.
  - 12509 Failed to inventory physical library %1.
  - 12511 Failed to move tape in library %1 from slot %2 to drive %3.
  - 12512 Failed to set disk capacity threshold error = %1.
  - 12514 Failed to restart job %1 (cmd %2
  - 12516 Revision is NULL.
  - 12517 Cannot find virtual device %1.
  - 12518 This virtual device %1 is not virtual library or virtual drive.
  - 12519 Partition checksum mismatch for virtual device %1.
  - 12521 Failed to move tape in library %1 from drive %2 to slot %3.
  - 12523 Failed to change firmware revision to %1 for %2 error = %3.
  - 12525 Failed to reclaim tape %1.
  - 12527 Failed to enable IBM 3494 library for %1 error = %2.
  - 12531 Failed to move tape from library vid:%1 source slot %2 to destination slot %3.
  - 12532 Failed to set IBM 3494 configuration.
  - 12534 Physical library %1 does not exist.
  - 12535 Cannot get the virtual tape import key information
  - 12536 Cannot rollback configuration %1.
  - 12538 Failed to alloc space for tape.
  - 12540 The physical drive %1 does not exist.
  - 12542 Failed to reset physical library %1.

- 
- 12545 Failed to set tape caching policies for virtual library %1.
  - 12546 Failed to update xml.
  - 12547 Cannot find TLE repository.
  - 12548 Failed to cancel job0.01
  - 12550 Cannot hold job %1 because it's running.
  - 12551 Failed to hold job %1.
  - 12553 Cannot resume job %1 because it's running.
  - 12554 Failed to resume job %1.
  - 12556 Cannot allocate space for return structure.
  - 12557 Failed to hold job %1 error = (%2
  - 12559 Failed to resume job %1 error = (%2
  - 12561 Failed to submit export job to physical library %1 for %2.
  - 12564 Failed to set compression.
  - 12565 Failed to move tape in library %1 from ieslot %2 to slot %3.
  - 12567 Failed to move tape in library %1 from slot %2 to ieslot %3.
  - 12569 Cannot find device %1.
  - 12570 Cannot update reserve\_for\_local\_use flags for %1
  - 12571 Failed to reserve for local use.
  - 12573 Failed to unreserve for local use.
  - 12575 Invalid library type %1 for physical library %2.
  - 12576 The tleioctl failed0.01
  - 12578 Failed to submit import job from physical library %1 for %2 to virtual library %3 for %4.
  - 12579 Failed to submit import job from physical drive %1 to virtual library %2 for tape %3.
  - 12580 Failed to rescan virtual library/drive unassigned from local system.
  
  - 12581 Failed to scan stacking physical tape %1: %2 error = %3.
  - 12583 Failed to submit job to export stacking virtual tapes to physical library %1.
  - 12585 Virtual tapes and physical tapes do not match.
  - 12586 Failed to allocate virtual tape list in physical tape.
  - 12587 Failed to allocate virtual tape list.
  - 12588 Failed to submit job to import stacked tapes from %1 to %2 error = %3.
  - 12590 Failed to purge job %1 error = (%2
  - 12592 Failed to set tape properties for %1.
  - 12594 Failed to set tape properties with mask %1 for %2.
  - 12596 Failed to set reschedule job.
  - 12598 Failed to purge physical tape %1 from database.

- 
- 12600 (%1) Failed to assign %2 to client %3 (%4 %5). Maximum number of Fibre Channel devices assigned to client is reached.
  - 12601 Failed to load ejected tape for virtual drive %1.
  - 12603 Failed to assign ACSLS/LS physical drive %1 error = %2.
  - 12605 Failed to eject physical tapes error = %1.
  - 12607 Failed to enter ACSLS/LS physical tapes error = %1.
  - 12609 Failed to assign physical tape %1 to vtl category.
  - 13100 Failed to retrieve primary's heartbeat information.
  - 13101 Failed to communicate with primary. Error: %1
  - 13102 Failed to run %1.
  - 13300 Failed to authenticate to the primary server --Failover Module stopped.
  - 13301 Failed to authenticate to the local server --Failover Module stopped.
  - 13302 Failed to transfer primary static configuration to secondary.
  - 13303 Failed to transfer primary dynamic configuration to secondary.
  - 13304 Failed to rename file %1.
  - 13305 Failed to write to file %1.
  - 13306 Failed to open file %1.
  - 13307 Failed to transfer primary credential information to secondary.
  - 13308 Invalid failover configuration detected. Failover will not occur.
  - 13309 Primary server %1 failed to respond command from secondary. Error: %2.
  - 13310 Failed to copy from %1 to %2.
  - 13311 Failed to merge static configuration for the primary server.
  - 13312 Failed to merge dynamic configuration for the primary server.
  - 13313 Out of memory --%1.
  - 13314 Failed to read from file %1.
  - 13315 Failed to merge authentication information for the primary server.
  - 13316 Fail to add virtual IP address. Error: %1.
  - 13317 Fail to release virtual IP address. Error: %1.
  - 13318 Failed to restore authentication information for this server.
  - 13319 Fail to stop IPStor failover module. Host may need to reboot.
  - 13320 Failed to update the configuration files to the primary server --%1.
  - 13700 Failed to allocate memory --Self-Monitor Module stopped.
  - 13701 Failed to release virtual IP address. Error: %1. Retrying the operation.
  - 13702 Failed to add virtual IP address: %1. Retrying the operation.
  - 13703 Failed to stop IPStor Self-Monitor Module.
  - 13704 IPStor module failure detected. Condition: %1.
  - 13818 Quorum disk negotiation failed.

- 
- 13821 Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.
  - 13827 Fail to stop quorum updating process. PID: %1. Maybe due to storage device or connection failure.
  
  - 13830 Get configuration file from storage failed.
  - 13833 Failed to backup file from %1 to %2.
  - 13834 Failed to copy file out from Quorum repository.
  - 13835 Failed to take over primary.
  - 13836 Failed to get configuration files from repository. Check and correct the configuration disk.
  - 13841 Secondary server does not match primary server status (%1).
  - 13843 Secondary server failed to get original conf file from repository before failback .
  - 13844 Failed to write %1 to repository.
  - 13850 Secondary server cannot locate quorum disk. Either the configuration is wrong or the drive is offline.
  - 13851 Secondary server can't take over due to %1
  - 13856 Secondary server %1 failed to communicate with primary server %2 through IP %3.
  - 13860 Failed to merge configuration file %1 %2.
  - 13861 Failed to rename file from %1 to %2.
  - 13862 Failed to write file %1 to repository
  - 13866 Failed to remove schedule
  - 13878 Primary server has invalid failover configuration.
  - 14000 Cannot find virtual device %1.
  - 14001 Partition checksum mismatch for virtual device %1.
  - 14003 Failed to parse config.
  - 14004 Cannot rename vdev %1 to %2.
  - 14005 Cannot update ipstor partition information.
  - 14006 Cannot write configuration %1.
  - 14008 Failed to rename pdev %1 to %2.
  - 14010 Cannot find client %1.
  - 14011 Failed to rename client %1 to %2.
  - 14016 Console (%1): Failed to renew caching tape id %2.
  - 14021 Failed to erase the physical disk(acsl=%1).
  - 14023 Failed to claim the physical disk(acsl=%1).
  - 14025 Failed to enable physical device(id=%1).
  - 14027 Failed to disable physical device(id=%1).
  - 15000 Snapshot copy failed to start because of invalid input arguments.

- 
- 15002 Snapshot copy from virtual device id %1 to id %2 failed because it failed to open file %3.
  - 15003 Snapshot copy from virtual device id %1 to id %2 failed because it failed to allocate (%3) memory.
  - 15004 Snapshot copy from virtual device id %1 to id %2 failed because an error occurred when writing to file %3 errno is %4.
  - 15005 Snapshot copy from virtual device id %1 to id %2 failed because an error occurred when lseek in file %3 errno is %4.
  - 15006 Snapshot copy from virtual device id %1 to id %2 failed because an error occurred when reading from file %3 errno is %4.
  - 15016 Timemark copy failed to start because of invalid input arguments.
  - 15018 Timemark copy from virtual device id %1 snapshot image %2 to id %3 failed because it failed to open file %4.
  - 15019 Timemark copy from virtual device id %1 snapshot image %2 to id %3 failed because it failed to allocate (%4) memory.
  - 15020 Timemark copy from virtual device id %1 snapshot image %2 to id %3 failed because an error occurred when writing to file %4 errno is %5.
  - 15021 Timemark copy from virtual device id %1 snapshot image %2 to id %3 failed because an error occurred when lseek in file %4 errno is %5.
  - 15022 Timemark copy from virtual device id %1 snapshot image %2 to id %3 failed because an error occurred when reading from file %4 errno is %5.
  
  - 15024 Timemark copy from virtual device id %1 snapshot image %2 to id %3 might have run out of snapshot reserved area. Please expand the snapshot reserved area.
  - 15032 Timemark rollback failed to start because of invalid input arguments.
  - 15034 Timemark rollback virtual device id %1 to snapshot image %2 failed because it failed to open file %3.
  - 15035 Timemark rollback virtual device id %1 to snapshot image %2 failed because it failed to allocate (%3) memory.
  - 15036 Timemark rollback virtual device id %1 to snapshot image %2 failed because an error occurred when writing to file %3 errno is %4.
  - 15037 Timemark rollback virtual device id %1 to snapshot image %2 failed because an error occurred when lseek in file %3 errno is %4.
  - 15038 Timemark rollback virtual device id %1 to snapshot image %2 failed because an error occurred when reading from file %3 errno is %4.
  - 15040 Timemark rollback virtual device id %1 to snapshot image %2 might have run out of snapshot reserved area. Please expand the snapshot reserved area.
  - 15050 Server ioctl call %1 failed on vdev id %2: Invalid Argument (EINVAL).
  - 15051 Server ioctl call %1 failed on vdev id %2: I/O error (EIO).
  - 15052 Server ioctl call %1 failed on vdev id %2: Not enough memory space (ENOMEM).
  - 15053 Server ioctl call %1 failed on vdev id %2: No space left on device (ENOSPC).

- 
- 15054 Server ioctl call %1 failed on vdev id %2: Already existed (EEXIST).
- 15055 Server ioctl call %1 failed on vdev id %2: Device or resource is busy (EBUSY).
- 16001 Console(%1): Converting file system failed: %2.
- 17001 Rescan replica cannot proceed due to replication already in progress.
- 17002 Rescan replica cannot proceed due to replication control area missing.
- 17003 Rescan replica cannot proceed due to replication control area failure.
- 17004 Replication cannot proceed due to replication control area failure.
- 17005 Replication cannot proceed due to replication control area failure.
- 17006 Rescan replica cannot proceed due to replication control area failure.
- 17007 Rescan replica failed.
- 17008 Replication failed.
- 17009 Failed to start replica rescan.
- 17010 Failed to start replication.
- 17011 Rescan replica failed due to network transport error.
- 17012 Replicating replica failed due to network transport error.
- 17013 Rescan replica failed due to local disk error.
- 17014 Replication failed due to local disk error.
- 17015 Replication failed because local snapshot used up all of the reserved area.
- 17016 Replication failed because the replica snapshot used up all of the reserved area.
- 17017 Rescan replica failed due to replica failed with error.
- 17018 Replication failed due to replica failed with error.
- 17019 Replication control area exchange failed with error.
- 17020 Replication failed with error.
- 18000 SIR: The physical storage device %1 [%2] is missing on this server.
- 18001 SIR: Startup of SIR Repository has been aborted because of the missing storage. Check that each member of the cluster is operating properly.
- 18050 SIR: Reclamation Dispatcher Daemon terminated because Cruncher has failed.
- 18055 SIR: Index Reclamation did not complete. Reason: %1
- 18060 SIR: Storage Reclamation did not complete. Reason: %1
- 18066 SIR: Index pruning did not complete. Reason: %1
- 18101 SIR: This standby server has failed to get IPMI status of the SIR node %1 at IP address %2. This may compromise SIR node failure protection. Check the IPMI configuration on that node.
- 18104 SIR: This standby server has failed to take over the SIR node %1 because the failed node reported its hostname as '%2' that is unknown to this server.
- 18105 SIR: This standby server has failed to take over the SIR node %1 because there is no standby node information in the SIR cluster configuration file.

- 
- 18106 SIR: This standby server has failed to take over the SIR node %1 because it could not shutdown the failed node using IPMI at IP address %2.
- 18107 SIR: This standby server has failed to take over the SIR node %1 because it could not add virtual IP %2 of the failed node.
- 18108 SIR: This standby server has failed to take over the SIR node %1 because it could not spoof WWPN of the failed node.
- 18109 SIR: This standby server has failed to take over the SIR node %1 because it could not change its hostname to that of the failed node.
- 18110 SIR: This standby server has failed to take over the SIR node %1 because it could not load the failed node's physical resources.
- 18111 SIR: This standby server has failed to take over the SIR node %1 because it could not copy the failed node's configuration files.
- 18112 SIR: This standby server has failed to take over the SIR node %1 because it could not start SIR services.
- 18113 SIR: This standby server has failed to take over the SIR node %1 because it was not allowed. Reason: %2.
- 18114 SIR: This standby server cannot see the physical device %1 [%2] used for SIR storage. This may compromise SIR node failure protection. Rescan devices on the standby node.
- 18116 SIR: This standby server detected the physical device %1 [%2] used for SIR storage
- 19003 The Snapshot Resource of the %1 Resource: %2 (ID: %3) failed to be expanded by the Administrator from %4 MB to %5 MB. Error: %6.
- 19056 [Remote Copy] The copying of the virtual tape to the remote server has failed while %1. Error: %2. (Server: %3 Virtual Tape: %4
- 19057 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to connect to remote server %1.
- 19058 [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 [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 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to open configuration file.
- 19061 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- unable to allocate memory.
- 19062 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed - unexpected error %1.
- 19063 [Remote Copy] The copying of the virtual tape %1 to the remote server has been manually aborted by user
- 19064 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- failed to load the virtual tape %1.
- 19065 [Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- virtual tape %1 is in the drive.

- 
- 19066 [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.
- 19068 [Auto Replication] The replica %1 of the virtual tape %2 cannot be promoted since target server is busy or RPC failure (%3).
- 19200 Console (%1): Failed to get the key list.
- 19201 Console (%1): Failed to get the key.
- 19202 Console (%1): Failed to create key %2.
- 
- 19204 Console (%1): Failed to delete Key %2.
- 19206 Console (%1): Failed to update information for key %2.
- 19208 Console (%1): Failed to create key package %2.
- 19210 Console (%1): Failed to get key package information.
- 19211 Console (%1): Failed to save keys from key package.
- 20002 SAN/IP driver failed to initialize.
- 21002 SAN SCSI driver failed to initialize.
- 22001 Fibre Channel Authentication error %1 at %2.
- 22004 Fibre Channel Authentication error. Client Name does not match on Server %1.
- 22005 Fibre Channel Authentication error. Signature does not match on Server %1.
- 25001 %1 failed to start --%2.
- 25003 %1 failed to pause --%2.
- 25005 %1 failed to resume --%2.
- 25007 %1 failed to stop --%2.
- 25011 Failed to open service manager --%1.
- 25012 Failed to open service --%1.
- 26000 Failed to create TCP socket.
- 26001 Failed to bind TCP socket.
- 26002 Failed to create TCP service.
- 26003 Failed to create TCP thread.
- 26100 Failed to access the %1 driver --%2.
- 26101 The SAN SCSI driver is the wrong version for this IPStor SAN Client. Driver version %1 will not work with client version %2.
- 26102 Failed to open the %1 driver --%2.
- 26103 Failed to start the %1 driver.
- 26104 Failed to stop the %1 driver.
- 26105 SAN SCSI cannot connect to IPStor Server %1 --%2.
- 26106 SAN SCSI cannot attach to IPStor SAN device %1/%2 --%3.
- 26107 SAN SCSI cannot detach from IPStor SAN device %1/%2 --%3.
- 26108 SAN SCSI cannot disconnect from IPStor Server %1 --%2.

---

26110 Failed to rescan SCSI port %1 --%2.  
26200 Failed to access '%1' --%2.  
26201 Failed to read the drive layout for '%1' --%2.  
26202 Failed to assign drive %1 to drive letter %2. It is already in use.  
26203 Failed to access drive %1 --%2.  
26204 Failed to dismount drive %1 --%2.  
26205 Failed to lock drive %1 --%2.  
26206 Failed to unlock drive %1 --%2.  
26207 Failed to define device %1 --%2.  
26208 Failed to undefine device %1 --%2.  
26209 Drive %1 is busy and cannot be detached. The SAN Client cannot stop at this time.  
27000 Failed to connect to IPStor Server '%1' --%2.  
27001 Failed to get the version of IPStor Server '%1' --%2.  
27002 Failed to get the information for IPStor Server '%1' --%2.  
27003 Failed to get the number of adapters for IPStor Server '%1' --%2.  
27004 Failed to get the information for IPStor Server '%1' adapter %3 --%2.  
27005 Failed to get the number of devices for IPStor Server '%1' --%2.  
27006 Failed to get the information for IPStor Server '%1' device %3 --%2.  
27007 Failed to get the list of IP addresses for IPStor Server '%1' --%2.  
27008 Failed to get the media information for IPStor Server '%1' device %3 --%2.  
28001 Failed to add IPStor Server '%1' --%2.  
28002 Failed to add IPStor Server '%1' adapter %2 --%3.  
  
28003 Failed to add IPStor Server '%1' adapter %2 channel %3 --%4.  
28004 Failed to add IPStor Server '%1' device %2 --%3.  
28005 Failed to add IPStor Server '%1' device %2 volume %3 --%4.  
29405 Notify Timeout error waiting on %1  
31003 Failed to open file %1.  
31004 Failed to add user %1 to the NAS server.  
31005 Failed to allocate memory.  
31006 Failed to delete file %1.  
31011 IPSTORUMOUNT: Failed to unmount %1.  
31012 The NASGRP group is missing from /etc/group.  
31013 IPSTORMOUNT: Failed to mount %1.  
31017 Failed to write to file %1.  
31020 Failed to rename file %1 to file %2.  
31023 IPSTORNASMGTD: Failed to create file %1.

- 
- 31024 IPSTORNASMGTD: Failed to lock file %1.
  - 31025 IPSTORNASMGTD: Failed to open file %1.
  - 31028 Failed to lock file %1.
  - 31029 Failed to create file %1.
  - 31030 Failed to create directory %1.
  - 31031 Failed to remove directory %1.
  - 31032 Failed to execute program '%1'.
  - 31034 Local IPStor SAN Client is not running.
  - 31035 Failed to add group %1 to the NAS server.
  - 31036 Failed to delete user %1 from the NAS server.
  - 31037 Error accessing NAS Resource state file for virtual device %1.
  - 31039 Failed to rename file %1 to file %2.
  - 31040 Failed to create the NAS Resource. Failed to allocate SCSI disk device handle - operating system limit reached.
  - 31041 Exceed maximum number of reserved NAS users
  - 31042 Exceed maximum number of reserved NAS groups
  - 31043 Failed to setup password database
  - 31044 Failed to make symlink from %1 to %2
  - 31045 Failed to update /etc/passwd
  - 31046 Failed to update /etc/group
  - 31047 Synchronization daemon is not running
  - 31048 Device %1 mount error
  - 31049 Device %1 umount error
  - 31050 Failed to detach device vid %1
  - 31051 Failed to attach device vid %1
  - 31053 Invalid file content in %1
  - 31054 Failed to get my hostname
  - 31055 SAM: connection failure.
  - 31061 Nas process %1 fail.
  - 31062 Failed to read from file %1
  - 31063 Failed to write to file %1
  - 31064 Error file system type %1
  - 31065 Error setting quota of uid %1 in %2
  - 31066 Invalid XML file
  - 31067 cannot parse dynamic configuration %1
  - 31068 dynamic configuration does not match %1
  - 31071 Missing file %1
  - 31072 Failed to update CIFS native configuration

---

31073 Failed to update NFS native configuration  
31074 Failed to parse xml file %1  
31075 Failed to unmount NAS resource %1 during failing over  
31078 Add NAS resource to iocore fail during failover processing %1  
31079 Missing file system commands %1 of %2  
31080 NAS: Access denied to %1 security accounts manager (SAM) database  
40002 Block list full on Drive %1  
40003 Corrupt Repository Rep VID %1  
40004 Unsupported device [%1][%2][%3]  
40005 Load Drive failed. Lib %1 Drive %2  
40006 TDE get drive info failed Drive %1  
40007 Unload tape from drive failed Drive %1  
40008 Failed to create new tape in Virtual Library %1  
40009 HW Error with Move Medium command Lib %1  
40010 Attach to tape %1 failed  
40011 Failed to read from Virtual Tape. Tape VID %1 EC %2  
40013 Export Tape failed not enough memory. Job id %1  
40014 Read tape info failed. Tape VID %1 EC %2  
40015 Export tape failed unsupported block size %1  
40016 Failed to write to Virtual Tape. Tape VID %1 EC %2  
40017 Failed to write to Physical Tape. Drive VID %1 EC %2  
40018 Failed to load Physical Tape. Lib VID %1 Drive VID %2  
40019 Failed to write to Virtual Tape. Tape VID %1 EC %2  
40021 Failed to locate Virtual Library %1  
40022 Failed to get Physical Tape block size. Drive VID %1 EC %2  
40023 Import failed not enough memory %1  
40029 Not enough memory to complete the operation  
40030 Failed to read from repository. Rep VID %1 EC %2  
40031 Failed to write to repository. Rep VID %1 EC %2  
40036 Failed to attach to repository %1  
40039 Read Element command to Physical Library %1 failed. EC %2 rc %3).  
40040 Attach to device %1 failed. EC %2  
40043 Move Medium command failed in Physical Library %1. SrcEle %2 DestEle %3  
40044 Unload command failed on Physical Tape Drive %1. EC %2  
40045 Read from Physical Tape Drive %1 failed. EC %2  
40046 Write to Physical Tape Drive %1 failed. EC %2  
40047 Write Filemark to Physical Tape Drive %1 failed. EC %2

- 
- 40048 Mode sense command to Physical device %1 failed. Pagecode %2 EC %3
  - 40049 Mode select command to Physical device %1 failed. EC %2
  - 40050 Rewind command to Physical Tape Drive %1 failed. EC %2
  - 40051 Inquiry command to Physical device %1 failed. EC %2
  - 40065 Read data from Virtual Tape failed. Attach handle %1 EC %2
  - 40066 Write data to Virtual Tape failed. Attach handle %1 EC %2
  - 40067 Failed to add Physical Drive %1 to repository %2. EC %3
  - 40068 Cannot create new Tape. EC %1
  - 40069 Cannot expand Tape %1. EC %2
  - 40070 Cannot delete Tape %1
  - 40071 Cannot import Tape dest slot %1 in Virtual Library %2 is full
  - 40074 Export to Physical Tape failed. Job ID %1 EC %2
  - 40076 Import Physical Tape failed. Job ID %1 EC %2
  - 40077 Import Physical Tape failed. Duplicate Virtual Tape Barcode. Job ID %1 DestTape [%2]
  - 40078 Import Physical Tape failed. Duplicate Virtual Tape Barcode. Dest Tape [%1]
  
  - 40085 Reverse block command failed on physical tape drive VID %1 Error [%2]
  - 40087 ACSLS/LS: Error in retrieving the hostname of this VTL server. Error: %1
  - 40088 ACSLS/LS: Failure in looking up the IP address of the VTL server (%1). Please verify that DNS is configured correctly for both ACSLS/LS and VTL server. Error: %2
  - 40089 ACSLS/LS: Out of system resources. Failed to fork a process. Error: %1
  - 40090 ACSLS/LS: Failed to execute a program. Error: %1
  - 40091 ACSLS/LS: Failed to open %1. Error: %2
  - 40092 ACSLS/LS: DNS configuration for VTL server is incorrect. DNS or /etc/hosts is returning %1 as the IP of VTL server (%2)
  - 40093 ACSLS/LS: Failed to successfully query %1 server with IP %2 and ACS %3. Error received: %4.
  - 40094 ACSLS/LS: Waited %1 seconds to get a response to a query from %2 (%3 ACS %4). The operation is timed out.
  - 40095 ACSLS/LS: Failed to mount %1 on drive %2. Error from %3 (%4): %5.
  - 40096 ACSLS/LS: Waited %1 seconds to get a response from %2 (%3) after trying to mount %4 on drive %5. The operation is timed out.
  - 40097 ACSLS/LS: Failed to dismount %1 from drive %2. Error from %3 (%4): %5.
  - 40098 ACSLS/LS: Waited %1 seconds to get a response from %2 (%3) after trying to dismount %4 from drive %5. Timing out.
  - 40099 ACSLS/LS: Failed to retrieve drive information in ACS %1. Error from %2 (%3): %4.
  - 40100 ACSLS/LS: Waited %1 seconds to get a response from %2 (%3) after trying to retrieve drive information in ACS %4. Timing out.

- 
- 40101 ACSLS/LS: Failed to retrieve volume information in ACS %1 and Pool %2. Error from %3 (%4): %5.
  - 40102 ACSLS/LS: Waited %1 seconds to get a response from ACSLS/LS (%2) after trying to retrieve volume information in ACS %3 and Pool %4. Timing out.
  - 40103 ACSLS/LS: Failed to retrieve LSM information in ACS %1. Error from %2 (%3): %4.
  - 40104 ACSLS/LS: Waited %1 seconds to get a response from %2 (%3) after trying to retrieve LSM information in ACS %4. Timing out.
  - 40105 %1: The number of drives %2 is more than max supported (%3).%3).
  - 40106 %1: The number of volumes %2 is more than max supported (%3).
  - 40109 Log sense command to Physical device %1 failed. Pagecode %2 EC %3 %3).
  - 40110 Failed to retrieve volume information in ACS %1. Error from %2 (%3): %4.
  - 40111 ACSLS/LS: Waited %1 seconds to get a response from Library Station (%2) after trying to retrieve volume information in ACS %3. Timing out.
  - 40116 Hardware compression failed. EC [ %1 ] complete code [%2]
  - 40117 Hardware decompression failed. EC [ %1 ] complete code [%2]
  - 40118 Software decompression of a block compressed using hardware failed. EC [ %1 ]
  - 40123 Failed to load tape because it is a cleaning tape. Lib VID %1 Drive VID %2
  - 40124 Write command to Configuration Repository Failed. Please check repository LUNs
  - 40126 Failed to reclaim the tape VID %1 Barcode [%2] in library VID %3.
  - 40128 Failed to reclaim disk space allocated for tape VID %1 Barcode [%2] in vault
  - 40132 The tape shredding job was failed on the tape [%1] -status:%2.
  - 40133 Unable to move tape [%1] to IE slot.
  - 40134 Unable to mount tape [%1] in library [%2] VID %3.
  - 40135 Unable to dismount tape [%1] in library [%2] VID %3.
  - 40136 Space command to Physical Library %1 failed. EC %2.
  - 40137 Failed to add import/export job to the job queue. Maximum of %1 jobs reached. Job ID:%2 Physical tape barcode:[%3].
  - 40141 Scan Physical Tape failed. Job ID %1 EC %2
  - 40142 Stack Import Physical Tape failed. Job ID %1 EC %2
  - 40143 Stack Export to Physical Tape failed. Job ID %1 EC %2
  
  - 40148 Stack Export Tape failed with not enough memory. Job id %1
  - 40152 Stack Import failed not enough memory %1
  - 40153 Cannot stack import Tape dest slot %1 in Virtual Library %2 is full
  - 40155 ACSLS/LS: Failed to eject %1 from CAP %2. Error from %3 (%4): %5.
  - 40156 ACSLS/LS: Waited %1 seconds for eject operation (%2 from %3 %4 CAP %5) to complete. Timing out.
  - 40158 ACSLS/LS: Failed to enter tapes from CAP %1. Error from %2 (%3): %4.

- 
- 40159 ACSLS/LS: Waited %1 second(s) for %2 server to enter tapes from CAP %3. Timing out.
  - 40161 ACSLS/LS: Failed to query CAP information for ACS %1. Error from %2 (%3): %4.
  - 40162 ACSLS/LS: Waited %1 second(s) for %2 server (%3) to return CAP information for ACS %4. The operation is timed out.
  - 40163 ACSLS/LS: Failed to find closest compatible drive for %1. Error from %2 (%3): %4.
  - 40164 ACSLS/LS: Waited %1 second(s) for %2 server (%3) to find the closest compatible drive for %4. The operation is timed out.
  - 40174 Export to Physical Tape failed because Physical Tape is WORM/VolSafe. Job ID %1 EC %2
  - 40177 Failed to read SIR data disk with GUID %1; Error code %2; Check the disk which might not be accessible. %3).
  - 40178 Console (%1): Failed to run patch script [%2]
  - 40179 Failed to parse configuration file %1.
  - 40180 Failed to save file %1.
  - 40190 OBSOLETE---Hardware compression card not ready -[ %1 ].
  - 40191 Hardware compression card failed -EC [ %1 ] complete code [%2]
  - 40193 ACSLS/LS: Failed to query %1 server with IP %2 and ACS %3. ACS ID %4 is invalid please verify input ACS ID.
  - 40194 ACSLS/LS: portmap/rpcbind daemon is required for ACSLS libraries. Please start portmap daemon using "portmap" command (On Solaris please use "rpcbind" to start rpcbind daemon) and do a rescan on the physical devices.
  - 40198 Repository consistency check detected critical errors. Check syslog for more information.
  - 40199 Compression data consistency check: Invalid data signature found on tape [%1] VID %2
  - 40200 Write Filemark Table failed. BC [%1] VID %2
  - 40201 Tape cannot be created -Duplicate VID found %1
  - 50000 iSCSI: Missing targetName in login normal session from initiator %1
  - 50002 iSCSI: Login request to nonexistent target %1 from initiator %2
  - 50003 iSCSI: iSCSI CHAP authentication method rejected. Login request to target %1 from initiator %2
  - 50111 SIR Cluster: Repository device %1 is not available on %2
  - 50115 SIR Cluster: %1 cannot detect fibre channel target(s) of %2
  - 50204 SIR: SIR tape drive (serial number: %1) cannot be found on SIR cluster node %2.
  - 50206 SIR: SIR data device %1 is not available.
  - 50305 SIR Replication: repository device %1 is not available on %2
  - 50501 RDE: Policy %1 was not saved. Error: %2.
  - 50503 RDE: Policy %1 was not deleted. Error: %2. Heartbeat %4][Secondary %2](HBInterval %5)(AutoRecovery %6)

---

50505 RDE: Policy %1 Tape [%2] [%3] failed to load in drive %4: %5.  
50507 RDE: Failed to unload tape %1 from drive %2. %3  
50509 RDE: Policy %1 failed to start: %2.  
50511 RDE: Policy %1 has completed with errors.  
50514 RDE: Policy %1 Tape [%2] scan failed to start: %3.  
50516 RDE: Policy %1 Tape [%2] terminated with error: %3.  
50519 RDE: Policy %1 Tape [%2] scan failed to suspend. Error: %3.  
50521 RDE: Policy %1 Tape [%2] scan failed to resume. Error: %3.

50523 RDE: Policy %1 Tape [%2] failed to convert to Virtual Index tape: %3.  
50525 RDE: Tape failed to resolve. VID: %1. %2.  
50531 RDE: Policy %1 Tape [%2] index replication terminated with error: %3.  
50534 RDE: Policy %1 Tape [%2] unique data replication terminated with error: %3.  
50538 RDE: Space Reclamation failed to start on SIR Node '%1'. %2  
50541 RDE: Space Reclamation failed session %1.  
50546 RDE: Space Reclamation failed for Tape %1[%2]; Error: %3.  
50554 RDE: Non-upgraded VIT %1[%2].

50702 SIR Scanner: Failed to start tape scan for Tape %1 in Drive %2; Reason is %3  
50706 SIR Scanner: Failed to create SIR folder for Tape %1 in Drive %2; Reason is %3  
50707 SIR Scanner: Failed to store data block from Tape %1 in Drive %2 to SIR folder;  
Reason is %3  
50709 SIR Scanner: Tape %1 scan failed in Drive %2; Reason is %3  
50714 SIR Scanner: Failed to convert Tape %1 in Drive %2 to Virtual Index Tape; Failed after:  
%3  
50719 SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 failed

50802 SIR Replication: Virtual Index Tape replica processing failed to start for Tape %1 in  
Source Drive %2 and Destination Drive %3; Reason is %4  
50803 SIR Replication: Failed to process data block from Tape %1 in Source Drive %2 and  
Destination Drive %3; Reason is %4  
50805 SIR Replication: Index tape replica processing failed for Tape %1 in Source Drive %2  
and Destination Drive %3; Reason is %4

50902 SIR Client: SIR client failed to initialize error %1  
50906 SIR Client: Store data block requested for folder %1 failed. Reason is %2  
50907 SIR Client: Failed to reach SIR server. Error is %1  
50908 SIR Client: Failed to initialize SIR server. Error is %1  
50909 SIR Client: Failed to get SIR server configuration. Error is %1  
50910 SIR Client: Failed to set SIR server configuration. Error is %1  
50911 SIR Client: Failed to get SIR object location. Error is %1

- 
- 50912 SIR Client: Failed to check SIR object hash status. Error is %1
  - 50913 SIR Client: Failed to create SIR folder. Error is %1
  - 50914 SIR Client: Replicate data block requested for folder %1 failed. Reason is %2
  - 50915 SIR Client: Close requested for folder %1 failed. Reason is %2
  - 50916 SIR Client: Abandon requested for folder %1 failed. Reason is %2
  - 50917 SIR Client: Flush requested for folder %1 failed. Reason is %2
  - 50952 SIR Server: Server not yet initialized. Reason is %1
  - 50954 SIR Server: Failed to access devices %1
  - 50955 SIR Server: Index storage device %1 is full
  - 50956 SIR Server: Data storage class %1 is full
  - 50958 SIR Server: Repository index is out of memory
  - 51003 SIR Failover: Failed to upload server %1 configuration file.
  - 51004 SIR Failover: Failed to set up shared secret between %1 and %2.

---

## Information Messages

- 1003 IPStor Server has detected virtual device[%1] at SCSI %2 channel %3
- 1004 IPStor Server has not detected any virtual device.
- 1009 There are %1 real device(s) associated with virtual device [%2].
- 1010 Real Device[%1 %2 %3 %4].
- 1013 IPStor Server [Build %1] is running on Linux %2.
- 1014 IPStor Server has been shut down.
- 1015 Maximum SCSI devices reached. On your IPStor Server verify with the command: cat /proc/scsi/scsi
- 1016 Primary virtual device %1 has failed. IPStor is switching to the secondary virtual device.
- 1017 Secondary virtual device %1 has failed.
- 1018 Snapshot for virtual device %1 created.
- 1019 Finished with snapshot on virtual device %1.
- 1020 Replication for virtual tape %1 started.
- 1021 Replication for virtual tape %1 finished.
- 1024 Device %1 has attached to the IPStor Server.
- 1025 Device %1 has detached from the IPStor Server.
- 1026 Replication has been started for virtual tape %1; it was triggered by the watermark.
- 1027 Replication has been started for virtual tape %1; it was triggered by the interval schedule.
- 1028 Replication has been started for virtual tape %1; it was triggered by the time of day schedule.
- 1029 Replication has been started for virtual tape %1; it was manually triggered by the administrator.
- 1041 Mirror synchronization started for virtual device %1.
- 1042 Mirror synchronization finished for virtual device %1.
- 1045 Rescan replica has completed for virtual device %1
- 1057 Replication control area exchange has completed for virtual tape %1
- 1058 Replication has finished for virtual tape %1. %2 KB in %3 seconds (%4KB/sec)
- 1062 Replication has been started for group %1; it was triggered by the watermark.
- 1063 Replication has been started for group %1; it was triggered by the interval schedule.
- 1064 Replication has been started for group %1; it was triggered by the time of day schedule.
- 1065 Replication has been started for group %1; it was manually triggered by the administrator.
- 1076 Starting replication for virtual device %1 of group %2 to replica device %3.
- 1077 Replication for group %1 has completed successfully.
- 1089 No data has been updated to the virtual tape %1 since last replication. Replication is completed without updating the replica.

- 
- 1090 Replication has been added into replication job queue for virtual tape %1 to check if the watermark is hit; if not the replication will not be started.
  - 1091 Replication has been added into replication job queue for virtual tape %1; it was triggered by the interval schedule.
  - 1092 Replication has been added into replication job queue for virtual tape %1; it was triggered by the time of day schedule.
  - 1093 Replication has been added into replication job queue for virtual tape %1; it was manually triggered by the administrator.
  - 1094 Replication cannot proceed --The updated data for virtual tape %1 is %2MB since last replication; It has not reached the watermark %3MB.
  - 1095 Replication has been added into replication job queue for virtual tape %1; it was triggered after migration.
  - 1096 Replication has been started for virtual tape %1; it was triggered after migration.
  - 1097 Replication has been added into replication job queue for virtual tape %1; it was triggered before migration.
  - 1098 Replication has been started for virtual tape %1; it was triggered before migration.
  
  - 1202 Path trespassed to %1 successfully.
  - 1205 Activated path successfully: %1.
  - 1209 Rescan FC adapters is recommended to correct the configuration.
  - 1213 Storage device added new path: %1.
  - 2000 Path status has changed : %1
  - 7000 Patch %1 installation completed successfully.
  - 7007 Patch %1 rollback completed successfully.
  - 10000 IPStor Server setup has begun.
  - 10007 IPStor Server setup is complete.
  - 10050 IPStor Server FSID update has begun.
  - 10051 IPStor Server FSID update vdev %1 local sect %2
  - 10052 IPStor Server FSID update pdev a:%1 c:%2
  - 10053 IPStor Server FSID update dynamic xml pdev from %1 to %2.
  - 10055 IPStor Server FSID update is complete.
  - 10056 Server Persistent Binding update has begun.
  - 10057 Server Persistent Binding update swap binding %1.
  - 10058 Server Persistent Binding update set default binding for %1.
  - 10060 Server Persistent Binding update is complete %1 changes.
  - 10202 Cancelled overwriting configuration %1.
  - 10206 Add scsi alias=%1.
  - 10208 Set Adapter %1 offline adapter count %2.
  - 11005 IPStor communication module started.

---

11010 Changed server time to %1.

11020 Auto save configuration enabled: FTP\_server=%1 directory=%2 interval=%3 copies=%4.

11021 Auto save configuration enabled: FTP\_server=%1 port=%2 directory=%3 interval=%4 copies=%5.

11022 Auto save configuration is disabled.

11037 Automated Tape Caching is %1 for virtual library %2.

11100 SAN Client (%1): SAN Client is added.

11102 SAN Client (%1): Authentication succeeded.

11105 SAN Client (%1): Logged in.

11108 SAN Client (%1): Logged out.

11198 Console (%1): Members of Physical Device %2 are changed from [%3] to [%4].

11199 Console (%1): Physical Device %2 has been modified by other members.

11210 Console (%1): Physical SCSI devices have changed.

11223 Console (%1): Logged in with read/write privileges.

11224 Console (%1): Logged in with read only privileges.

11225 Console (%1): Logged out.

11226 Console (%1): Configuration file %2 saved.

11227 Console (%1): Virtual device %2 added.

11228 Console (%1): Virtual device %2 removed.

11229 Console (%1): SAN Client (%2) added to virtual device %3.

11230 Console (%1): SAN Client (%2) removed from virtual device %3.

11239 Console (%1): Authentication module restarted.

11241 Console (%1): IPStor Server module started.

11243 Console (%1): IPStor Server module stopped.

11246 Console (%1): User %2 added.

11248 Console (%1): User %2 deleted.

11250 Console (%1): Password for user %2 reset.

11252 Console (%1): Password for user %2 updated.

11254 Console (%1): Virtual device %2 modified.

11256 Console (%1): Virtual device %3 for SAN Client (%2) modified.

11258 Console (%1): SAN Client (%2) added.

11260 Console (%1): SAN Client (%2) deleted.

11264 Console (%1): Configuration file %2 restored.

11267 Console (%1): Virtual device %2 partition erased.

11271 Console (%1): Mirror added for virtual device %2.

11273 Console (%1): Mirror removed for virtual device %2.

- 
- 11275 Console (%1): Mirroring stopped for virtual device %2.
  - 11277 Console (%1): Mirror synchronization for virtual device %2 started.
  - 11279 Console (%1): Mirror swapped for virtual device %2.
  - 11281 Console (%1): Shared secret created for IPStor Server %2.
  - 11283 Console (%1): Device category changed for physical device %2 to %3.
  - 11286 Console (%1): Failover command executed (%2).
  - 11288 Console (%1): Failover mode set (%2).
  - 11290 Console (%1): IPStor Server module restarted.
  - 11293 Console (%1): IP address swapped from %2 to %3.
  - 11297 Console (%1): Report file %2 removed.
  - 11299 Console (%1): Tested target device %2 successfully.
  - 11304 User %1 at IP address %2 authenticated.
  - 11305 Machine %1 at IP address %2 authenticated.
  - 11312 Client agent %1 requested license successfully.
  - 11314 Client agent %1 released license successfully.
  - 11503 Expand %1 by %2 MBytes to %3 MBytes.
  - 11509 Console (%1): Properties set for the IPStor Server.
  - 11513 Console (%1): Replica for virtual tape %2 was added to IPStor Server %3 (watermark: %4 MB time: %5
  - 11515 Console (%1): Replica for virtual tape %2 was removed from IPStor Server %3 (watermark: %4 MB time: %5
  - 11517 Console (%1): Virtual tape replica %2 was created.
  - 11519 Console (%1): Replication for virtual tape %2 started.
  - 11521 Console (%1): Replication for virtual tape %2 stopped.
  - 11523 Console (%1): Virtual tape replica %2 promoted to a virtual tape.
  - 11525 Console (%1): IPStor Server X-Ray has been run.
  - 11527 Console (%1): Copy Manager %2 added.
  - 11529 Console (%1): Removed Copy Manager %2 successfully.
  - 11531 Console (%1): Backed up Configuration files successfully.
  - 11533 Console (%1): Restored IPStor configuration files successfully.
  - 11536 Console (%1): Replication parameters for virtual tape %2 to IPStor Server %3 updated (watermark: %4 MB time: %5
  - 11538 Console (%1): Physical device %2 has been claimed.
  - 11543 Console (%1): Virtual tape replica %2 removed.
  - 11545 Console (%1): Virtual tape replica %2 modified.
  - 11547 Console (%1): Replication for virtual tape %2 is marked in sync.
  - 11550 Console (%1): Option "%2 %3" set.
  - 11552 Console (%1): Snapshot option %3 for virtual device %2 has been set.

- 
- 11555 Console (%1): Failover option <self check interval: %2 sec> has been set.
- 11557 Console (%1): Snapshot copy from device %2 to device %3 started.
- 11559 Console (%1): Initializing snapshot copy from virtual device %2 to virtual device %3 stopped.
- 11562 Console (%1): License %2 added.
- 11564 Console (%1): License %2 removed.
- 11570 Console (%1): Set %2 to Fibre Channel mode %3.
- 11573 Console (%1): Fibre Channel device %2 assigned to %3.
- 
- 11576 Console (%1): Fibre Channel device %2 unassigned from %3.
- 11580 Console (%1): Set %2 Fibre Channel Properties.
- 11582 Console (%1): Set NAS option to %2.
- 11583 Console (%1): Failed to update Fibre Channel client (%2) WWPNS.
- 11584 Console (%1): Fibre Channel client (%2) WWPNS updated.
- 11586 Console (%1): Set Fibre Channel option to %2.
- 11588 Console (%1): Virtual device %2 demoted to a replica.
- 11595 Console (%1): Set Email Alerts option to %2.
- 11597 Console (%1): Set hostedbackup option to %2.
- 11598 Console (%1): Failed to set hostedbackup option %2 because of conflicting adapter number %3.
- 11599 Console (%1): Set NDMP option to %2.
- 11600 [Task %1] Notified client IP %2 virtual device %3 snapshot ready.
- 11601 [Task %1] Notify client IP %2 virtual device %3 snapshot ready %4.
- 11602 [Task %1] Notified client IP %2 virtual device %3 snapshot taken.
- 11603 [Task %1] Notify client IP %2 virtual device %3 snapshot taken %4.
- 11604 [Task %1] Snapshot for virtual device %2 is pending for client notification.
- 11606 Console (%1): Selected timemark %2 character device for virtual device %3.
- 11607 Console (%1): Deselected timemark for virtual device %2.
- 11611 Console (%1): Created timeview for device %2 with timemark %3 successfully.
- 11612 Console (%1): TimeMark for device %2 enabled successfully.
- 11614 Console (%1): TimeMark for device %2 disabled successfully.
- 11616 Console (%1): Replication schedule for virtual tape %2 id %3 suspended.
- 11617 Console (%1): Replication schedule for virtual tape %2 id %3 resumed.
- 11620 Created timemark %1 successfully for virtual device %2.
- 11622 Deleted timemark %1 for virtual device %2. capacity: %2 previous reclaimed count: %3.
- 11624 Copied timemark %1 of virtual device %2 as virtual device %3. capacity: %2 previous reclaimed count: %3.

- 
- 11626 Succeeded to rollback timemark to timestamp %1 for virtual device %2. capacity: %2 previous reclaimed count: %3.
- 11628 Auto delete group member timemark %1 for virtual device %2.
- 11630 Expand snapshot storage for virtual device %1.
- 11634 Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec autoRecoveryInterval: %3 sec> has been set.
- 11635 Console (%1): Failover option on secondary server <heartbeatInterval: %2 sec autoRecoveryInterval: disabled> has been set.
- 11647 Virtual device id %1 snapshot resource usage is now %2 percent (target threshold %3 percent). total objects deleted: %2 total time elapsed: %3.
- 11664 Console (%1): Enable backup for virtual device %2.
- 11666 Console (%1): Disable backup for virtual device %2.
- 11669 Console (%1): Stopped active backup sessions for virtual device %2.
- 11670 Console (%1): Virtual device %2 joined snapshot group %3 group id %4.
- 11671 Console (%1): Virtual device %2 leaved snapshot group %3 group id %4.
- 11674 Console (%1): Virtual tape %2 is in replication session.
- 11675 Console (%1): Virtual device %2 is in backup session. total objects freed: %2 total time elapsed: %3.
- 11677 [Task %1] Start snapshot client notification and image creation for virtual device id %2 (and group members).
- 11678 [Task %1] Created snapshot image %2 on virtual device id %3.
- 11680 Console (%1): Cache resource %2 (ID: %3) resumed successfully.
- 11682 Console (%1): Cache resource %2 (ID: %3) suspended successfully.
- 11685 Console (%1): %2 Resource %3 (ID: %4) added successfully.
- 
- 11687 Console (%1): %2 Resource %3 (ID: %4) deleted successfully.
- 11689 Console (%1): HotZone resource %2 (ID: %3) resumed successfully.
- 11691 Console (%1): HotZone resource %2 (ID: %3) suspended successfully.
- 11697 Console (%1): Snapshot/TimeMark policy for resource (ID: %2) updated successfully.
- 11700 Console (%1): Reinitialize snapshot resource (ID: %2) for virtual device (ID: %3) successfully and all the previous timemarks are discarded.
- 11702 Virtual Tape Library Emulation option was enabled successfully.
- 11703 Virtual Tape Library Emulation option was disabled successfully.
- 11708 Console (%1): %2 %3(s) created successfully.
- 11713 Console (%1): Replication for %2 %3(s) configured successfully.
- 11718 Console (%1): Replication for %2 %3(s) removed successfully.
- 11723 Console (%1): %2 %3(s) are deleted successfully.
- 11728 Console (%1): %2 %3(s) are promoted successfully.

- 
- 11730 Console (%1): Replication properties for %2 %3(s) are updated successfully. is offline. This may compromise SIR node failure protection. Check the storage connectivity.
  - 11732 Console (%1): Replica properties for %2 %3(s) are updated successfully. is now online.
  - 11733 Console (%1): Virtual library %2 created successfully. Target Server: %3 Virtual Tape Replica: %4.
  - 11737 Console (%1): %2 virtual tape drives created successfully.
  - 11743 Console (%1): %2 %3(s) are promoted with testmode successfully.
  - 11750 Console (%1): Add Virtual Tape Library Emulation option successfully.
  - 11751 Console (%1): Remove Virtual Tape Library Emulation option successfully.
  - 11752 Console (%1): Set Multi-Node group configuration for group %2 members %3 successfully. Remote Server: %3 Tape Replica: %4.
  - 11762 Console (%1): Activated license (%2) successfully.
  - 11763 Console (%1): Failover was removed successfully.
  - 11780 Tape id %1 [%2] is enabled with auto-replication move mode and will be deleted in %3 at about %4. Remote Server: %3 Tape Replica: %4.
  - 11781 The scheduled deletion for virtual tape id %1 is cancelled.
  - 11792 Virtual tape %1 is resized to %2 MB successfully. Remote Server: %5 Tape Replica: %6)
  - 11794 FC client %1 VSA mode is changed from %2 to %3.
  - 11795 FC client %1 Celerra mode is changed from %2 to %3.
  - 11800 Reserved
  - 11801 IPStor Server Linux Class
  - 11802 IPStor Server Unix Class
  - 11803 DynaPath Agent
  - 11804 Snapshot Agent
  - 11805 Capacity-On-Demand
  - 11806 SERVivor Agent
  - 11807 IPStor Client
  - 11808 IPStorSentry
  - 11810 Service Enable Disk Option
  - 11811 Server base license
  - 11812 Replication Option
  - 11813 TimeMark Option
  - 11814 IBM 3494 Option
  - 11815 IBM ISERIES Option
  - 11816 Hosted Backup Option
  - 11817 Mirroring Option
  - 11818 NDMP Option
  - 11819 High Availability Option

- 
- 11820 SAN/IP Protocol Option
  
  - 11821 Unlimited CPU
  - 11822 Up to 2 CPUs
  - 11823 Up to 4 CPUs
  - 11824 Up to 8 CPUs
  - 11825 Up to 16 CPUs
  - 11826 Up to 32 CPUs
  - 11827 Up to 64 CPUs
  - 11828 Fibre Channel Protocol Option
  - 11829 iSCSI Protocol Option
  - 11830 ACSLS/LS Library Option
  - 11831 OS: All
  - 11832 OS: Linux
  - 11833 OS: Solaris
  - 11834 OS: AIX
  - 11835 OS: HP-UX
  - 11836 OS: Windows
  - 11837 OS: True64
  - 11838 OS: NetWare
  - 11839 OS: Mac
  - 11841 Application: All
  - 11842 Application: Oracle
  - 11843 Application: Exchange
  - 11844 Application: Microsoft SQL
  - 11845 Application: Sybase
  - 11846 Application: Lotus Notes
  - 11851 Protocol: All
  - 11852 Protocol: SAN/IP
  - 11853 Protocol: Fibre Channel
  - 11854 Protocol: ISCSI
  - 11861 Edition: Enterprise
  - 11862 Edition: Departmental or a change in a virtual device.
  - 11863 Edition: eLite
  - 11868 Virtual Tape Library Option
  - 11869 Bare Metal Recovery Option
  - 11870 FalconStor

- 
- 11871 Network PeripheralsInc.
  - 11872 Runtop
  - 11873 Accton
  - 11874 ASSC
  - 11875 Dot Hill
  - 11876 AnexTek
  - 11877 ECCS
  - 11878 ADTX
  - 11879 NEC
  - 11880 MTI
  - 11881 Driveline
  - 11882 INLINE
  - 11883 Beijing Soul
  - 11884 BestCom
  - 11885 TiGi
  - 11886 Unknown
  - 11890 Async Mirror Option
  
  - 11891 Worm Tape Option
  - 11892 Tape Library Option
  - 11893 HotZone Option
  - 11894 Tape Encryption Option
  - 11895 SCSI Option
  - 11896 4 Target Ports Option
  - 11897 8 Target Ports Option
  - 11898 Write Coalescing Option
  - 11899 Virtual Tape Library Cache Option
  - 11905 Directory %1 created.
  - 11911 Report file %2 (type %1) created.
  - 11912 %1 property set for the IPStor server.
  - 12000 IPStor logger started.
  - 12001 IPStor logger stopped.
  - 12500 Set virtual library %1 properties successfully.
  - 12510 Moved tape in library %1 from slot %2 to drive %3 successfully.
  - 12513 Set disk capacity threshold successfully.
  - 12515 Restarted job %1 successfully.
  - 12520 Moved tape in library %1 from drive %2 to slot %3 successfully.

- 
- 12524 Changed firmware revision to %1 for %2 successfully.
  - 12526 Reclaimed tape %1 successfully.
  - 12528 Enabled IBM 3494 library for %1 successfully.
  - 12530 Moved tape in library %1 from slot %2 to slot %3 successfully.
  - 12533 Set IBM 3494 configuration successfully.
  - 12537 Submitted import job from physical library %1 for %2 to virtual library %3 for %4 successfully.
  - 12539 Submitted export job to physical library %1 for %2 successfully.
  - 12541 Submitted import job from physical drive %1 to virtual library %2 for tape %3 successfully.
  - 12543 Reset physical library %1 successfully.
  - 12544 Set compression successfully.
  - 12549 Cancelled job %1 successfully.
  - 12552 Succeeded to hold job %1.
  - 12555 Resumed job %1 successfully.
  - 12558 Succeeded to hold job %1.
  - 12560 Resumed job %1 successfully.
  - 12562 Set tape caching policies for tape %1 successfully.
  - 12563 Inventoried physical library %1 successfully.
  - 12566 Moved tape in library %1 from ieslot %2 to slot %3 successfully.
  - 12568 Moved tape in library %1 from slot %2 to ieslot %3 successfully.
  - 12572 Assigned vid:%1 scsi:%2 lun:%3 to Hosted BackupClient successfully.
  - 12574 Unassigned vid:%1 scsi:%2 lun:%3 from HostedBackupClient successfully.
  - 12577 Added acsls lib to physical library %1 successfully.
  - 12582 Scanned stacking physical tape %1 successfully.
  - 12584 Submitted job to export stacking virtual tapes to physical library %1 successfully.
  - 12589 Submitted job to import stacked tapes from %1 to %2 successfully.
  - 12591 Purged job %1 successfully.
  - 12593 Set tape properties for %1 successfully.
  - 12595 Set tape properties with mask %1 for %2 successfully. timeout set to %2.
  - 12597 Set rescheduled job successful.
  - 12599 Purged physical tape %1 from database successfully.
  - 12602 Loaded ejected tape for virtual drive %1 successfully.
  - 12604 Assigned ACSLS/LS physical drive %1 successfully.
  
  - 12606 Ejected physical tapes successfully.
  - 12608 Succeeded to enter ACSLS/LS physical tapes.
  - 12610 Assigned physical tape %1 to vtl category successfully.

---

13000 IPStor Failover Module started --[Primary %1 IP %3  
13001 The IPStor Console has requested that this server take over for the primary server.  
13002 Transferring primary static configuration to secondary.  
13003 Transferring primary dynamic configuration to secondary.  
13004 Transferring primary credential information to secondary.  
13005 Taking over tasks for the primary server.  
13006 The primary IPStor Server is recovering.  
13007 Restoring this server to its original configuration.  
13008 IPStor Failover Module stopped.  
13009 Synchronizing the IPStor configuration with the primary server.  
13103 The system times of the failover pair differ by more than %1 second(s).  
13500 IPStor Self-Monitor Module started --(Self check interval: %1 seconds)  
13501 all IPStor related processes and resources function normally  
13502 Take back the virtual IP address: %1.  
13504 Stopping Self-Monitor module.  
13600 Releasing virtual IP address: %1.  
13801 Secondary server will take over primary server operation.  
13802 Manual failover initiated.  
13803 Primary acknowledged takeover request. Resources are released.  
13804 Quorum disk failed to release to secondary.  
13805 Virtual drives released successfully.  
13808 IP address released successfully.  
13809 Failover completed successfully.  
13810 Primary server restored. Waiting for failback.  
13811 Primary server failback initiated.  
13812 Server IP address added successfully.  
13814 Quorum disk returned to primary.  
13815 Virtual drives added successfully.  
13816 Primary server restored.  
13824 Environment variable ISFCFORPCTO set to %1  
13825 Environment variable ISFOQUORUMREQ set to %1  
13826 Environment variable ISFOQUORUMCON set to %1  
13828 Almost running out of file handlers (current %1 max %2)  
13829 Almost running out of memory (current %1 K max %2 K)  
13831 Get configuration file from storage successful.  
13832 Primary server operation is resumed either by user initiated action or secondary server is suspended.  
13837 Configuration files retrieved from repository successfully.

- 
- 13838 Successfully copy file out from Quorum repository.
  - 13839 Secondary server initiated failback to primary (%1).
  - 13840 Secondary server will take over (%1).
  - 13846 Force takeover is initiated. Secondary will perform SCSI reserve to lock the storage.
  - 13847 Secondary server is performing SCSI release to storage.
  - 13852 Secondary server is being requested to release its own resources during takeover %1
  - 13853 Secondary notified primary to go up because secondary is unable to take over.
  - 13854 Secondary suspended failover for %1 min.
  - 13855 Secondary resumed failover.
  - 13865 Primary server will resume due to user initiated action.
  - 13867 Primary server is resuming and forcing device reset to clear SCSI reservation
  
  - 13868 Secondary server takeover unilaterally. All resources will be released. Primary server reboot is required for recovery.
  - 13869 Removing schedule %1 for failover process clean-up.
  - 13870 Schedule removal completed
  - 13871 Primary server failure condition still exists: %1
  - 13872 Waiting for primary to acknowledge takeover request. May take approx. %1 sec.
  - 13873 Waiting for primary to release resources. May take approx. %1 sec.
  - 13874 NAS option is enabled. Takeover may need more than %1 min. to complete.
  - 13875 Primary server is starting to activate virtual drives.
  - 13876 Primary server has completed activating virtual drives.
  - 13877 Secondary server failed to take over.
  - 13880 Primary server will recover its own resources due to secondary server failover suspend.
  - 13881 Primary server failover status change to %1.
  - 14002 Succeeded to rename the virtual device %1.
  - 14007 Succeeded to rename vdev %1 to %2.
  - 14009 Succeeded to rename pdev %1 to %2.
  - 14012 Succeeded to rename client %1 to %2.
  - 14013 Shrink %1 to %2 MBytes.
  - 14014 Console (%1): Virtual tape %2 removed.
  - 14015 Console (%1): Renew caching tape id %2.
  - 14022 Succeeded to erase the physical disk(acsl=%1).
  - 14024 Succeeded to claim the physical disk(acsl=%1).
  - 14026 Succeeded to enable physical device(id=%1).
  - 14028 Succeeded to disable physical device(id=%1).
  - 15001 Snapshot copy from virtual device id %1 to id %2 started.

- 
- 15007 Snapshot copy from virtual device id %1 to id %2 finished.
- 15017 Timemark copy from virtual device id %1 snapshot image %2 to id %3 started.
- 15023 Timemark copy from virtual device id %1 snapshot image %2 to id %3 has finished.
- 15033 Timemark rollback virtual device id %1 to snapshot image %2 started.
- 15039 Timemark rollback virtual device id %1 to snapshot image %2 has finished.
- 17021 Replication failed due to VIT status of tape
- 18051 SIR: Initiating Space Reclamation total object count: %1
- 18052 SIR: Initiating Index Pruning total object count: %1
- 18053 SIR: Initiating Data Disk Space Reclamation total object count: %1 EC %2
- 18054 SIR: Index Reclamation has started successfully. EC %2
- 18056 SIR: Index Reclamation initial survey completed total tapes to check: %1.
- 18057 SIR: Index Reclamation is in progress; completed approximately %1. SrcEle %2  
DestEle %3
- 18058 SIR: Index Reclamation completed total objects checked: %1;
- 18059 SIR: Storage Reclamation has started successfully.
- 18061 SIR: Storage Reclamation in progress. Approximate percent completed: %1
- 18062 SIR: Storage Reclamation completed. Total free blocks: %1 Total time elapsed: %2
- 18063 SIR: Index pruning has started successfully.
- 18064 SIR: Index pruning is in progress; completed approximately %1.
- 18065 SIR: Index pruning completed total objects checked: %1
- 18100 SIR: Execute: %1
- 18102 SIR: This standby server has shut down the failed SIR node %1 using IPMI at IP  
address %2 as prerequisite to take over that node. BC %3
- 18103 SIR: This standby server has successfully taken over the failed SIR node %1. Fix and  
restore the failed SIR node.
- 18115 SIR: This standby server now sees the physical device %1 [%2] used for SIR storage.
- 18117 SIR: This standby server detected the physical device %1 [%2] used for SIR storage
- 
- 19000 The replication configuration has been created successfully. Primary Server: %1 Virtual  
Tape: %2
- 19001 The failover configuration has been created successfully. Primary Server: %1  
Secondary Server: %2
- 19002 The Snapshot Resource of the %1 Resource: %2 (ID: %3) has been expanded by the  
Administrator from %4 MB to %5 MB successfully. VLib slot %3 DestTape [%4] SrcTape  
[%5] Throughput %6 MB/min
- 19050 [Remote Copy] The configuration for remote copy has been set up successfully. Server:  
%1 Virtual Tape: %2
- 19051 [Remote Copy] The copying of the virtual tape %1 to the remote server has been  
started.0.05

- 
- 19052 [Remote Copy] The copying of the virtual tape %1 to the remote server has finished. Slot %3 DestTape [%4]0.05
- 19053 [Remote Copy] The configuration for remote copy is removed. Server: %1 Virtual Tape: %2 Slot %3 DestTape [%4]0.05
- 19054 [Remote Copy] The replica of the virtual tape %1 has been moved to the virtual library %2 on the remote server successfully.
- 19055 [Remote Copy] The virtual tape has been copied to the remote server successfully. Server: %1 Virtual Tape: %2
- 19067 [Remote Copy] The copying of the virtual tape %1 to the remote server has been added into replication job queue.
- 19069 [Auto Replication] The virtual tape %1 is without any physical segments auto replication cannot proceed.
- 19070 The request for %1 to create replica cannot proceed. If not the max number of replica will be exceeded.
- 19071 The request for %1 to create replica cannot proceed. If not the max number of virtual devices will be exceeded.
- 19203 Console (%1): Key %2 has been created successfully.
- 19205 Console (%1): Key %2 has been deleted successfully.
- 19207 Console (%1): Information for key %2 has been updated successfully.
- 19209 Console (%1): Key package %2 has been created successfully.
- 19212 Console (%1): %2 keys from key package have been saved successfully.
- 19213 Maximum tape count licensed has been reached on server %1. Reduce creation tape count to %2.
- 19214 Console (%1): IPMI power control is enabled.
- 19215 Console (%1): IPMI power control is disabled. EC %4
- 19216 Console (%1): This machine does not support IPMI.
- 20000 SAN/IP driver started.
- 20001 SAN/IP driver stopped.
- 21000 SAN SCSI driver started.
- 21001 SAN SCSI driver stopped.
- 22000 Fibre Channel Authentication started with %1.
- 22002 Fibre Channel Authentication stopped with %1.
- 25000 %1 started.
- 25002 %1 paused.
- 25004 %1 resumed.
- 25006 %1 stopped.
- 25008 %1 shutdown.
- 25009 %1 starting.
- 25010 %1 stopping.
- 26210 Both %1 and %2 have the same disk signature (%3).

---

29101 IPStor Server '%1' failed over.

29102 IPStor Server '%1' recovered from failover.

29301 Taking a snapshot of IPStor Server '%1' device %2.

29302 Snapshot of IPStor Server '%1' device %2 was taken.

29401 Backing up IPStor Server '%1' device %2.

29402 Backed up IPStor Server '%1' device %2.

31001 IPStor NAS synchronization module started.

31002 IPStor NAS synchronization module stopped.

31007 NAS mode changed to %1.

31008 Unmounting file system %1.

31009 Share created on %1.

31010 Share deleted on %1.

31014 Adding mount %1.

31015 Deleting mount %1.

31016 Formatting disk %1.

31018 Resize file system %1. SrcTape [%3] DestTape [%4]

31019 IPSTORMOUNT: %1 mounted.0.04

31021 IPSTORNASMGTD: New user added to the authenticating server/domain. SrcTape [%3] DestTape [%4]

31022 IPSTORNASMGTD: Resynchronizing user database.

31026 Delete virtual device %1.

31027 Add virtual device %1.

31033 Device %1 renamed to device %2.

31038 NAS debug level changed to %1.

31057 All NAS resources unmount successfully.

31059 All NAS resources mounted successfully.

31070 Convert file system of device %1 from %2 to %3

40000 TLE Module Started

40001 TLE Module Stopped

40012 Unsupported SCSI command %1

40024 Import job %1 completed successfully VLib VID %2

40025 Export job %1 completed successfully. SrcTape [%2] DestTape [%3] Throughput %4 MB/min

40026 Export Job %1 submitted to Physical Library %2. SrcTape [%3] DestSlot [%4]

40027 Direct Access Import completed successfully. VLib VID %1 Physical Drive VID %2

40028 Import job submitted. Job id %1 VLib VID %2

40033 Export job %1 active. Tape Drive used %2

- 
- 40034 Import job %1 active. Tape drive used %2
  - 40035 Successfully attached to repository %1
  - 40037 Physical Library assigned to exclusive use for TLE. Vid %1 [%2][%3]
  - 40038 Physical Library unassigned. Vid %1 [%2][%3]
  - 40041 Physical Tape Drive assigned to exclusive use for VTL. VID %1 [%2][%3]
  - 40042 Physical Tape Drive unassigned. Vid %1 [%2][%3]
  - 40052 Inventory of Physical Library %1 completed successfully
  - 40053 Virtual Library %1 initialized. [%2][%3]
  - 40054 Virtual Tape Drive %1 initialized. [%2][%3]
  - 40055 Virtual Tape Drive %1 deleted from Virtual Library %2
  - 40056 Virtual Tape Drive %1 created successfully in Virtual Library %2
  - 40057 Virtual Library %1 created successfully. [%2][%3]
  - 40058 Virtual Library %1 deleted successfully. [%2][%3]
  - 40059 Virtual Tape added to Virtual Library %1 slot %2. Total Tapes in Library: %3. %4 %5
  - 40060 Stand alone Virtual Tape Drive %1 created successfully. [%2][%3]
  - 40061 Stand alone Virtual Tape Drive %1 deleted. [%2][%3]
  
  - 40062 Virtual Tape %1 moved to vault from device %2
  - 40063 Virtual Tape %1 from vault imported to Virtual Library %2 slot %3
  - 40064 Virtual Tape %1 from vault imported to Virtual Tape Drive %2
  - 40072 Properties of Tape %1 has been changed. Barcode %2 MaxCapacity %3 MB
  - 40073 Tape Created in Stand Alone Virtual Tape Drive. Tape VID %1 Drive VID %2
  - 40075 Export Job %1 submitted to Physical stand alone Tape Drive %2 SrcTape [%3] hardware complete code [%3] while writing tape to [%4] VID [%5]
  - 40079 Deleted tape marked for delayed deletion. Tape [%1] VID %2 hardware complete code [%3] while reading tape from [%4] VID [%5]
  - 40107 %1: Successfully mounted %2 on drive %3
  - 40108 %1: Successfully dismounted %2 from drive %3
  - 40115 Please add tapes.
  - 40119 Global [%1] Compression %2 on Repository %3
  - 40122 Export Job %1 submitted to Physical Library %2. SrcTape [%3] DestTape [%4] DestSlot [%5]0.06
  - 40125 Disk space allocated for tape VID %1 Barcode [%2] in library VID %3 has been reclaimed successfully BC %3
  - 40127 Disk space allocated for tape VID %1 Barcode [%2] in vault has been reclaimed successfully
  - 40129 No Free physical drive to load direct link tape VID %1 BarCode [%2].
  - 40131 The tape shredding job is successful on the tape [%1].

---

40138 Scan job %1 completed successfully SrcTape [%2]  
40139 Stack Import job %1 completed successfully VLib VID %2  
40140 Stack Export job %1 completed successfully. DestTape [%2] Throughput %3 MB/min  
40144 Physical Tape Database with capacity %1 is reaching maximum capacity %2  
40145 Scan Job %1 submitted to Physical Library %2. SrcTape [%3] Slot [%4]  
40146 Stack Export Job %1 submitted to Physical Library %2. Destination Physical Tape [%3]0.04  
40147 Stack Export Job %1 submitted to Physical Library %2. Destination Physical Tape [%3]0.04  
40149 Stack Export job %1 active. Tape Drive used %2  
40150 Stack job submitted. Job id %1 VLib VID %2  
40151 Stack Import job %1 active. Tape drive used %2  
40157 ACSLS/LS: Successfully ejected %1 from %2 %3 CAP %4.  
40160 ACSLS/LS: Successfully entered %1 from %2 %3 CAP %4.  
40169 FiberChanel: Target mode is enabled on WWPN [%1]. SrcTape [%3] Throughput %4 MB/min  
40170 FiberChanel: Target mode is disabled on WWPN [%1].  
40171 Start tape shredding on tape [%1] VID:%2. SrcTape [%3]  
40181 TapeDuplication: Job %1 -Master tape duplication job is created. The job will copy data from tape [%2] to physical tape [%3] on physical library %4. SrcTape [%3]  
40182 TapeDuplication: Job %1.%2.%3 -An extra tape copy job is created. The job will copy data from tape [%4] to physical tape [%5] on physical library %6. SrcTape [%3] DestTape [%4]  
40192 No operation can be performed on the physical library [ %1 ] -The physical library is disabled.  
40196 Repository consistency check completed  
50001 iSCSI: Login request to target %1 from initiator %2.  
50100 Failed to start replication --replication is already in the power management queue for virtual tape %2.  
50101 SIR Cluster: Checking fibre channel connectivity from %1 to %2  
50102 SIR Cluster: Creating the quorum device on %1  
  
50103 SIR Cluster: Creating the scratch device on %1 Slot %3 DestTape [%4]0.05  
50104 SIR Cluster: Creating repository index storage %1 on %2  
50105 SIR Cluster: Creating repository data storage %1 on %2  
50106 SIR Cluster: Setting up cluster %1 for node(s): %2  
50107 SIR Cluster: Creating storage pool for repository storage on %1  
50108 SIR Cluster: Adding repository storage to storage pool on %1  
50109 SIR Cluster: Setting up security from %1 to %2

---

50110 SIR Cluster: Checking repository devices on %1  
50112 SIR Cluster: Configuring storage connection from %1 to %2  
50113 SIR Cluster: Changing root password on %1  
50114 SIR Cluster: SIR cluster %1 is created and configured successfully on %2  
50116 SIR Cluster: Setting up cluster on %1  
50201 SIR: Associating SIR cluster %1 with VTL.  
50202 SIR: Creating tape drives for SIR cluster %1.  
50203 SIR: Checking tape drive connectivity for SIR cluster %1.  
50205 SIR: Configuring storage connection from SIR cluster %1 to VTL.  
50207 SIR: SIR cluster %1 association added and configured successfully.  
50208 SIR: SIR cluster %1 checked for new disks successfully.  
50209 SIR: SIR cluster %1 association removed successfully.  
50210 SIR: SIR is configured successfully on server %1.  
50211 SIR: SIR is disabled successfully on server %1.  
50300 SIR Replication: Setting up replication from SIR cluster %1 to SIR cluster %2  
50301 SIR Replication: Configuring repository storage connection from %1 to %2 SrcTape [%3] DestTape [%4]  
50302 SIR Replication: Setting up iSCSI user account on %1  
50303 SIR Replication: Configuring iSCSI initiator on %1  
50304 SIR Replication: Checking repository devices on %1  
50306 SIR Replication: Creating storage pool for repository storage on %1  
50307 SIR Replication: Adding repository storage to storage pool on %1  
50308 SIR Replication: Setting up replication on %1  
50309 SIR Replication: Replication from SIR cluster %1 to SIR cluster %2 set up successfully  
50500 RDE: Policy %1 saved successfully.  
50502 RDE: Policy %1 deleted successfully.  
50504 RDE: Policy %1 Tape [%2] [%3] started at end of backup. Total data: %4.  
50506 RDE: Tape %1 unloaded from drive after scanning %2.  
50508 RDE: Policy %1 started %2. Total tapes: %3; Tapes with new data: %4; Total data: %5.  
50510 RDE: Policy %1 has completed successfully. Total time for policy: %2.  
50513 RDE: Policy %1 is still active. Execution skipped.  
50515 RDE: Policy %1 Tape [%2] scan completed. Total data: %3; Unique data: %4; De-dupe ratio: %5; Scan time: %6.  
50517 RDE: Policy %1 Tape [%2] scan process interrupted by other request.  
50518 RDE: Policy %1 Tape [%2] is being accessed by backup client. Scanning is suspended. hardware complete code [%3] while accessing tape [%4] VID [%5].  
50520 RDE: Policy %1 Tape [%2] scan process resumed.  
50524 RDE: Policy %1 Tape [%2] replication completed. Total data: %3; Unique data: %4; Replication time: %5.

- 
- 50528 RDE: Policy %1 Tape [%2] has no new data to process.
  - 50530 RDE: Policy %1 Tape [%2] index replication completed. Index data replicated: %3.
  - 50532 RDE: Policy %1 Tape [%2] has no new index information to replicate.
  - 50533 RDE: Policy %1 Tape [%2] has no new unique data to replicate.
  - 50535 RDE: Policy %1 Replication: Total tapes: %2; Total data: %3; Unique data: %4; Total dedupe ratio: %5.
  
  - 50536 RDE: Policy %1 tape scan: Total tapes: %2; Total data: %3; Unique data: %4; Total dedupe ratio: %5.
  - 50537 RDE: Space Reclamation started successfully for SIR Cluster '%1' session(s): %2. EC %3
  - 50540 RDE: Initial index tape survey completed successfully for Space Reclamation session %1.
  - 50543 RDE: Policy %1 Tape [%2] replicating to '4.6 ALL IN ONE' display of resolving status and statistics not supported.
  - 50545 RDE: Space Reclamation on Tape %1[%2] started; %3 of %4 tapes.
  - 50547 RDE: Space Reclamation found %1 non-empty VIT tapes.
  - 50548 RDE: Policy %1 : %2 tapes are skipped because they are either in-use or no new data. stubtape=%3 -Mark the tape as READ ONLY
  - 50555 RDE: Space reclamation has been triggered and will be processed momentarily on SIR cluster %1. COD=%3
  - 50556 SIR Replication: Reuse Tape %1 in vault as Local Index Tape for Replica Index Tape %2 same barcode [%3] and name [%4].
  - 50558 RDE: Policy %1 Tape [%2] has been added into queue for deduplication at the end of backup.
  - 50559 RDE: Policy %1 Tape [%2] replication has started.
  - 50560 RDE: Policy %1 Tape [%2] has finished backup and will be processed once its current replication session has completed.
  - 50562 RDE: Policy %1 Tape [%2] replication has been postponed because currently not within the replication time range [%3].
  - 50701 SIR Scanner: Tape scan started successfully for Tape %1 in Drive %2
  - 50703 SIR Scanner: Tape format for Tape %1 in Drive %2 is %3
  - 50704 SIR Scanner: Tape format for Tape %1 in Drive %2 is not recognized; Generic format is assumed with following additional details: %3
  - 50705 SIR Scanner: Create SIR folder for Tape %1 in Drive %2
  - 50708 SIR Scanner: Tape %1 scan completed successfully in Drive %2; Time elapsed: %3 second; Total data: %4; Redundancy elimination ratio: %5
  - 50711 SIR Scanner: Tape %1 in Drive %2 is being accessed by a backup client; Scanning suspended
  - 50712 SIR Scanner: Tape %1 scan is resumed in Drive %2

- 
- 50713 SIR Scanner: Tape %1 in Drive %2 has been converted to Virtual Index Tape successfully
  - 50715 SIR Scanner: SCSI sense data: %1
  - 50716 SIR Scanner: Tape %1 in Drive %2 is empty
  - 50717 SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 started successfully
  - 50718 SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 finished successfully
  - 50720 SIR Scanner: Generic parsing has been invoked for Block at %1 Tape %2
  - 50721 SIR Scanner: Generic parsing has been invoked for Tape %1 Drive %2
  - 50801 SIR Replication: Index tape replica data confirmation started successfully for Tape %1 in Source Drive %2 and Destination Drive %3
  - 50804 SIR Replication: Index tape replica processing completed successfully for Tape %1 in Source Drive %2 and Destination Drive %3; Time elapsed: %4; Total data: %5; Redundancy elimination ratio: %6
  - 50901 SIR Client: SIR initialization started
  - 50903 SIR Client: SIR client initialized successfully
  - 50904 SIR Client: Folder %1 creation requested
  - 50905 SIR Client: Folder %1 closed successfully
  - 50951 SIR Server: Server initialization started
  - 50953 SIR Server: Server initialized successfully
  - 50957 SIR Server: Configuration file is missing
  - 51001 SIR Failover: Failover has been set up successfully on %1.

---

## Warning Messages

- 1022 Replication has failed for virtual tape %1 --%2.
- 1061 I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): %1; New path (A.C.S.L): %2
- 1082 Replication for virtual tape %1 has been cancelled by user or other operation.
- 1083 Replication for group %1 has been cancelled by user or other operation.
- 1201 Kernel memory is low. Add more memory to the system if all possible! Restart the host if possible.
- 1208 Path %1 does not belong to active path group.
- 1210 No valid path is available for device %1.
- 1211 No valid group is available.
- 1212 No active path group found. Storage connectivity failure. Check cables switches and storage system to determine cause. GUID: %1.
- 1216 T300 storage path trespassing.
- 1217 HSG80 storage path trespassing.
- 1218 MSA1000 storage path trespassing.
- 7004 Patch %1 installation failed --it has already been applied.
- 7008 Patch %1 rollback failed --there is no original file to restore.
- 10200 Configuration %1 exists.
- 10201 Overwriting existing configuration %1.
- 10210 Marked Physical Device [%1] OFFLINE because its GUID: %2 does not match scsi GUID: %3.
- 10211 Marked Physical Device [%1] OFFLINE because its wwid %2 does not match scsi wwid %3 [GUID: %4].
- 10212 Marked Physical Device [%1] OFFLINE because scsi status indicate OFFLINE [GUID: %2].
- 10213 Marked Physical Device [%1] OFFLINE because it did not respond correctly to inquiry [GUID: %2].
- 10214 Marked Physical Device [%1] OFFLINE because its GUID is an invalid FSID [GUID: %2].
- 10215 Marked Physical Device [%1] OFFLINE because its storage capacity has changed [GUID: %2].
- 10248 Remove all scsi alias from %1.
- 10249 Remove missing scsi alias %1 from %2.
- 10250 Remove scsi alias %1 from %2 because their categories are different.
- 10251 Remove scsi alias %1 from %2 because their GUIDs are different.
- 10497 0.01
- 11007 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. IPStor requires %2 MB of disk space to continue.

- 
- 11300 Invalid user name (%1) used by client at IP address %2.
  - 11301 Invalid password for user (%1) used by client at IP address %2.
  - 11302 Invalid passcode for machine (%1) used by client at IP address %2.
  - 11303 Authentication failed in stage %1 for client at IP address %2.
  - 11408 Synchronizing the system time with %1. A system reboot is recommended.
  - 11644 Take timeview %1 id %2 offline because the source timemark has been deleted.
  - 11646 Delete timemark %1 on virtual device %2 to maintain snapshot resource threshold.
  - 11679 Console (%1): Virtual device %2 is a snapshot image copying target.
  - 11793 Appliance Hardware Problem: %1.
  - 11908 File %1 does not exist.
  - 12006 Log size warning.
  - 13503 No heartbeat request detected for %1 seconds.
  
  - 13710 The Live Trial period has expired for IPStor Server %1. Please contact FalconStor or its representative to purchase a license.
  - 13711 The following options are not licensed: %1. Please contact FalconStor or its representative to purchase a license.
  - 13820 Failed to detect primary server heartbeat.
  - 13822 Secondary will not take over because storage connectivity is not 100%.
  - 13823 Primary failed to acknowledge takeover request in time. Secondary will take over forcefully.
  - 13842 Secondary server will takeover. Primary is still down.
  - 13845 Quorum disk failure detected. Secondary is still in takeover mode.
  - 13848 Primary is already shut down. Secondary will take over immediately.
  - 13849 One of the heartbeat channels is down: IP address: %1.
  - 15008 Snapshot copy from virtual device id %1 to id %2 might have run out of snapshot reserved area. Please expand the snapshot reserved area.
  - 16100 Email Alerts failed to connect to SMTP server %1 on port %2.
  - 16101 Email Alerts failed to send email to SMTP server %1 on port %2.
  - 19004 %1% of total storage is being used. Total storage capacity is %2. Available storage space is %3.
  - 21010 SAN SCSI received an abort request.
  - 21011 SAN SCSI received a reset bus request for a special command.
  - 21012 SAN SCSI received a reset bus request.
  - 21013 SAN SCSI failed to send a SCSI command.
  - 21014 SAN SCSI failed to receive a SCSI reply.
  - 21015 SAN SCSI failed to attach to a virtual device.
  - 21016 SAN SCSI failed to detach from a virtual device.

- 
- 21017 SAN SCSI failed to connect to an IPStor Server.
  - 21018 SAN SCSI received a disconnect request. This may be from the Client Monitor or due to a network failure IPStor Server shutdown/failover
  - 21019 SAN SCSI received an unsupported request.
  - 22003 Fibre Channel Authentication warning from system %1.
  - 29403 Backup of IPStor Server '%1' device %2 failed.
  - 29404 IPStor Notify user specified error %1 description '%2'.
  - 29406 Notify Error waiting on %1.
  - 31052 Failover force mounting %1
  - 31056 Delay mount due to unclean file system on vid %1
  - 31058 Not all NAS resources unmounted successfully.
  - 31060 Not all NAS resources mounted successfully.
  - 31069 Do not destroy file system's superblock of %1
  - 31076 Due to storage failure NAS Secondary Server has to reboot to resume its tasks. %1
  - 31077 NAS device %1 is not complete in iocore during failover processing
  - 40020 Job %1 cancelled
  - 40032 Physical Tape %1 not available to start auto archive job. Waiting for tape...
  - 40080 Tape drive %1 in physical library %2 not accessible. Locked by other party
  - 40081 Tape [%1] in physical library %2 not accessible. Locked by other party
  - 40082 Slot %1 in physical library %2 not accessible. Locked by other party
  - 40083 Inventory physical library %1: Tape [%2] or Slot %3 not accessible. Locked by other party
  - 40084 Tape [%1] is blank. Cannot export blank tapes
  - 40112 Physical Tape %1 is not available in physical library %2 to start tape caching job. Waiting for tape...
  - 40113 A Manual Export job is not allowed because tape <%1> has tape caching set.
  - 40114 The export job is not allowed because physical tape [%1] in library [%2][%3] is being used by tape caching.
  
  - 40120 The tape [%1] has no data. No export/tapestacking job will be submitted.
  - 40121 The direct link tape VID %1 BarCode [%2] has been deleted.
  - 40130 Unable to renew cache for tape VID %1. Data will be redirected to physical tape [%2]. Drive %3
  - 40165 Door opened condition reported on Physical Library VID-%1 %2 %3. Start Block %3 Start Block Offset %4 End Block %5 End Block Offset %6 Total Bytes %7
  - 40166 Tape Alert from device [%1][%2] ACSL %3:%4:%5:%6 -%7
  - 40167 Encryption key %1 does not exist. Decryption/tape writing disabled for tape VID %2.
  - 40168 No license for Virtual Tape Encryption. Decryption/tape writing disabled for tape VID %1.

- 
- 40172 The tape shredding job has been cancelled on the tape [%1] VID:%2.
  - 40175 Encountered metadata inconsistency on Virtual Tape VID %1 [%2]. Write protecting tape. %3
  - 40176 Physical Tape [%1] is not available to start tape duplication job. Set the job %2 to HOLD.
  - 40183 TapeDuplication: Job %1.0.%2 -An extra tape copy job cannot be created due to no more physical libraries with same barcode [%3].
  - 40184 TapeDuplication: Job %1.0.%2 -The tape [%3] will not be deleted after copy job since all copy jobs could not be created.
  - 40185 TapeDuplication: Job %1.0.%2 -The tape [%3] cannot not be reclaimed since not all physical copies were created.
  - 40186 TapeDuplication: Job %1 -The tape [%2] cannot be reclaimed because an extra tape copy job was not completed successfully.
  - 40187 TapeDuplication: Job %1 -The tape [%2] cannot be moved because an extra tape copy job was not completed successfully.
  - 40188 Stack Import job %1 completed: VLib VID %2 SrcTape [%3] Throughput %4 MB/min. [%5] tapes with non unique barcodes not imported.
  - 40189 Scan job %1 completed successfully PhyTape [%2] is not a Stack tape.
  - 40195 The tape [%1] is being deduped at the moment -export job cannot be submitted.
  - 40197 Repository consistency check detected non critical inconsistencies. Check syslog for more information.
  - 40202 TapeProperty: VTL management did not find the tape [%1] VID=%2
  - 40203 TapeProperty: Found tape maximum capacity mismatch on tape [%1] VID=%2 -Mark the tape as READ ONLY
  - 40204 TapeProperty: Found tape allocated size mismatch on tape [%1] VID=%2 -Mark the tape as READ ONLY
  - 40205 TapeProperty: Found stub tape property mismatch on tape [%1] VID=%2
  - 40206 TapePropertyCheckUpCall: Found tape capacity on demand property mismatch on tape [%1] VID=%2
  - 40207 Encountered tape header inconsistency on Virtual Tape [%1] VID [%2]. Write protecting tape.
  - 50512 RDE: Policy %1 has been stopped.
  - 50526 RDE: Policy %1 Tape [%2] unable to load for deduplication. Tape is in a library drive and may be in use. Will retry.
  - 50539 RDE: Cannot start Space Reclamation on SIR Cluster '%1' while a RDE process is currently running.
  - 50542 RDE: Policy %1 Tape [%2] index replication was cancelled: %3.
  - 50544 RDE: Policy %1 Tape [%2] scan process interrupted by emergency stop.
  - 50549 RDE: Policy %1 SIR [%2] is still loading.
  - 50550 RDE: Policy %1 SIR [%2] is inaccessible.
  - 50551 RDE: SIR [%1] is still loading.

- 
- 50552 RDE: SIR [%1] is inaccessible.
  - 50553 RDE: Policy %1 Tape [%2] scan process cancelled by backup client or user.
  
  - 50557 RDE: Policy %1 Tape [%2] unique data replication was cancelled by user or other operation.
  - 50561 RDE: Policy %1 Tape [%2] There are not enough resources available for replication to occur. Replication will start as soon as resources are available.
  - 50710 SIR Scanner: Tape %1 scan has been cancelled in Drive %2
  - 50806 SIR Replication: Index tape replica processing has been cancelled for Tape %1 in Source Drive %2 and Destination Drive %3

# 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 correctly*

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 the <i>Physical Resources</i> object and select <i>Rescan</i> ). Make sure that the <i>Discover New Devices</i> option is specified. Specify a <i>LUN Range</i> that you reasonably expect will include the LUN.  |
| Check system log messages | Check the Event Log or syslog ( <i>/var/adm/messages</i> ) 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> , 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.

### *An HBA port is missing after rebooting and restarting VTL*

Be sure to use the default QLogic HBA modules if the QLogic port is direct-connected to the storage.

Loop mode is required for the storage. The default QLogic driver uses "Loop preferred, then Point-to-Point".

### *Client does not see any devices*

When using a Multi-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.

### *Client cannot see tape library/drive as provisioned by VTL*

Check device discovery by operating system

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 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 a virtual device*

This can have different causes:

- 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.
- If the VTL is shut down for a long period, the devices offered to the clients will time out or be set to *offline*. If this occurs, you will need to perform a rescan from the host machine to regain access.
- ACSLS library users - If you did not select the *Firewall Support* option during configuration, the *portmap* process needs to be running. Otherwise, the system will fail to assign or retrieve the library's status after restarting VTL services or rebooting. To enable *portmap*, you will have to run the following command: `chkconfig --add portmap`

### *VIT tape is marked "Full"*

If you see a VIT marked as "*full*", check the log to see if there was enough disk space available during the backup but before the deduplication process started.

If there was not enough space, the tape is marked as "*full*" and this status is preserved after deduplication. If this occurs, you must use a different tape for backups.

---

## Replication

### *Replication of virtual tapes*

Replication configuration fails with a “Failed to add replication target” error. This can occur if the replica server has a device assigned to it from the primary server. You will need to remove the device assignment before you can create your replication configuration.

### *Replication when a tape is corrupted*

Replication appears to be successful, but you get a message in the Event Log similar to the following: "Encountered metadata inconsistency on Virtual Tape VID #. Write protecting tape".

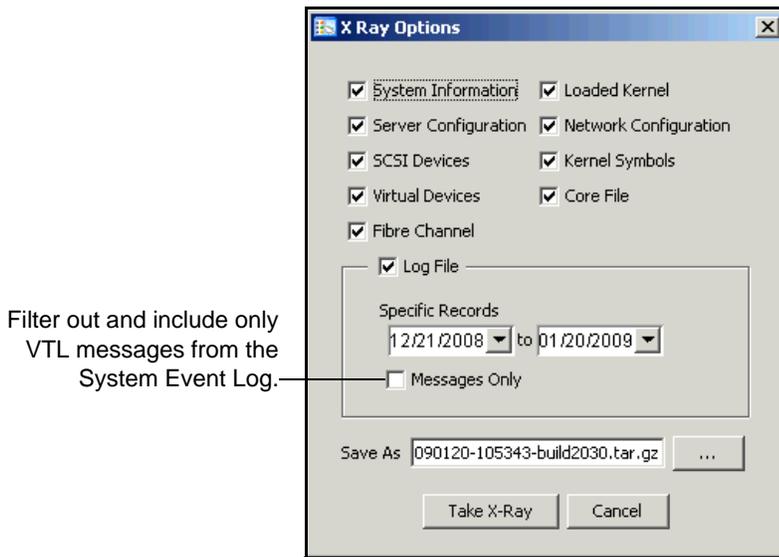
This can be caused due to corruption on the virtual tape. Replication will proceed as long as there are sectors available, even if a tape is corrupted.

## 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 your VTL server and select *Capture 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.

# Error Codes

## VTL Prime Error Codes

No.	Type	Text	Probable Cause	Suggested Action
1005	Error	Out of kernel resources. Failed to get major number for VTL SCSI device.	Too many Linux device drivers are installed.	Type <code>cat /proc/devices</code> for a list to see if any can be removed.
1006	Error	Failed to allocate memory.	Memory leak from various modules in the Linux OS, most likely from network adapter or other third party interface drivers.	Check Knowledge Base for known memory leak problems in various drivers.
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- [Error].	Another application is using UDP port 11577.	Confirm using <code>netstat -a</code> , then remove or reconfigure the offending application.
1023	Error	Failed to connect to physical device [Device number]. Switching to alias to [ACSL].	Adapter/cable problem.	Check for loose or damaged cable on affected drive.
1030	Error	Failed to start replication -- replication is already in progress for virtual tape.	Replication is still in progress when a new replication is manually triggered by a user or started by the scheduler based on the replication policy.	<p>If the replication is manually triggered by the user, check the replication status at the right panel of the replica before starting another replication.</p> <p>If the replication is triggered by the scheduler, adjust the schedule in the replication policy to avoid replicating too often.</p>
1043	Error	A SCSI command terminated with a non-recoverable error condition that was most likely caused by a flaw in the medium or an error in the recorded data.	Most likely caused by a flaw in the medium or an error in the recorded data.	Check the system log for additional information. Contact hardware manufacturer for diagnostic procedure.

No.	Type	Text	Probable Cause	Suggested Action
1044	Error	A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.).	General I/O error that is not medium related. This can be caused by a number of potential failures, including controller failure, device failure, parity error, etc.	Check the system log for additional information. Contact hardware manufacturer for diagnostic procedure.
1061	Warning	I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): [ACSL]; New path (A.C.S.L): [ACSL].	An alias is in use due to primary path failure.	Check primary path from VTL appliance to physical device.
1067	Error	Replication cannot proceed - - unable to connect to replica server.	The primary server cannot connect to the target server. Either there's problem with the network or the target server is busy.	Check if the network is working properly as well as the server activity. If the replication is triggered by the user, wait until the network is working properly or when the server is not as busy.
1069	Error	Replication cannot proceed - - virtual tape [VT#] no longer has a replica or the virtual tape replica does not exist.	The replica of the virtual tape no longer exists on the target server. It might have been removed from the target server while the primary server is not available.	Remove replication setup from the virtual tape console since it no longer has a valid replica.
1084	Error	A SCSI command terminated with a recovered error condition. This may indicate that the device is becoming less reliable. Please check the system log for additional information.	The physical devices, i.e., the SCSI disks or the RAID, returned an error code reporting that the I/O operation initially encountered an error, but was successful after a retry. This may indicate the reliability of the storage device may be questionable.	If possible, determine the true cause of the problem by contacting the hardware manufacturer. If the drive is reaching MTBF*, it may be prudent to replace the drive.
7000	Informational	Patch %1 installation completed successfully.	A patch has been applied to the server.	None.
7001	Error	Patch %1 failed -- environment profile is missing in /etc.	Unexpected loss of environment variables defined in /etc/.is.sh on the server.	Check server package installation.
7002	Error	Patch %1 failed -- it applies only to build %2.	The server is running a different build than the one for which the patch is made.	Get the patch, if any, for your build number or apply the patch on another server that has the expected build number.

No.	Type	Text	Probable Cause	Suggested Action
7003	Error	Patch %1 failed -- you must be the root user to apply the patch.	The user account running the patch is not root user	Run the patch with root account.
7004	Warning	Patch %1 installation failed - it has already been applied.	You tried to apply the patch again.	None.
7005	Error	Patch %1 installation failed - prerequisite patch %2 has not been applied.	Required previous patch is not applied.	Apply the required patch before applying this one.
7006	Error	Patch %1 installation failed - cannot copy new binaries.	Unexpected error on the binary file name or path in the patch.	Contact Tech Support.
7007	Informational	Patch %1 rollback completed successfully.	A patch is rolled back.	None.
7008	Warning	Patch %1 rollback failed -- there is no original file to restore.	Patch has not been applied or already rolled back.	None.
7009	Error	Patch %1 rollback failed -- cannot copy back previous binaries.	Unexpected error on the binary file name or path in the patch.	Contact Tech Support.
7010	Error	Patch %1 failed -- the file %2 has the patch level %3, higher than this patch. You must rollback first %4.	A patch with higher level and conflicting with the current patch has been applied.	Roll back first the high level patch, apply this patch, and then apply again the high level patch.
7011	Error	Patch %1 failed -- it applies only to kernel %2.	Patch applied to a server running on an unexpected OS.	Apply the patch on a server that has the expected kernel.
10001	Error	Insufficient privilege (uid: [UID]).	VTL software is not running with root privilege.	Login as root to the Linux server where VTL is to be running before starting VTL.
10002	Error	VTL Server environment is corrupt.	The configuration file in the / etc directory which provides the VTL home directory and other environmental information is either corrupted or deleted.	Determine the cause of such corruption and correct the situation. Perform regular backups of VTL configuration data so it can be restored if corrupted by known elements.
10003	Error	Failed to initialize configuration[Filename].	During the initialization process, one or more critical processes experienced a problem. This may be due to system drive failure, storage hardware failure, or system configuration corruption.	Check storage device connectivity, check the system drive for errors (use OS provided utilities), and check for VTL environment corruption as described in 10002.

No.	Type	Text	Probable Cause	Suggested Action
10004	Error	Failed to get SCSI device information.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	Check the storage devices for power status, controller status, etc. Check for proper connectivity. Fibre Channel Switch connection status lights do not guarantee a solid connection. Disconnect/Reconnect the Fibre Channel connector for verification. Check the specific storage device using OS provided utilities such as hdparm.
10006	Error	Failed to write configuration[File name].	Error encountered when writing the VTL configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or encountered a hardware failure.	Check the system drive using OS provided utilities. Free up space if necessary. If the drive is unreliable or reaching MTBF*, it may be prudent to replace the drive.
10100	Error	Failed to scan new SCSI devices.	Error occurred when adding newly discovered SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004 for checking storage devices. If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware of software components, restart the server machine to make sure the OS is in a healthy state before trying again.
10101	Error	Failed to update configuration [File name].	Error encountered when updating the VTL configuration file on the system drive. This can only happen if the system drive is corrupted or has failed.	Check the system drive using OS provided utilities.
10102	Error	Failed to add new SCSI devices.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004.

No.	Type	Text	Probable Cause	Suggested Action
10200	Warning	Configuration [File name] exists.	A VTL configuration file already exists when installing the VTL software, possibly from previous installation. The configuration file will be reused.	If there is reason to believe the existing configuration should not be used, e.g.. the file is suspected to be corrupted, then remove the VTL directory before reinstallation.
10210	Warning	Marked virtualized PDev [GUID] OFFLINE, guid does not match SCSI guid [GUID].	A physical device has a different GUID written on the device header than the record in the configuration file. This is most likely caused by old drives being imported without proper initialization, or much unlikely, due to the corruption of the configuration or the device header.	Check the physical connection of the storage, and the storage system. If problem persists, call tech support.
10212	Warning	Marked PDev [GUID] OFFLINE because scsi status indicate OFFLINE.	The physical storage system response indicates the specific device is off-line. It may have been removed, turned off, or malfunctioning.	Check the storage system, including all cabling. Once the problem is corrected, rescan on the adapter with the connected drive. Limit the scope of the scan to that SCSI address.
10213	Warning	Marked PDev [GUID] OFFLINE because it was not detected.	The physical device that exists in the configuration is not responding to commands. Its status is now set to OFF-LINE. All virtual drives affected will also be set to OFF-LINE. Most likely the drive or storage system is turned off, or the cable is disconnected, etc.	Check the storage system, including all cabling. Once the problem is corrected, rescan on the adapter with the connected drive. Limit the scope of the scan to that SCSI address.
10214	Warning	Marked PDev [GUID] OFFLINE because its GUID is an invalid FSID.	The GUID in the header of the drive does not match the unique ID, called the FSID, which is based on the external properties of the physical drive. It maybe caused by drives changed while VTL is down.	Make sure drives are not changed without using the VTL console to eliminate them from the virtual resource list first. Also never allow other applications to directly access the physical drives without going through VTL.
10215	Warning	Marked PDev [GUID] OFFLINE because its storage capacity has changed.	The physical drive geometry, including the number of sectors, is different from the original record.	Rescan the drive to re-establish its properties.

No.	Type	Text	Probable Cause	Suggested Action
10240	Error	Missing SCSI Alias [A,C,S,L].	One of the existing SCSI paths for the device is not accessible. This is most like caused by storage cable being disconnected, or fibre channel switch re-zoning. This can also be caused by failure of one of the storage ports.	Check cabling and storage system. After situation is corrected, rescan the adapter connected to the drive, and limit the scope to that path.
10241	Error	Physical Adapter [Adapter number] could not be located in /proc/scsi/.	The adapter driver could be unloaded.	Check the loaded drivers.
10244	Error	Invalid FSID, device [Device ID] LUN in FSID [FSID] does not match actual LUN.	The FSID is generated with the LUN of the device. Once a device is used by VTL, it is not allowed to have the LUN changed.	Do not change the LUN of a virtualized drive. Revert back to the original LUN.
10246	Error	Fail to generate FSID for device acsl:[A C S L], can't validate FSID.	The physical drive does not present valid data for unique ID generation, even if the inquiry pages exist.	Only use this type of drive for virtual drive, and not SED.
10247	Error	Device (acsl:[A C S L]) GUID is blank, can't validate FSID.	Some process may have erased the disk header. This can be due to the accidental erase by fdisk.	Never access the virtual drives bypassing VTL.
11000	Error	Failed to create socket.	This kind of problem should rarely happen. If it does, it may indicate network configuration error, possibly due to system environment corruption. It is also possible that the network adapter failed or is mis-configured. It is also possible that the network adapter driver is the problem.	Restart the network. If problem persists, restart the OS, or restart the machine (hard/cold reset). If problem still persists, you may need to reinstall the OS. If that is the case make sure you properly save all VTL configuration information before proceeding.
11001	Error	Failed to set socket to re-use address.	System network configuration error, possibly due to system environment corruption.	See 11000.
11002	Error	Failed to bind socket to port [Port number].	System network configuration error, possibly due to system environment corruption.	See 11000.

No.	Type	Text	Probable Cause	Suggested Action
11003	Error	Failed to create TCP service.	System network configuration error, possibly due to system environment corruption.	See 11000.
11004	Error	Failed to register TCP service (program: [Program name], version: [Version number]).	System network configuration error, possibly due to system environment corruption.	See 11000.
11006	Error	VTL communication module Failed to start.	Most likely due to the port for VTL comm module is being occupied by a previous unexpected failure of the communication module, or by another application.	Restart the OS and try again. If problem persists, use the OS provided utilities, such as netstat to check the port used.
11032	Error	Auto save configuration: cannot connect to FTP server port.	FTP sever is not accessible.	Please make sure that FTP server is running and accessible from VTL system.
11033	Error	Auto save configuration: cannot login user.	Incorrect user name or password	Please double check the user name and password specified in the auto save configuration settings.
11034	Error	Auto save configuration: directory doesn't exist.	The target directory specified in the auto save configuration setting doesn't exist on the FTP server.	Please create the specified directory or use an existing directory.
11035	Error	Auto save configuration: failed to copy to FTP server.	The specified FTP user may not have write access to copy files. It can also happen if the FTP server doesn't have enough space.	Please check the user access rights for the FTP user specified in the auto save configuration setting. Also check the free space available on the FTP server.
11036	Error	Auto save configuration: failed to delete old file from FTP server.	The specified user doesn't have rights to delete files on the FTP server.	Please check the access rights of the specified user.
11050	Warning	Cannot start replication for virtual device [VD#] because it's on LUN [L#], which is being migrated.	A replication operation was triggered for a tape that has segments on a LUN that is being migrated.	No specific user action required. Replication will continue at the next scheduled time, after the LUN migration is completed.
11101	Error	SAN Client ([host name]): Failed to add SAN Client.	This error is most likely due to system configuration error, or system resources running low.	Check OS resources using provided utilities such as top.

No.	Type	Text	Probable Cause	Suggested Action
11104	Error	There are too many SAN Client connections.	The number of simultaneous connections exceeded the supported limit the current system resource can handle.	This is an unlikely condition as long as the recommended memory is available for the server.
11112	Error	SAN Client ([host name]): Failed to parse configuration file [File name].	The configuration file is corrupted, or manually tempered to the degree that is no longer recognizable by VTL. If corruption is the cause, then it is most likely due to a system drive hardware error.	If there is a valid configuration file saved, it can be restored to the system. Make sure to use reliable storage devices for any critical system functions.
11114	Error	SAN Client ([host name]): Failed to allocate memory.	System resources are running low. This may be due to too little memory installed for the system, or a runaway process that is consuming too much memory.	Use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system.
11170	Error	Failed to virtualize LUN [L#] because of mismatching size between configuration file and disk. Please do rescan and try it again.	Attempting to virtualize a LUN that has a different capacity than what was previously seen.	Rescan for new devices and try again.
11201	Error	There are too many Console connections.	Too many VTL console processes are connected to the particular VTL server. This is a highly unlikely condition.	None.
11202	Error	Console ([host name]): Illegal access.	The VTL console host attempts to perform operation outside of the granted privilege level. This rarely happens. If it does, it is either due to a retry operation from an unexpectedly terminated connection that was assigned a different privilege level, or it is a deliberate break-in attempt by reverse engineering of VTL console software, which as indicated by this error message, is not feasible	See 11107.

No.	Type	Text	Probable Cause	Suggested Action
11203	Error	Console ([host name]): SCSI device re-scanning has failed.	Error occurred when adding newly discovered the SCSI devices to the system. Most likely due to unreliable storage connectivity, or hardware failure, or system resource is running low.	See 10100.
11204	Error	Console ([host name]): SCSI device checking has failed.	Error occurred when accessing the SCSI devices when console requests the server to check the known storage devices. Most likely due to storage connectivity failure or hardware failure.	Check the storage devices, e.g., power status; controller status, etc. Check the connectivity, e.g., cable connectors. In Fibre Channel switches, even the connection status light indicates the connection is good, it is still not a guarantee. Disconnect/reconnect the connector to make sure. Check the specific storage device using OS provided utilities such as hdparm.
11209	Error	Console ([host name]): Insufficient privilege access.	A 'read only' user attempts to do an operation that requires configuration change.	Login as administrator user if configuration changes need to be made.
11211	Error	Console ([host name]): Failed to save file [filename].	Error encountered when writing the VTL configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	See 10006.
11212	Error	Console ([host name]): Failed to create index file [file name] for Event Log.	Failed to create an index file for the event log retrieval. Most likely due to insufficient system disk space.	Free up disk space, or add additional disk space to system drive.
11216	Error	Console ([host name]): Out of system resources. Failed to fork process.	The VTL server is low in memory resource for normal operation.	See 11114.
11219	Error	Console ([host name]): Failed to add virtual device [Device number].	Failed to create a virtual drive due to either system configuration error, or storage hardware failure, or system resource access failure.	Check system resources, such as memory, system disk space, and storage device connectivity (cable connections).

No.	Type	Text	Probable Cause	Suggested Action
11233	Error	Console ([host name]): Failed to map the SCSI device name for [ACSL].	The mapping of the SCSI address, namely the adapter, channel, SCSI ID, and LUN, (ACSL) is no longer valid. This must be due to sudden failure, or improper removal, or change of storage devices in the VTL server.	See 11204. Check and restore the physical configuration to proper state if changed improperly.
11234	Error	Console ([host name]): Failed to execute hdparm for [Device number].	Failed to perform the device throughput test for the given device. This can be due to either OS in a bad state such that the program cannot be run, or the storage device failed.	Test run the hdparm program from the VTL server console directly. Check storage devices as described in 11204.
11240	Error	Console ([host name]): Failed to start the VTL Server module.	When any VTL process cannot be started, it is most likely due to insufficient system resources, an invalid state left by VTL processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this frequently occurs, there must be external factors that contributed to the behavior and these must be investigated and removed before running the VTL server.	If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware or software components, restart the server machine to make sure the OS is in a healthy state before trying again.

No.	Type	Text	Probable Cause	Suggested Action
11242	Error	Console ([host name]): Failed to stop the VTL Server module.	When any VTL process cannot be started, it is most likely due to insufficient system resources, an invalid state left by VTL processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this frequently occurs, there must be external factors that contributed to the behavior and these must be investigated and removed before running the VTL server.	If system resource is low, use top to check the process that is using the most memory. If physical memory is below the recommendation, install more memory to the system. If the OS is suspected in bad state due to unexpected failure in either hardware or software components, restart the server machine to make sure the OS is in a healthy state before trying again.
11257	Error	Console ([host name]): Failed to add SAN Client ([Host name]).	See 11101.	See 11101.
11261	Error	Console ([Host name]): Failed to get SAN Client connection status for virtual device [Device ID].	Failed to inquire a SAN Client connection status due to either system configuration error, or storage hardware failure, or system resource access failure. This should rarely happen.	Check system resource, such as memory, system disk space. Check the syslog for specific reason of the failure.
11262	Error	Console ([host name]): Failed to parse configuration file [File name].	See 11112.	See 11112.
11263	Error	Console ([host name]): Failed to restore configuration file [File name].	See 10006.	See 10006.
11266	Error	Console ([host name]): Failed to erase partition of virtual device [Device number].	Storage hardware failure.	See 10004.
11278	Error	Console: Failed to swap mirror for repository.	Hardware problem with the repository mirror disk.	Check the repository mirror disk.
11291	Error	Console ([host name]): Failed to update meta information of physical device [Device number].	Storage hardware failure.	See 10004.

No.	Type	Text	Probable Cause	Suggested Action
11292	Error	Console ([host name]): Failed to swap IP address from [IP address] to [IP address].	See 11000.	See 11000.
11295	Error	Console ([host name]): Invalidconfigurationformat.	See 11112.	See 11112.
113150	Error	You have no license for %1 protocol.	An attempt was made to enable a protocol such as Fibre Channel, iSCSI with no appropriate license keys.	Install appropriate license keys that include support for the needed protocol
113160	Error	You have exceeded the storage capacity allowed by your license, used space=%1MB, needed space=%2MB, licensed capacity=%3MB.	Physical capacity usage has exceeded the capacity allowed by the license.	Contact Sun StorageTek to purchase additional capacity license.
11406	Error	Failed to prepare the failover configuration package.	Suspend fail over initiated while packaging fail over configuration information.	No action required. (Operation will be retried automatically)
11407	Error	Failed to extract the failover configuration package.	Same as 11406	No action required (Operation will be retried automatically)
11500	Error	Out of disk space to expand virtual tape.	There is no more storage space available for expanding a virtual tape.	Add more storage to VTL system.
11512	Error	Console: Failed to add a replica for virtual tape to IPStor Server (watermark: MB, time: , interval: , watermark retry: , suspended: ).	It can be connection error while the primary server is synchronizing the initial status of the virtual tape to the replica on the target server, or the virtual tape is loaded to the drive at the moment by backup software or the console on different machine.	Check if the network is working properly first and correct the problem first if it is. If the virtual tape is moved to the drive, reconfigure the replication later.

No.	Type	Text	Probable Cause	Suggested Action
11514	Error	Console: Failed to remove the replica for virtual tape from IPStor Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration file to the VTL system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Check to make sure there is enough free space on the system disk. (This should never happen since the VTL system has a mechanism to automatically prune the syslog periodically to prevent syslog from using up all system disk free space). If enough space is available on system disk, check the integrity of system disk file system using fsck utility
11516	Error	Console: Failed to create the virtual tape replica.	Could not update the virtual tape partition information on disk.	Check the Storage system and make sure that storage is working properly.
11518	Error	Console: Failed to start replication for virtual tape.	The replication triggered manually by the user failed. It can be due to one of the following reasons. Network problems, Virtual tape is loaded in a drive, replication is in progress or the replica no longer exists.	See actions for corresponding events: 1067, 1030 and 1069.
11522	Error	Console: Failed to promote virtual tape replica to a virtual tape.	Failed to update the virtual tape partition information. It	Check if the physical disk is working properly or the server is busy. Retry the operation when the physical disk is working properly or when the server is not busy.
11524	Error	Console ([host name]): Failed to run VTL Server X-Ray.	See 11240.	See 11240.
11534	Error	Console ([host name]): Failed to reset the umap for virtual device [Device number].	Storage hardware failure.	See 10004.
11535	Error	Console: Failed to update the replication parameters for virtual tape to IPStor Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	Error encountered when writing the updated configuration file to the VTL system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Check if the system drive is out of space or has any corruption.

No.	Type	Text	Probable Cause	Suggested Action
11537	Error	Console ([host name]): Failed to claim physical device [Device number].	This may due a specific version of the VTL server limiting the support of the storage.	Check license agreement for the version of VTL server.
11539	Error	Console ([host name]): Failed to import physical device [Device number].	Storage hardware failure.	See 10004.
11542	Error	Console: Failed to remove virtual tape replica.	Error encountered when writing the updated configuration to the VTL configuration file to the system drive. This can only happen if the system drive ran out of space, or is corrupted, or if there is hardware failure in the system drive.	Check if the system drive is out of space or has any corruption.
11554	Error	Console ([host name]): Failed to set failover option <selfCheckInterval:>	IP Network communication failure	Check network connectivity.
11569	Error	Console ([host name]): Failed to set [Device number] to Fibre Channel mode [Mode].	This is possibly due to the fibre channel driver being improperly loaded, or the wrong version of the driver is loaded. VTL FC target mode requires the VTL version of the driver to be used.	Use lsmod to check that the proper VTL driver is loaded. If it is, check to make sure it is the correct revision. The correct revision should be located in the VTL/lib directory.
11578	Error	Console ([host name]): Failed to get Fibre Channel initiator information.	See 11569.	See 11569.
11632	Error	Console: Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: sec>.	IP Network communication failure.	Check Network connectivityNotes Link
11633	Error	Console : Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: disabled>.	Same as 11632	Check Network connectivity.
11648	Error	Failed to get inquiry string on SCSI device [Device ID].	Hardware problem with SCSI device.	Check hardware.
11650	Error	Failed to get capacity size for SCSI device [Device ID].	Hardware problem with SCSI device.	Check hardware.
11651	Error	Medium test failed for SCSI device [Device name].	Hardware problem with SCSI device.	Check hardware.

No.	Type	Text	Probable Cause	Suggested Action
11652	Error	Could not get type for SCSI device [Device ID] because of inquiry string failure.	Hardware problem with SCSI device.	Check hardware.
11655	Error	Discarded scsi device [Device ID], bad capacity size.	Hardware problem with SCSI device.	Check hardware.
11741	Error	Console: Failed to create virtual library with [#of Slots] slots due to only [#of Slots] slots available.	Specified slot count for the virtual library exceeds the total slot count supported by the system.	Specify appropriate slot count.
11742	Error	Console: Create only [count] out of [count] virtual drives requested due to memory allocation failure.	System is out of memory, which prevents the creation of the specified number of virtual tape drives.	Increase system memory.
11744	Error	Console: The configuration file update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write to the VTL configuration file.	Check /usr partition for free space. If the partition is out of space, delete unwanted files to create space.
11745	Error	Console: The disk partition update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write update partition information to disks.	Check physical connectivity to the storage system/LUN.
11746	Error	Console: The testmode promotion of [# of tapes] tapes was rolled back.	Cannot add device to IOCore module.	Call technical support.
11782	Error	Barcode of the source tape already exist on target server. Auto-replication cannot be configured.	A tape with the same barcode exist on the remote sever.	Remove the tape with same barcode from the remote server or change it's barcode.
11788	Error	Appliance Hardware Problem:	Detected an error on the VTL appliance.	Check the error message for information on the error to determine the solution.
11791	Error	Failed to re-size virtual tape to MB. Error:	Virtual tape partition information couldn't be updated. This could happen in rare cases when the system is extremely busy and updates to disks take too long.	No user action required since it doesn't cause any problem for backup/restore. If this error happens the tape will not be resized.
11793	Warning	Appliance Hardware Problem: message	Detected a hardware problem with the appliance	Check the error message and take appropriate hardware maintenance.
11796	Error	Failed to set the migration disk threshold.	Connectivity issues with the storage where VTL repository is located.	Check storage connectivity.

No.	Type	Text	Probable Cause	Suggested Action
11797	Error	Failed to set the reclamation disk threshold, error = EC.	Connectivity issues with the storage where VTL repository is located.	Check storage connectivity.
12509	Error	Failed to inventory physical library VID.	Physical library inventory process failed.	Check server log for more information on the cause of the HW failure.
12511	Error	Failed to move tape in library VID from slot %2 to drive VID.	Physical tape move from slot to drive failed.	Check server log for more information on the cause of HW failure.
12521	Error	Failed to move tape in library VID from drive VID to slot VID.	Physical library may have hardware issues.	Check server log for more information on the cause of HW failure.
12611	Error	Failed to add ACSLS lib to physical library %1, tleioctl failed, errno = %2.	ACSLs server cannot be added into the list of physical libraries due to connection problems or initialization issues.	Check the ACSLS library to make sure it is running properly and is connected correctly to the VTL server.
13309	Error	Failed to communicate with the primary server.	Secondary server failed to talk to primary server	Check network connectivity
13704	Warning	VTL failure detected.	VTL secondary server detected software/hardware failure on Primary server. This will trigger a take over operation.	Once the primary server is brought back up, initiate fails back operation manually.
13710	Warning	The Live Trial period has expired for VTL Server[Server name]. Please contact Sun StorageTek or its representative to purchase a license.	Exceeded the 30-day live trial grace period.	Contact Sun StorageTek or its representative to obtain proper license.
13711	Warning	The following options are not licensed: [VTL option]. Please contact Sun StorageTek or its representative to purchase a license.	The specific option is not licensed properly.	Contact Sun StorageTek or its representative to obtain proper license.
13800	Warning	Primary server failure detected. Failure condition:	VTL Primary server detected software/hardware failure on itself. This will trigger a fail over operation to secondary server.	Once the primary server is brought back up, manually fail back operations to primary.
13804	Error	Quorum disk failed to release to secondary.	Negotiation through Quorum disk failed.	Check Storage or connectivity to Storage.

No.	Type	Text	Probable Cause	Suggested Action
13817	Error	Primary server failback operation failed.	Primary server had a software/hardware failure condition during fail back.	Check Hardware such as FC ports, Storage and connectivity to Storage.
13820	Warning	Primary server heartbeat not detected. Testing network connectivity.	Network communication failure	Check network connectivity
13821	Error	Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.	Network connectivity failure and no connectivity to outside network.	Check network connectivity and the secondary server health.
13822	Warning	Secondary will not take over because storage connectivity is not 100%.	Storage or Storage connectivity failure on secondary.	Check Storage or connectivity to storage.
13828	Warning	Almost running out of file handler (current [Number of handles], max [Number of handles]).	The Linux system is running out of resource for file handles.	Determine the appropriate amount of memory required for the current configuration and applications. And determine if there are processes that are leaking memory.
13829	Warning	Almost running out of memory (current [Number of KB] K, max [Number of KB]).	The Linux system is running out of memory.	See 13828.
13830	Error	Failed to get configuration file from storage.	Failed to access storage LUN where the repository is located during recovery process.	Check storage LUN where the repository is located.
13856	Error	Secondary server ServerName failed to communicate with primary server ServerName through IP IPAddress.	Network connectivity failure happened between primary and secondary servers.	Check network connectivity between primary and secondary servers.
14005	Error	Cannot update ipstor partition information.	Storage is offline.	Check connectivity to storage.
15055 v5.0	Error	Server ioctl call [Device ID] failed on vdev id [Device ID]: Device or resource is busy (EBUSY).	The virtual drive is busy with I/O and is not responsive to the upper layer calls.	Try again when the system is less busy, or determine the cause of the extensive I/O, and correct the situation if necessary.
16100	Warning	Email Alerts failed to connect to SMTP server ServerIP on port PortID.	Connectivity problems with the SMTP server due to IP address or PortID.	Check network connectivity, SMTP server IP address and PortID.
16101	Warning	Email Alerts failed to send email to SMTP server ServerIP on port PortID.	See 16100.	See 16100.

No.	Type	Text	Probable Cause	Suggested Action
18001	Error	SIR: Startup of SIR Repository has been aborted because of missing storage. Please check that each member of the cluster is operating properly.	SIR: Startup of SIR Repository has been aborted because of missing storage.	<ol style="list-style-type: none"> <li>1. Make sure storage is healthy.</li> <li>2. Make sure each node of the SIR cluster can connect to the storage.</li> <li>3. Restart the services.</li> </ol>
18050	Error	SIR: Reclamation Dispatcher Daemon terminated because Cruncher has failed.	A tape has been relabeled to be reused, so the reclamation process started on SIR server but Index Pruning failed so we do not want to trigger any reclamation because the Index Disk may be in a bad state.	Call Tech Support.
18051	Informational	SIR: Initiating Space Reclamation, total object count %1, capacity %2, previous reclaimed count %3.	A tape has been relabeled to be reused, so SIR Space Reclamation is initializing reclamation for the data disk space and memory. It is also reporting information regarding the total objects currently in the system, the total object capacity of the system, and how many objects reclaimed since the previous Space Reclamation.	No action required.
18052	Informational	SIR: Initiating Index Pruning, total object count %1, capacity %2, previous reclaimed count %3.	A tape has been relabeled to be reused, so SIR Index Pruning is initializing reclamation for the index disk space. It is also reporting information regarding the total objects that currently in the system, the total object capacity of the system, and how many objects were reclaimed since the previous Index Pruning.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
18053	Informational	SIR: Initiating Data Disk Space Reclamation, total object count %1, capacity %2, previous reclaimed count %3.	A tape has been relabeled to be reused, so SIR Data Disk Space Reclamation is initializing reclamation for the data disk. It is also reporting information regarding the total objects currently in the system, the total object capacity of the system, and how many objects reclaimed since the previous Data Disk Space Reclamation.	No action required.
18055	Error	SIR: Index Reclamation did not complete. Reason: %1	There are numerous possible causes. Refer to reason.	Take action based on indicated reason.
18100	Informational	SIR: Execute: %1	The specified general action has been executed.	No action required.
18101	Error	SIR: Unable to get IPMI status for SIR node, %1, at IP address %2. This may compromise SIR node failure protection. Please check the IPMI configuration for this SIR node.	<ol style="list-style-type: none"> <li>1. IPMI may not be configured properly.</li> <li>2. IPMI may not be functioning correctly.</li> <li>3. IPMI may not be turned on.</li> <li>4. Machine may not have IPMI.</li> <li>5. IPMI may be down due to lack of electrical power.</li> </ol>	<ol style="list-style-type: none"> <li>1. Make sure IPMI is configured correctly.</li> <li>2. Make sure IPMI is healthy and functioning.</li> <li>3. Make sure IPMI is enabled / on. You can enable it by the command 'ipmiset enable'.</li> <li>4. Make sure machines support IPMI.</li> <li>5. Make sure electrical power is up and running for the machine.</li> </ol>
18102	Informational	SIR: This server has shutdown failed SIR node, %1, using IPMI at IP address %2 as prerequisite for SIR node takeover.	One of the nodes failed and the standby node is taking over. It will use IPMI to shutdown the failed SIR node.	No action required.
18103	Informational	SIR: This server has successfully taken over failed SIR node %1. Please correct and restore the failed SIR node.	<ol style="list-style-type: none"> <li>1. The standby node has successfully shut down the failed SIR node and is currently an active node in the SIR cluster.</li> <li>2. The failed SIR node can now be fixed and brought back online. It will then assume the role of standby node.</li> </ol>	Fix the failed SIR node and bring it online. It will then assume the role of the standby node.

No.	Type	Text	Probable Cause	Suggested Action
18104	Error	SIR: This server has failed to take over SIR node '%1' because the failed node reported its hostname as '%2' that is unknown to this server.	<ol style="list-style-type: none"> <li>1. There may be an Interruption in communication.</li> <li>2. Hostname string may have been reported incorrectly.</li> <li>3. The server is not registered with the N+1 configuration.</li> </ol>	Call Tech Support.
18105	Error	SIR: This server has failed to take over SIR node '%1' because there is no standby node information in the SIR cluster configuration file.	N+1 setup was not properly configured or there could be a failure during the configuration process.	Call Tech Support
18106	Error	SIR: This server has failed to take over SIR node '%1' because it could not shutdown the failed node using IPMI at IP address %2.	The standby server could not communicate with the failed server via IPMI IP address specified because of standby server or failed server's IPMI misconfiguration or the IP address for the failed server might have been set after the N+1 was configured.	<ol style="list-style-type: none"> <li>1. Make sure IPMI is properly set with the IP address being used for the N+1 failover setup.</li> <li>2. Make sure the IPMI is functioning correctly for both the standby and the failed server.</li> </ol>
18107	Error	SIR: This server has failed to take over SIR node '%1' because it failed to add virtual IP %2 of the failed node.	Heartbeat may not have been properly set.	Call Tech Support
18108	Error	SIR: This server has failed to take over SIR node '%1' because it failed to spoof WWPN of the failed node.	The standby server could not spoof the WWPN of the failed node.	Call Tech Support
18109	Error	SIR: This server has failed to take over SIR node '%1' because it failed to change its hostname to that of the failed node.	The standby server had problems changing its hostname to that of the failed node to assume the identity of the failed node.	Call Tech Support
18110	Error	SIR: This server has failed to take over SIR node %1 because it failed load the failed node's physical resources.	Storage may have an issue. The standby node needs to be able to see the storage/ resources of the active node in order to take over.	Call Tech Support
18111	Error	SIR: This server has failed to take over SIR node '%1' because it failed to copy out the from the configuration repository the failed node's configuration files.	The standby node could not get access to the failed node's configuration files and cannot assume its identity.	Call Tech Support

No.	Type	Text	Probable Cause	Suggested Action
18112	Error	SIR: This server has failed to take over SIR node '%1' because it failed to startup SIR services.	There may be a problem with the standby node's modules / services. The node needs to be able to start certain services to become active and take over the failed node.	Call Tech Support
19004	Warning	Allocate space at MB has reached the threshold of the total capacity.	Storage utilization has reached limit specified by user.	Check Storage utilization and delete unused virtual tapes to free up space or add more storage.
19057	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- unable to connect to remote server.	Replication configured using remote copy failed due to network problem.	See 1067.
19065	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- virtual tape is in the drive.	Virtual tape is moved to the tape drive while remote copy processing started.	Remove the replication setup configured through remote copy. Reconfigure remote copy when the virtual tape is moved to the vault or slot.
19202	Error	Console (User Name): Failed to create key KEYNAME	Key name already exists. Another user using a different console may have created key with same name.	Retry the operation.
19204	Error	Console (User Name): Failed to delete Key KEYNAME	The key may be deleted or renamed by somebody else in different console.	Retry the operation. Console will be automatically updated, if another user had deleted the key from another console.
19206	Error	Console (User Name): Failed to update information for key KEYNAME	The key name maybe deleted or changed, or the new key name may exist already.	Retry the operation. Console will be automatically updated, if another user had deleted/created the key from another console.
19208	Error	Console (User Name): Failed to create key package PACKAGENAME.	The keys to be exported may be modified or deleted.	Retry the operation.
19210	Error	Console (User Name): Failed to get key package information.	The key package format/content may be invalid.	Recreate the key package.
40002	Error	Block list full on tape.	Too many very small sized blocks (< 512 bytes) have been written to tape.	Increase the block size used by backup application.

No.	Type	Text	Probable Cause	Suggested Action
40010	Error	Attach to tape failed.	A physical device is not available.	Check the storage device connectivity and make sure that the software can access the devices.
40011	Error	Failed to read from Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40013	Error	Export Tape failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory available on the system may also resolve the problem.
40014	Error	Read tape info failed.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40015	Error	Export tape failed, unsupported block size.	Backup application has used an unsupported block size on virtual tape. 1MB is currently the max block size supported.	Change backup application configuration to use smaller block size.
40017	Error	Failed to write to Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40018	Error	Failed to load Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40019	Error	Failed to write to Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40022	Error	Failed to get Physical Tape block size.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40023	Error	Import failed, not enough memory.	System is running low on memory. May be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory available on the system may also resolve the problem.
40030	Error	Failed to read from repository.	The storage LUN where the repository is located cannot be accessed.	Check the LUN where the repository is located.
40031	Error	Failed to write to repository.	The storage LUN where the repository is located cannot be accessed.	Check the LUN where the repository is located.

<b>No.</b>	<b>Type</b>	<b>Text</b>	<b>Probable Cause</b>	<b>Suggested Action</b>
40032	Warning	Physical Tape not available to start export job in lib.	There is an import/export job in the queue waiting for a physical tape.	Insert tapes with appropriate barcodes in the physical library and perform an inventory operation.
40039	Error	Read Element command to Physical Library failed.	There is a hardware problem with the physical tape library.	Check with the tape library vendor.
40043	Error	Move Medium command failed in Physical Library.	There is a hardware problem with the physical tape library.	Check with the tape library vendor.
40044	Error	Unload command failed on Physical Tape Drive.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40045	Error	Read from Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40046	Error	Write to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40047	Error	Write File Mark to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40048	Error	Mode sense command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40049	Error	Mode select command to physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40050	Error	Rewind command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40051	Error	Inquiry command to Physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40065	Error	Read data from Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located.
40066	Error	Write data to Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located.
40069	Error	Cannot expand Tape.	Not enough storage space is available to expand a virtual tape.	Add more storage space to the system or free up space by deleting virtual tapes that are no longer required.
40074	Error	Export to Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40076	Error	Import Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.

No.	Type	Text	Probable Cause	Suggested Action
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	VTL doesn't allow duplicate barcodes in a system. Delete the existing tape or use a different barcode while importing.
40078	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	VTL doesn't allow duplicate barcodes in a system. Delete the existing tape or use a different barcode while importing.
40085	Error	Init Element Status command failed on Physical Library, Error.	Physical Library hardware problem.	Check physical library hardware.
40086	Error	Write command to Configuration Repository Failed. Please check repository LUNs.	Storage or Storage connectivity problems.	Check Storage and Storage connectivity.
40090	Error	Failed to load tape because it is a cleaning tape. Lib VID ##, Drive VID ##, BC ###	A cleaning tape is manually moved into a drive from console or a cleaning tape is used for import/export jobs.	Please check and make sure that cleaning tapes are not used for import/export jobs.
40092	Error	Error in retrieving the hostname of this CDL server.	Cannot get the system's hostname.	On CDL appliance verify that 'uname -a' returns the hostname.
40093	Error	Failure in looking up the IP address of the CDL server (ServerName). Please verify that DNS is configured correctly for both ACSLS and CDL server.	Couldn't find the IP address of the CDL server from DNS nor the /etc/hosts file.	If DNS is configured then verify that the DNS server is running and is configured correctly for both CDL appliance and ACSLS. If DNS is not configured then verify that the /etc/hosts file contains the public IP of the CDL appliance.
40096	Error	Failed to open [AAA].	Could not open ACSLS configuration file.	Verify that the ACSLS conf file exists at /usr/local/VTL/etc/acsls_ls_cdk.conf
40097	Error	DNS configuration for CDL server is incorrect. DNS or /etc/hosts is returning x.x.x.x as the IP of CDL server ServerName	Couldn't find the IP of the DL server from DNS nor the /etc/hosts file.	If DNS is configured then verify that the DNS server is running and is configured correctly for both CDL and ACSLS server. If DNS is not configured then verify that the /etc/hosts file contains the public IP of the CDL appliance.

No.	Type	Text	Probable Cause	Suggested Action
40098	Error	Failed to successfully query ACSLS server with IP x.x.x.x Error from ACSLS: EC	Failed to contact the ACSLS with the entered IP address.	Please verify that the IP is valid and that users can ping the ACSLS server from the DL server.
40099	Error	Waited N seconds to get a response from ACSLS x.x.x.x. Timing out...	Failed to contact the ACSLS with the entered IP address.	Please verify that the IP is valid and that users can ping the ACSLS server from the DL server.
40100	Error	Failed to mount BARCODE on drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS]	Mount operation failed.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the mount failed.
40101	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to mount BARCODE on drive x.x.x.x. Timing out...	Mount operation failed, timing out.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the mount failed.
40102	Error	Failed to dismount BARCODE from drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS server].	Dismount operation failed.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the dismount failed.
40103	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to dismount BARCODE from drive x.x.x.x. Timing out...	Dismount operation failed, timing out.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the dismount failed.
40104	Error	Failed to retrieve drive information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get drives list from ACSLS server.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the 'display' command failed.
40105	Error	[Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve drive information in ACS ##. Timing out...	Failed to get drives list from ACSLS server. Timing out.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the 'display' command failed.
40106	Error	Failed to retrieve volume information in ACS ## and Pool ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get volume list from ACSLS server.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the 'display' command failed.

No.	Type	Text	Probable Cause	Suggested Action
40107	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve volume information in ACS ## and Pool ##. Timing out.	Failed to get volume list from ACSLS server. Timing out.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the 'display' command failed.
40108	Error	Failed to retrieve LSM information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get LSM list from ACSLS server.	Check the ACSLS manager server's event log to see why the 'display' command failed.
40109	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve LSM information in ACS ##. Timing out.	Failed to get LSM list from ACSLS server. Timing out.	Check the ACSLS manager server's event log (\$ACSLSHOME/log/acsss_event.log) to see why the 'display' command failed.
40191	Error	Hardware compression card failed - EC [ %1 ], complete code [%2], hardware complete code [%3] while accessing tape [%4] VID [%5].	Compression card reported a failure.	Contact compression card vendor.
40193	Error	ACSLS/LS: Failed to query %1 server with IP %2 and ACS %3 due to wrong ACS ID %4.	ACS ID specified in ACSLS configuration is incorrect.	Use the correct ACS ID in ACSLS configuration.
40194	Error	ACSLS/LS: portmap daemon is required for ACSLS libraries. Please start portmap daemon using "portmap" command and do a rescan on the physical devices.	portmap daemon is not running.	Check and make sure portmap daemon is running.
40195	Warning	The tape [%1] is being deduped at the moment - export job cannot be submitted.	An attempt was made to manually export a tape when a deduplication operation is in progress.	Run export jobs after deduplication is completed.
40197	Warning	Repository consistency check detected non critical inconsistencies. Check syslog for more information.	Possible non-critical information/structure inconsistencies detected in VTL database (repository). Integrity of the disk LUN that stores the VTL database may be compromised.	Check syslog for details of inconsistencies. Check the storage for possible errors/issues.

No.	Type	Text	Probable Cause	Suggested Action
40198	Error	Repository consistency check detected critical errors. Check syslog for more information.	Critical information/structure inconsistencies detected in VTL database (repository). Integrity of the disk LUN that stores the VTL database may be compromised.	Check syslog for details of inconsistencies. Check the storage for possible errors/issues.
40199	Error	Compression data consistency check: Invalid data signature found on tape [%1] VID %2	Data integrity signature in compressed blocks does not match the original signature. Data received from the storage is corrupted.	Check storage for possible corruption and take appropriate actions to correct it.
40200	Error	Write Filemark Table failed. BC [%1], VID %2, EC %3	Write operation on Filemark Table (part of virtual tape meta data) failed possibly due to issues with storage.	Check storage and make sure that storage is accessible.
40201	Error	Tape can not be created - Duplicate VID found %1	A tape is being created with VID that already exists possibly due to inconsistencies in internal information.	Contact Sun StorageTek technical support.
40202	Warning	TapeProperty: VTL management did not find the tape [%1], VID=%2	It is possibly due to inconsistencies in internal information.	Contact Sun StorageTek technical support.
40203	Warning	TapeProperty: Found tape maximum capacity mismatch on tape [%1], VID=%2 - Mark the tape as READ ONLY	A mismatch in the maximum capacity of a tape was detected by consistency checks.	Contact Sun StorageTek technical support.
40204	Warning	TapeProperty: Found tape allocated size mismatch on tape [%1], VID=%2 - Mark the tape as READ ONLY	A mismatch in allocation size of a tape was detected by consistency checks.	Contact Sun StorageTek technical support.
40205	Warning	TapeProperty: Found stub tape property mismatch on tape [%1], VID=%2, stubtape=%3 - Mark the tape as READ ONLY	A mismatch in stub tape property was detected by consistency checks	Contact Sun StorageTek technical support.
40206	Warning	TapePropertyCheckUpCall: Found tape capacity on demand property mismatch on tape [%1], VID=%2, COD=%3	A mismatch in COD property was detected by consistency checks.	Contact Sun StorageTek technical support.
50101	Informational	SIR Cluster: Checking fibre channel connectivity from %1 to %2	SIR Cluster configuration process is checking to make sure there is connectivity between the nodes.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50102	Informational	SIR Cluster: Creating the quorum device on %1	SIR Cluster configuration process is creating its quorum device.	No action required.
50104	Informational	SIR Cluster: Creating SIR index storage %1 on %2	SIR Cluster configuration process is setting up its index disks to store index log information.	No action required.
50105	Informational	SIR Cluster: Creating SIR data storage %1 on %2	SIR Cluster configuration process is setting up its data disks for the data repository.	No action required.
50106	Informational	SIR Cluster: Setting up cluster %1 for node(s): %2	SIR Cluster configuration process is preparing the following nodes to be included in the SIR Cluster.	No action required.
50107	Informational	SIR Cluster: Creating storage pool for SIR storage on %1	SIR Cluster configuration process is creating an SIR storage pool for the nodes in the SIR Cluster. Each node's storage pool will contain data disks from the other nodes of the cluster.	No action required.
50108	Informational	SIR Cluster: Adding SIR storage to storage pool on %1	SIR Cluster configuration process is adding to each node's storage pool all the other SIR node's storage.	No action required.
50109	Informational	SIR Cluster: Setting up security from %1 to %2	SIR Cluster configuration process is setting up the security between the nodes of the SIR Cluster.	No action required.
50110	Informational	SIR Cluster: Checking SIR devices on %1	SIR Cluster configuration process is checking to make sure each node sees all the SIR devices of the SIR Cluster.	No action required.
50111	Error	SIR Cluster: SIR device %1 is not available on %2	The current node cannot access the SIR device of the SIR Cluster.	Check the connectivity between the nodes.
50112	Informational	SIR Cluster: Configuring storage connection from %1 to %2	SIR Cluster is configuring connection between node and connection with storage devices. Each node needs to be able to see other's storage and resources.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50113	Informational	SIR Cluster: Changing root password on %1	SIR Cluster configuration process is changing the current node's password to have the password on each node to be the same.	No action required.
50114	Informational	SIR Cluster: SIR cluster %1 is created and configured successfully on %2	SIR Cluster configuration process has successfully configured the current node to be included as part of the SIR Cluster.	No action required.
50115	Error	SIR Cluster: %1 cannot detect fibre channel target(s) of %2	SIR Cluster nodes cannot see other's fibre channel target ports because of FC zoning or connectivity.	Check the fibre channel zoning and make sure the nodes can see each other's target ports.
50116	Informational	SIR Cluster: Setting up cluster on %1	SIR Cluster configuration process is starting to setup the current node to be added into the SIR Cluster.	No action required.
50201	Informational	SIR Failover: Failover has been set up successfully on %1.	N+1 failover configuration has been configured successfully for current node of the SIR Cluster.	No action required.
50202	Informational	SIR Failover: All Failover setup steps have been completed successfully.	The overall N+1 failover configuration has been setup successfully.	No action required.
50203	Error	SIR Failover: Failed to upload server %1 configuration file.	During the N+1 configuration process, there was some communication issues between the nodes or not enough space to store each of the nodes configuration files.	Call Tech Support to clean up before retrying the N+1 failover setup
50204	Error	SIR Failover: Failed to set up shared secret between %1 and %2.	There is a previous N+1 failover configuration that has not been cleaned up correctly.	Call Tech Support to clean up before retrying the N+1 failover setup.
50300	Informational	SIR Replication: Setting up replication from SIR cluster %1 to SIR cluster %2	SIR Cluster is starting to set up the replication association to another SIR Cluster to do SIR replication.	No action required.
50301	Informational	SIR Replication: Configuring SIR storage connection from %1 to %2	SIR Replication configuration process is configuring the storage from the source SIR Cluster to the target SIR Cluster.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50302	Informational	SIR Replication: Setting up iSCSI user account on %1	SIR replication is setting up SIR replication using the iSCSI protocol.	No action required.
50303	Informational	SIR Replication: Configuring iSCSI initiator on %1	SIR replication configuration process is setting up the iSCSI initiator on the target SIR Cluster.	No action required.
50304	Informational	SIR Replication: Checking SIR devices on %1	SIR replication configuration process is checking that the SIR devices from the source SIR Cluster can be seen by the target SIR Cluster	No action required.
50305	Error	SIR Replication: SIR device %1 is not available on %2	One of the cluster nodes cannot access the SIR device for SIR replication.	<ol style="list-style-type: none"> <li>1. Make sure the nodes of the target SIR Cluster can access the source SIR Cluster's SIR devices.</li> <li>2. Rescan for the devices.</li> </ol>
50306	Informational	SIR Replication: Creating storage pool for SIR storage on %1	SIR replication configuration process is creating an SIR storage pool on the target SIR Cluster which will contain the data disks from the source SIR Cluster.	No action required.
50307	Informational	SIR Replication: Adding SIR storage to storage pool on %1	SIR Cluster configuration process is adding to each target SIR Cluster node's storage pool all the disks from the source SIR Cluster.	No action required.
50308	Informational	SIR Replication: Setting up replication on %1	SIR is starting to setup replication on the current node.	No action required.
50309	Informational	SIR Replication: Replication from SIR cluster %1 to SIR cluster %2 set up successfully	The overall SIR replication configuration process has been successfully created	No action required.
50405	Error	SIR Replication: Invalid request %1	Resolver job transmitted an invalid request due to a possible network or tape corruption.	This should rarely happen. Restore the tape, check the network, or retry the job.
50406	Error	SIR Replication: Unable to read Guid %1, reason %2	Disk request was unable to be satisfied due to a possible network or tape corruption.	Restart replication services, and retry the job. If that still fails, check the tape by restoring, or check the network.

No.	Type	Text	Probable Cause	Suggested Action
50409	Warning	SIR Replication: Shutting down due to: %1	Resolver job was unable to properly initialize the replication source server.	Another replication source server may already be running. In extremely rare cases, there might be some operating system issues.
50410	Error	SIR Replication: Session terminated, because connection timed out.	The TCP connection is timed out. The default timeout value for TCP connection is 40 minutes.	Increase TCP connection timeout value to higher number of minutes using the environment variable ResolverConnectionTimeout .
50561	Warning	RDE: Policy %1 , Tape [%2] unique data replication was cancelled because replication window has been exceeded. Rescheduled.	The policy has a timed window where the replication can be performed. The time has been exceeded so replication will be cancelled.	Enlarge the time window for replication.
50918	Warning	SIR Client: Store data block requested for folder %1 warning. Reason is %2	This is mostly caused by folder being abandoned and can happen when dedupe is cancelled, for example, in case the tape in deduplication is requested by a backup client.	No action required.
50701	Informational	SIR Scanner: Tape scan started successfully for Tape %1 in Drive %2	SIR scanner has successfully started to scan the current tape in one of the SIR tape drives.	No action required.
50702	Error	SIR Scanner: Failed to start tape scan for Tape %1 in Drive %2; Reason is %3	SIR Cluster may not be connected to the VTL SIR tape drive resources.	Make sure the all the SIR nodes in the SIR cluster can access the VTL's SIR tape drive resources.
50703	Informational	SIR Scanner: Tape format for Tape %1 in Drive %2 is %3	SIR has determined the supported backup application format of the tape it is currently scanning.	No action required.
50704	Informational	SIR Scanner: Tape format for Tape %1 in Drive %2 is not recognized; Generic format is assumed with following additional details: %3	SIR has determined that the current tape's format is not one of the supported backup application. It will switch over to the generic scanner.	No action required.
50705	Informational	SIR Scanner: Create SIR folder for Tape %1 in Drive %2	As SIR scans the tape, it creates an associated folder on the Folder Disk drive that contains information relating to the contents of the scan session.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50706	Error	SIR Scanner: Failed to create SIR folder for Tape %1 in Drive %2; Reason is %3	The SIR folder disk may not be accessible	Make sure the storage that contains the folder disk is accessible by the SIR Cluster.
50707	Error	SIR Scanner: Failed to store data block from Tape %1 in Drive %2 to SIR folder; Reason is %3	SIR server lost connectivity to its storage or the SIR repository may have failed.	Make sure the SIR can access its storage; If the SIR repository has failed, call Tech Support.
50708	Informational	SIR Scanner: Tape %1 scan completed successfully in Drive %2; Time elapsed: %3; Total data: %4; Redundancy elimination ratio: %5	SIR scanning has completed for the current tape. Information such as scan time, total data scanned, and de-dupe ratio is recorded.	No action required.
50709	Error	SIR Scanner: Tape %1 scan failed in Drive %2; Reason is %3	<ol style="list-style-type: none"> <li>1. Access to the tape drive may have been lost.</li> <li>2. SIR may have been busy due to heavy I/O so the SIR Server was not accessible.</li> <li>3. A repository error may have occurred.</li> </ol>	<ol style="list-style-type: none"> <li>1. Make sure SIR Cluster has access to the tape drives and retry scan on the tape.</li> <li>2. If SIR is busy at the time, retry scan on the tape.</li> <li>3. Make sure SIR storage is accessible by the SIR Cluster.</li> </ol>
50710	Warning	SIR Scanner: Tape %1 scan has been cancelled in Drive %2	<ol style="list-style-type: none"> <li>1. SIR scanning may have been cancelled by user.</li> <li>2. SIR resolving may have been cancelled by the user or backup application.</li> </ol>	No action required.
50711	Informational	SIR Scanner: Tape %1 in Drive %2 is being accessed by a backup client; Scanning suspended	Tape scan is paused because the backup client needs access to the tape do backup / restores / etc.	No action required.
50712	Informational	SIR Scanner: Tape %1 scan is resumed in Drive %2	Tape scanning was paused by the backup application and now it is finished so SIR scans will resume on that tape.	No action required.
50714	Error	SIR Scanner: Failed to convert Tape %1 in Drive %2 to Virtual Index Tape; Failed after: %3	A general indication of failure of the dedupe scanner. Will almost always be preceded by other error messages.	Take action based on other error messages.

No.	Type	Text	Probable Cause	Suggested Action
50715	Informational	SIR Scanner: SCSI sense data: %1	An SCSI error has occurred. This may have been retried successfully or may have caused a reported failure. Any failure of scanner or replication will be indicated with additional messages.	Examine storage and storage connectivity and check other error messages.
50716	Informational	SIR Scanner: Tape %1 in Drive %2 is empty	Deduplication of an empty tape triggered.	No action required.
50717	Informational	SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 started successfully	SIR scanning has been started and the Index information has successfully started transferring to the destination.	No action required.
50718	Informational	SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 finished successfully	SIR scanning has completed and all the index information has been successfully transferred to the destination tape.	No action required.
50719	Error	SIR Scanner: Transferring Index Info to Tape %1 in Drive %2 failed	<ol style="list-style-type: none"> <li>1. SIR may have lost access to the VTL resources while it was trying to transfer the index info to the destination tape - 2 tape model.</li> <li>2. May not be enough storage space on the VTL.</li> </ol>	<ol style="list-style-type: none"> <li>1. Make sure SIR Cluster can access the VTL SIR Tape Drives and VTL's tapes.</li> <li>2. Make sure VTL has enough storage space.</li> </ol>
50720	Informational	SIR Scanner: Generic parsing has been invoked for Block at %1, Tape %2, Drive %3	The SIR scanner could not determine the format for a particular block on the tape. It will switch to generic scanner and instead of using the backup application specific scanner.	No action required.
50721	Informational	SIR Scanner: Generic parsing has been invoked for Tape %1, Drive %2, Start Block %3, Start Block Offset %4, End Block %5, End Block Offset %6, Total Bytes %7	The SIR scanner could not determine the format for a particular block(s). Once the scanner recognizes subsequent blocks, it will switch back to the backup application specific scanner and print out information relating to what blocks it had to process using the generic scanner.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50801	Informational	SIR Resolver: Index tape replica data confirmation started successfully for Tape %1 in Source Drive %2 and Destination Drive %3	SIR replication resolving process has been successfully initiated for the replica tape on the replica server.	No action required.
50802	Error	SIR Resolver: Virtual Index Tape replica processing failed to start for Tape %1 in Source Drive %2 and Destination Drive %3; Reason is %4	A general indication of failure of the VIT replication. It will almost always be preceded by other error messages.	Take action based on other error messages.
50803	Error	SIR Resolver: Failed to process data block from Tape %1 in Source Drive %2 and Destination Drive %3; Reason is %4	A needed block of data could not be replicated to the target SIR.	Take action based upon the reason indicated.
50804	Informational	SIR Resolver: Index tape replica processing completed successfully for Tape %1 in Source Drive %2 and Destination Drive %3; Time elapsed: %4; Total data: %5; Redundancy elimination ratio: %6	SIR replication resolving process has completed for the replica tape. Information regarding the resolution process is reported such as total time to resolve, total data resolved, de-duplication ratio.	No action required.
50805	Error	SIR Resolver: Index tape replica processing failed for Tape %1 in Source Drive %2 and Destination Drive %3; Reason is %4	A general indication of failure of the unique data replication. It will almost always be preceded by other error messages.	Take action based on other error messages.
50806	Warning	SIR Resolver: Index tape replica processing has been cancelled for Tape %1 in Source Drive %2 and Destination Drive %3	Deduplication policy canceled manually or through a backup software.	No action required.
50901	Informational	SIR Client: SIR initialization started	SIR client such as scanner, resolver, or internal utility has started the initialization process.	No action required.
50902	Error	SIR Client: SIR client failed to initialize, error %1	SIR scanner or resolver client task could not be started. It will almost always be preceded by other error messages.	Take action based on other error messages.
50903	Informational	SIR Client: SIR client initialized successfully	SIR scanner or resolver client has started and initialized successfully.	No action required.

No.	Type	Text	Probable Cause	Suggested Action
50904	Informational	SIR Client: Folder %1 creation requested	The SIR scanning session has started and an associated folder has been successfully created for that session.	No action required.
50905	Informational	SIR Client: Folder %1 closed successfully	The SIR scanning session has completed and the associated folder for the scanning session has been successfully closed.	No action required.
50906	Error	SIR Client: Store data block requested for folder %1 failed. Reason is %2	The SIR scanner or resolver client could not write to the repository.	Check the reason given and act accordingly to fix it.
50907	Error	SIR Client: Failed to reach SIR server. Error is %1	SIR Server not running.	Check the error condition and start SIR server modules.
50908	Error	SIR Client: Failed to initialize SIR server. Error is %1	SIR server is not configured or SIR server has already been started.	Check error condition and SIR configuration.
50909	Error	SIR Client: Failed to get SIR server configuration. Error is %1	SIR server is not properly configured.	Call Tech Support.
50910	Error	SIR Client: Failed to set SIR server configuration. Error is %1	SIR server is not properly configured.	Call Tech Support.
50911	Error	SIR Client: Failed to get SIR object location. Error is %1	There may be some data inconsistency.	Call Tech Support.
50912	Error	SIR Client: Failed to check SIR object hash status. Error is %1	There may be some data inconsistency.	Call Tech Support.
50913	Error	SIR Client: Failed to create SIR folder. Error is %1	1. SIR may not be able to access the folder disk. 2. The folder disk may not have enough space.	1. Check that SIR can access its folder disk. 2. Expand the folder disk drive.
50914	Error	SIR Client: Replicate data block requested for folder %1 failed. Reason is %2	There are numerous possible causes. Refer to reason.	Take action based on indicated reason.
50915	Error	SIR Client: Close requested for folder %1 failed. Reason is %2	There are numerous possible causes. Refer to reason.	Take action based on indicated reason.
50916	Error	SIR Client: Abandon requested for folder %1 failed. Reason is %2	There are numerous possible causes. Refer to reason.	Take action based on indicated reason.

No.	Type	Text	Probable Cause	Suggested Action
50917	Error	SIR Client: Flush requested for folder %1 failed. Reason is %2	There are numerous possible causes. Refer to reason.	Take action based on indicated reason.
50951	Informational	SIR Server: Server initialization started	SIR Cluster configuration process has started the initialization process.	No action required.
50952	Error	SIR Server: Server failed to initialize. Reason is %1	This may be displayed without indicating a problem when the system is first being configured. In other circumstance, it indicates the SIR Client module could not initialize / start successfully.	Call Tech Support.
50953	Informational	SIR Server: Server initialized successfully	SIR Server has been started up and initialized successfully.	No action required.
50954	Error	SIR Server: Failed to access devices %1	1. SIR may have lost access to its storage devices. 2. The nodes may have failed to see each others resources.	1. Make sure there is connectivity between SIR and its storage. 2. Make sure the nodes of the SIR Cluster can see each others resources.
50955	Error	SIR Server: Index storage device %1 is full	Index disks are full.	Call Tech Support
50956	Error	SIR Server: Data storage class %1 is full	Data disks are full.	Add more data disks to all nodes of the SIR Cluster - currently only supported when SIR Cluster is setup using physical storage.
50957	Informational	SIR Server: Configuration file is missing	SIR Server never configured.	Configure SIR.
50958	Error	SIR Server: Repository index is out of memory	Index memory reserved for the SIR has been filled up.	Call Tech Support.

\*MTBF - Mean Time Between Failures -- Average lifespan of a device before failure, measured in hours, divide by 8600 to obtain year figure and adjust according to estimated duty cycle.

For any error not listed in this table, please contact Technical Support.

# Index

## A

- Activity Log 39
- Administrator
  - Management 29
  - Types 29
- Appliance
  - Connect 19
- Attention required tab 21, 37
  - Command line 178
- Auto expansion 46
- Auto Replication 45, 80

## B

- Backup server
  - Device scan 15
  - Open access 14
  - Secured access 14
- Backup software
  - Detect devices 16
  - Discover library 15
- Backups
  - FC backup servers 14
  - iSCSI backup servers 14
  - Overview 17
  - Prepare 14
  - Run jobs 17

## C

- Client 1, 24
  - Add 11, 55
  - Command line
    - Add 144
    - Delete 144
    - Properties 145
    - Virtual device list 143
  - HBA settings 113
  - iSCSI 122
  - NetWare
    - QLogic driver 112
  - Troubleshooting 241, 242

## COD

- Virtual tapes 46

## Command line

- Clients 143
- Commands 140
- Common arguments 141
- Deduplication 179
- Event Log 169
- Get 169
- Login/logout 142
- Physical devices 166
- Replication 159
- Reports 170
- System configuration 157
- Usage 140
- Virtual devices 143
- X-ray 178

## Components 1

## Configuration wizard

- VTL Console 6

## Connect

- Appliance 19

## D

- Database 10, 23

## Date

- System 28

## Deduplication 60

- Command line 179
- Create policy 13
- Enable 12, 61
- Monitor 70
- Perform 69
- Policies 66
- Reclaim disk space 77
- Statistics 70

## Deduplication policies

- Add 66
- Enable replication 68
- Modify 69

---

Device scan 15, 16

Devices

Rescan 25

Disaster recovery

Replication 82

## E

ECO

Appliance 1

Deduplication Policies object 23

Replication 84

Email Alerts 129

Configuration 129

Message severity 133

Modifying properties 133

System log check 132

Triggers 131, 134

Customize email 134

New script 134

Output 135

Return codes 135

Sample script 135

Event Log 21, 30, 169

Command line 169

Export 30

Filter information 30

Print 31

Sort information 30

Everyone client 14

## F

Fibre Channel Target Mode 107

Client HBA settings 113

AIX 114

HP-UX 114

Linux 114

NetWare 115

Solaris 115

Windows 113

Enable 9

Fabric topology 112

Hardware configuration 112

Server 109

Initiator mode 119

Installation and configuration 107

NetWare clients

QLogic driver 112

Persistent binding 111

Clients 113

Ports 109

QLogic configuration 112

QLogic ports 119

Server HBA settings 112

Switches 110

Configure for hard zoning 111

Configure for soft zoning 110

Target mode 119

Target port binding 111

Zoning 109

Find

Virtual tapes 51

## H

Halt server 28

HBA

Multi-ID

Troubleshooting 243

Hostname 8

Change 28

## I

Icons

Physical resource 25

Virtual tape 23

Introduction 1

iSCSI Target Mode 122

Initiators 122

Linux

Add iSCSI client 127

Configuration 127

Create targets for iSCSI client 128

Enable 127

Log client onto target 128

Prepare iSCSI initiator 127

Targets 122

Users 122

Windows 124

Configuration 123

Disable 126

Enable 123

Requirements 123

## J

Jumbo frames 8

## K

Keycode

Command line

- 
- Add 157
  - Remove 157
- L**
- Licensing 6
    - Command line
      - Add keycode 157
      - Remove keycode 157
  - Local Replication 82
  - Location 21, 39
  - Logical resources
    - Troubleshooting 241
  - Logs 27
    - VTL Console 27
- M**
- Messages
    - SNMP 41
  - Mirroring
    - Fix minor disk failure 43
    - Remove configuration 43
    - Replace disk in active configuration 43
    - Replace failed disk 43
    - Status 42
    - Swap 43
  - MTU 8
  - Multi-ID
    - HBA
      - Troubleshooting 243
- N**
- NetWare Client
    - QLogic driver 112
  - Network configuration 6
  - Network Time Protocol 28
  - NTP 28
- O**
- Offline tapes
    - Troubleshooting 241
- P**
- Passwords
    - Add/delete administrator password 29
    - Change administrator password 29
  - Patch
    - Apply 40
    - Rollback 40
  - Performance statistics 21, 38
  - Persistent binding 111
    - Clients 113
  - Physical device
    - Command line
      - Get device information 166
      - Import disk 167
      - Prepare disk 168
      - Rescan 167
      - Storage allocation 168
  - Physical resource icons 25
  - Physical resources
    - Troubleshooting 240
  - Ports 182
    - Target mode 9
  - Prepare virtual devices 10
- Q**
- QLogic
    - Configuration 112
    - Ports 119
- R**
- Reboot server 28
  - Recovery 42
  - Remote copy 81
  - Remote Replication 82
  - Replica resources 23
  - Replication 79
    - Access data on tape 102
    - Change configuration options 102
    - Command line
      - Create replica 159
      - Demote in test mode 165
      - Get properties 163
      - Get status 163
      - Promote in test mode 164
      - Promote replica 160
      - Remove 160
      - Resume 161
      - Set properties 162
      - Start 163
      - Stop 164
      - Suspend 161
    - Connect appliances 64
    - Deduplicated tapes 84
    - Deduplication repository
      - Add target server 64, 68, 94
    - Force 103
    - Local 82

- Policies 90
- Primary tape 82
- Promote 101
- Remote 82
- Remove 103
- Remove configuration 103
- Replica resource 82
  - FVIT 62, 85
- Requirements 63, 69, 86
- Resume schedule 102
- Setup 88
- Start manually 103
- Status 99
- Stop in progress 103
- Suspend schedule 102
- Troubleshooting 244
- Using an alternate NIC 96
- Virtual tapes 82
  - Troubleshooting 244
- Virtual vault
  - LVIT 62
- Reports 24, 32
  - Command line 170
  - Create 33
  - Delete 36
  - Email 36
  - Export data 34
  - Properties 35
  - Refresh 36
  - Retention 35
  - Schedule 34
  - View 34
- Rescan
  - Devices 25
- Round Robin Logic 50

**S**

- SAN Client 24
  - Add 11, 55
  - iSCSI 122
    - Authenticated access 124
    - Unauthenticated access 125
- Search
  - Virtual tapes 51
- Security
  - Ports 182
  - System 182
- Server
  - Check processes 138

- General info 21
- Location 21, 39
- Performance statistics 21, 38
- Properties 39
- Restart processes 137
- Start processes 137
- Stop processes 139
- Version info 21
- Setup
  - Confirm successful backup 18
- SNMP 41
  - Traps 39
- SNMP Messages 185
- Software updates
  - Add patch 40
  - Rollback patch 40
- Sort
  - Virtual tapes 52
- Standalone tape drive
  - Command line
    - Create 151
- Statistics
  - Repository 75
- Storage monitoring 39
- System maintenance 28
  - Halt 28
  - Reboot 28
  - Restart network 28
  - Restart VTL 28
  - Set hostname 28

**T**

- Tape capacity-on-demand 46
- Target mode 9
- Target port binding 111
- Time
  - System 28
- Traps 41
- Troubleshooting 238, 246

**V**

- Version info 21
- Virtual device
  - Command line
    - Assign 145
    - Create 146
    - Delete 147
    - List 143
    - Unassign 146

---

- Prepare 10
- Virtual tape drives 22
  - Command line
    - Add 150
    - Get supported 148
- Virtual tape icons 23
- Virtual tape libraries 22
  - Assign 12
  - Assign to clients 57
  - Command line
    - Create 149
    - Get supported 148
  - Create 11, 44
- Virtual tapes
  - Command line
    - Copy 154
    - Create 151
    - Move 153
    - Set properties 155
  - Create 48
  - Display 51
  - Filter 51
  - Find 51
  - How they are allocated 50
  - Locate 51
  - Sort 52
- Virtual vault 22
- VIT
  - Troubleshooting 243
- VTL appliance 1
- VTL Console 1
  - Administrator Management 29
  - Connect 19
  - Connections problems 238
  - Display problems 240
  - Launch 19
  - Log 27
  - Overview 19, 20
  - Physical Resources object 24
  - Reports object 24
  - Rescan devices 25
  - SAN Clients object 24
  - Server
    - Properties 39
  - Server object 21
  - Set options 27
  - System maintenance 28
  - Troubleshooting 238
  - User interface 20
  - Virtual Tape Library System object 22
- VTL info
  - Command line 157
- VTL Server
  - Check processes 138
  - Restart processes 137
  - Start processes 137
  - Stop processes 139
- vtlconsole.log 27

**W**

- World Wide Port Names 120
- WWPN 120
  - Determining 9

**X**

- X-ray 245
  - Command line 178

**Z**

- Zoning 109