Sun StorageTek Virtual Tape Library

VTL Prime 1.1

User's Guide

316198201 Rev AA
September 2009

Virtual Tape Library

VTL Prime 1.1 User's Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 316198201
September 2009, Revision AA

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

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

Revision History

Name	Part #	Revision	Date	Comments
VTL Prime 1.1 User's Guide	316198201	AA	September 2009	Initial release.

Preface

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

Documentation, Support, and Training

Sun Function	URL
Documentation	`http://www.sun.com/documentation/`
Support	`http://www.sun.com/support/`
Training	http://www.sun.com/training/

Sun Welcomes Your Comments

Visit the Sun Documentation site at http://docs.sun.com and click on the FEEDBACK link at the bottom right of the screen to access the Opinion Lab feedback system.

Contents

Revision History

Preface

Introduction

Getting Started

VTL Console

Manage Tape Drives and Tapes

Data Deduplication

Data Replication

Fibre Channel Configuration

iSCSI Clients

Email Alerts

VTL Server

Command Line

Appendix

Troubleshooting

Index

Introduction

Important Note about ECO references in this document

This document describes Sun 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. It will be included in a subsequent release. Please disregard references to ECO in this document.

Sun StorageTek Virtual Tape Library overview

Sun 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 - don't 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 obtains these keys before you perform the configuation 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 vtlconsole (VTL GUI) utility

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

```
cd /usr/local/vtlconsole
./vtlconsole&
```

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

Load VTL console software on a laptop or workstation

VTL Console can be installed on 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 sofware.

   Go to the Solaris directory and run:

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

4. Start the VTL console.

   Go to /usr/local/vtlconsole and type:

   ```
   # ./vtlconsole &
   ```

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.

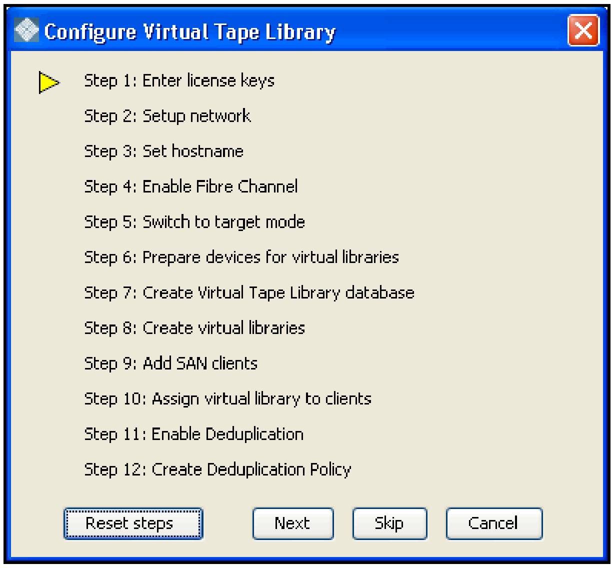
Once you are connected to a server, the server icon will change to show that you are connected:

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.



Configure Virtual Tape Library

▷ Step 1: Enter license keys

Step 2: Setup network

Step 3: Set hostname

Step 4: Enable Fibre Channel

Step 5: Switch to target mode

Step 6: Prepare devices for virtual libraries

Step 7: Create Virtual Tape Library database

Step 8: Create virtual libraries

Step 9: Add SAN clients

Step 10: Assign virtual library to clients

Step 11: Enable Deduplication

Step 12: Create Deduplication Policy

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.

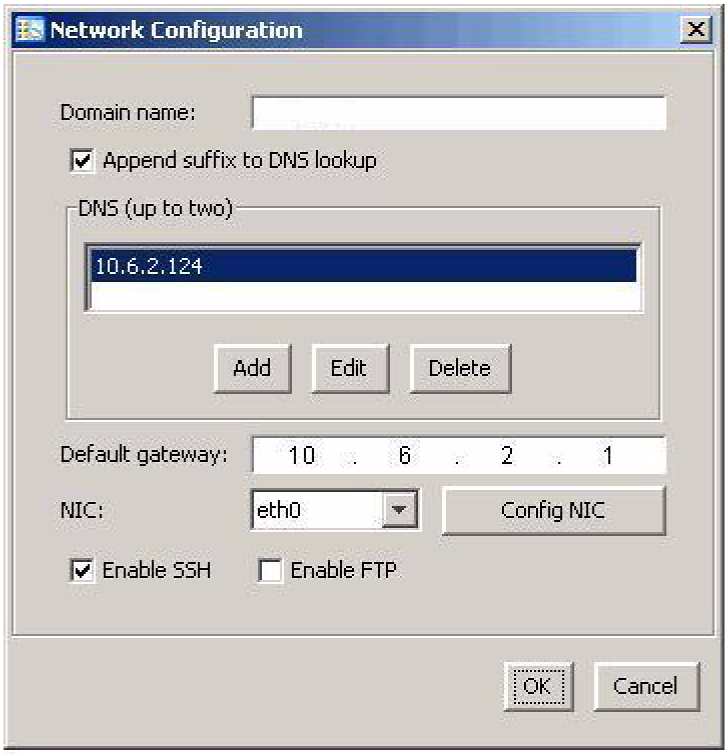
Be sure to enter keycodes for any options you have purchased. Each VTL option requires that a keycode be entered before the option can be configured and used.

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:

☑ Append suffix to DNS lookup

DNS (up to two)

10.6.2.124

Default gateway: 10 . 6 . 2 . 1

NIC: eth0

☑ Enable SSH ☐ Enable FTP

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.

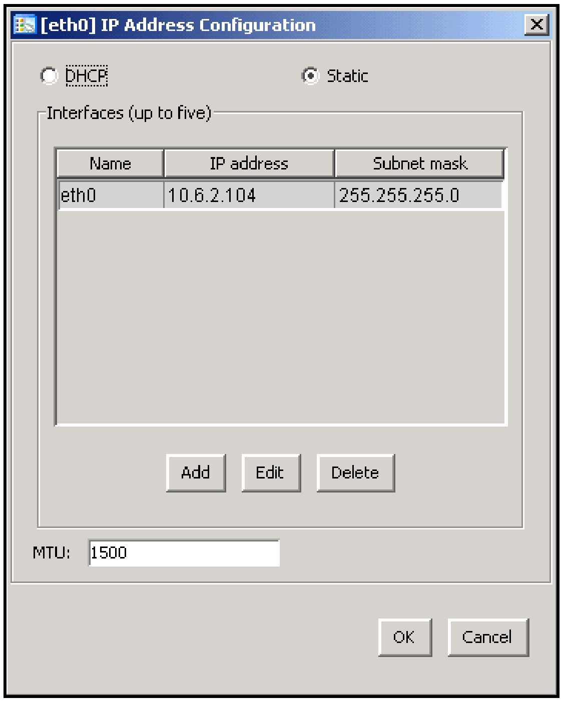
Default gateway - IP address of your default gateway.

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 “vsftp” installed in order to use FTP.

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



[eth0] IP Address Configuration

○ DHCP ● Static

Interfaces (up to five)

Name	IP address	Subnet mask
eth0	10.6.2.104	255.255.255.0

MTU: 1500

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

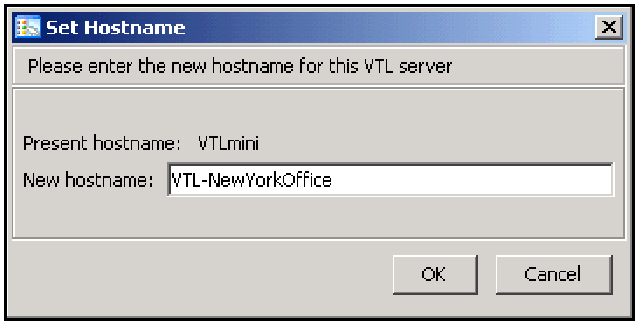
MTU - Set the maximum transfer unit of each IP packet. If your card supports it, set this value to 9000 for jumbo frames.

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.



Set Hostname

Please enter the new hostname for this VTL server

Present hostname: VTLmini

New hostname: VTL-NewYorkOffice

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

Note: 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*.

> **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.

Step 5: Switch to target mode

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

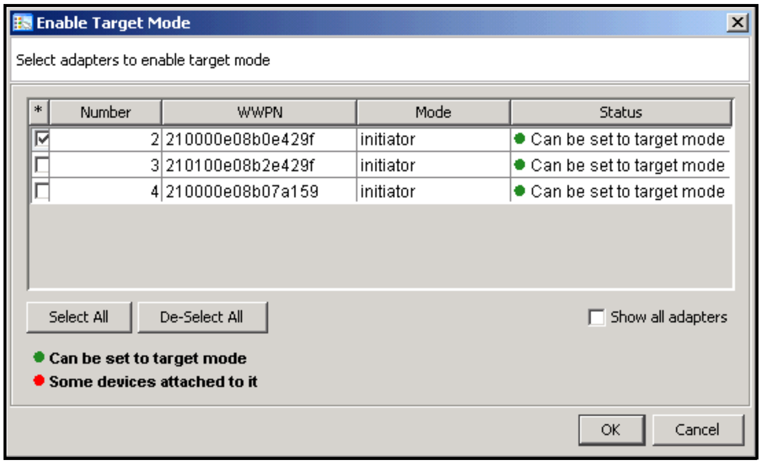
In order to identify your ports, you need to know the WWPN of each. One way to find the WWPN is through the SNS table at your Fibre Channel switch.

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

Note: 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.



Select adapters to enable target mode

*	Number	WWPN	Mode	Status
☑	2	210000e08b0e429f	initiator	● Can be set to target mode
□	3	210100e08b2e429f	initiator	● Can be set to target mode
□	4	210000e08b07a159	initiator	● Can be set to target mode

● Can be set to target mode
● Some devices attached to it

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).

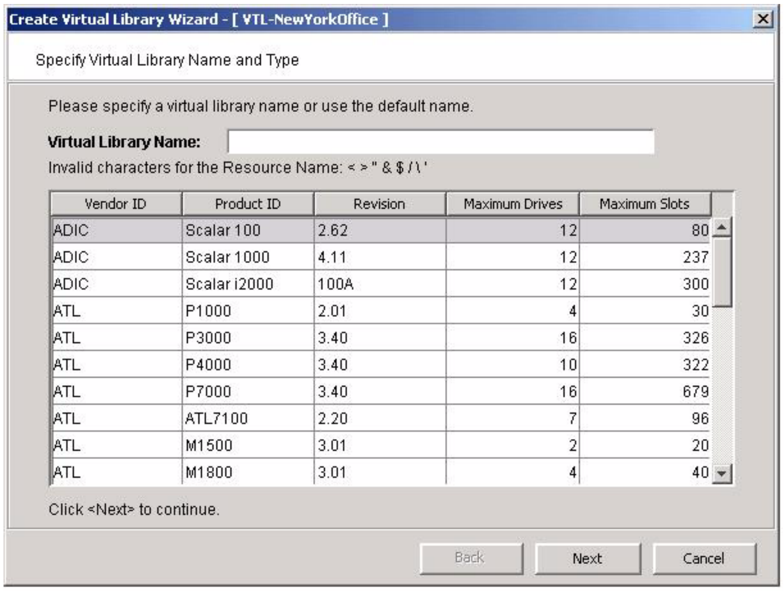
   Express automatically creates the resource for you using an available device(s).

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.



Create Virtual Library Wizard - [VTL-NewYorkOffice]

Specify Virtual Library Name and Type

Please specify a virtual library name or use the default name.

Virtual Library Name:

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

Vendor ID	Product ID	Revision	Maximum Drives	Maximum Slots
ADIC	Scalar 100	2.62	12	80
ADIC	Scalar 1000	4.11	12	237
ADIC	Scalar i2000	100A	12	300
ATL	P1000	2.01	4	30
ATL	P3000	3.40	16	326
ATL	P4000	3.40	10	322
ATL	P7000	3.40	16	679
ATL	ATL7100	2.20	7	96
ATL	M1500	3.01	2	20
ATL	M1800	3.01	4	40

Click <Next> to continue.

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; 1hash 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_lpfc_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.

Note: 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).

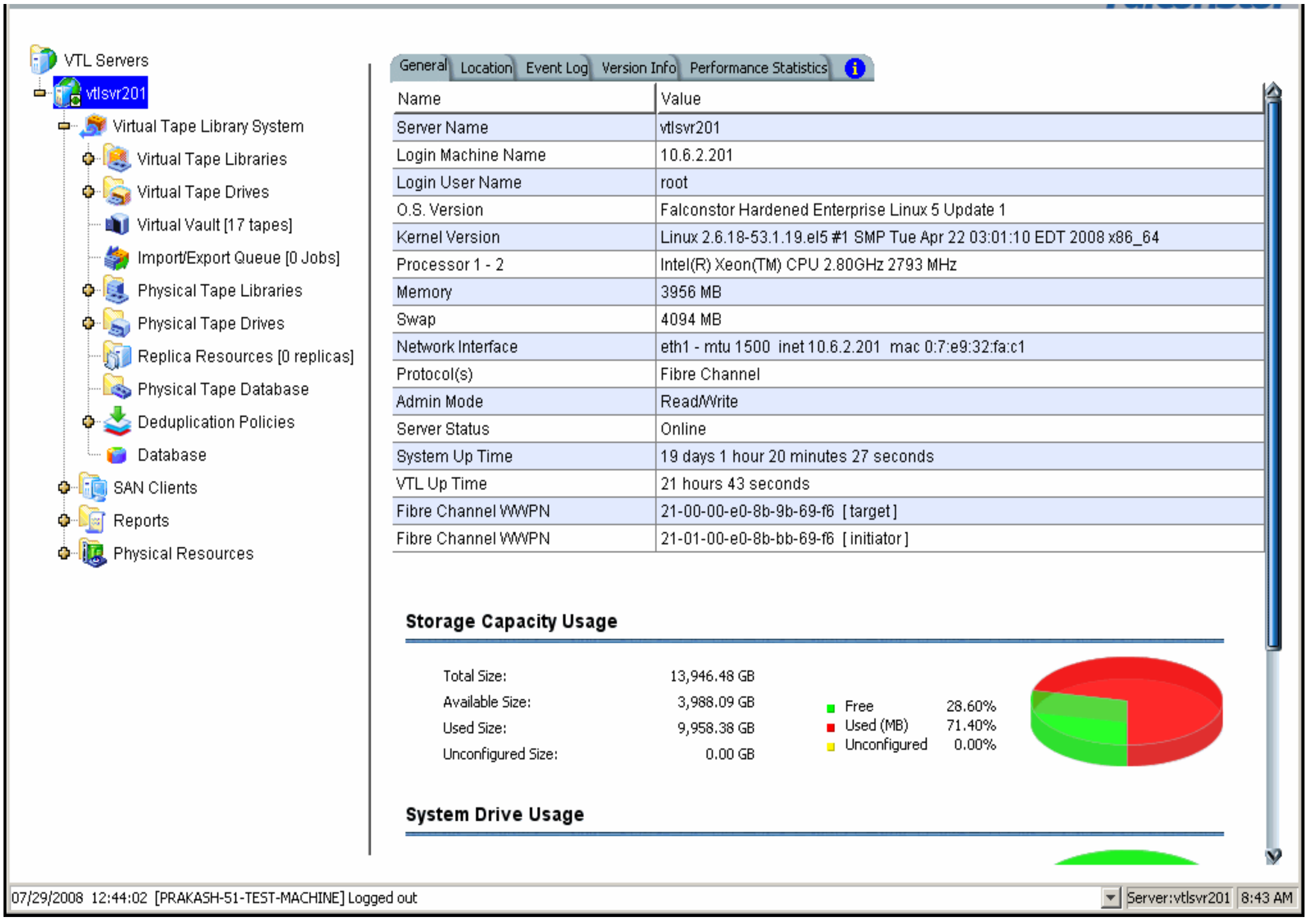
   Once you are connected to a server, the server icon will change to show that you are connected:
   .

   > **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.

   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.



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]

Storage Capacity Usage

Total Size:	13,946.48 GB
Available Size:	3,988.09 GB
Used Size:	9,958.38 GB
Unconfigured Size:	0.00 GB

🟩 Free	28.60%
🟥 Used (MB)	71.40%
🟨 Unconfigured	0.00%

System Drive Usage

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
C	The C icon indicates that this virtual tape drive has compression enabled.
O	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

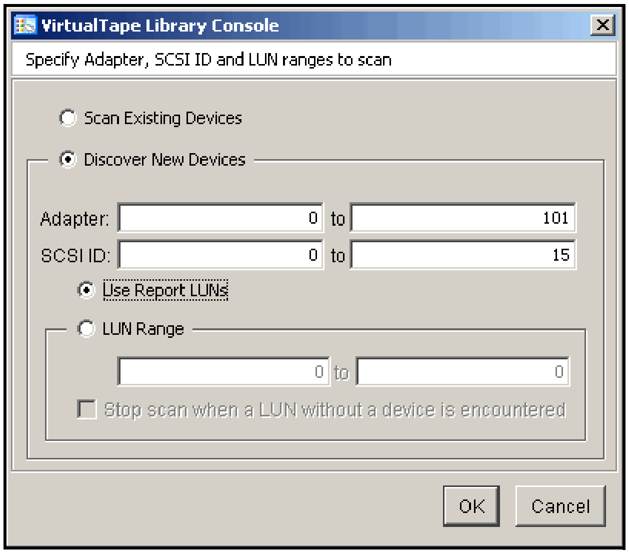
The following table describes the icons that are used to describe physical resources in the console:

Icon	Description
T	The T icon indicates that this is a target port.
I	The I icon indicates that this is an initiator port.
D	The D icon indicates that this is a dual port.
T	The red arrow indicates that this Fibre Channel HBA is down and cannot access its storage.
V	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*.



Specify Adapter, SCSI ID and LUN ranges to scan

○ Scan Existing Devices

● Discover New Devices

Adapter: 0 to 101

SCSI ID: 0 to 15

● Use Report LUNs

○ LUN Range

0 to 0

□ Stop scan when a LUN without a device is encountered

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.

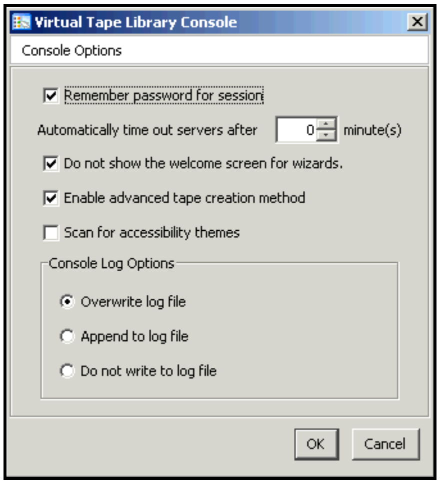
> **Note:** Discovering new devices in Solaris may take a long time. This can lead to the console becoming unresponsive. If this happens, you will need to end the process using the *Windows Task Manager*.

I

Console options

To set options for the console:

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



Virtual Tape Library Console

Console Options

☑ Remember password for session

Automatically time out servers after 0 minute(s)

☑ Do not show the welcome screen for wizards.

☑ Enable advanced tape creation method

□ Scan for accessibility themes

Console Log Options

● Overwrite log file

○ Append to log file

○ Do not write to log file

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.

> **Note:** 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 *Network Configuration*. Using any other third-party utilities will not update the information correctly. Refer to ‘Set up network’ for more information.

Set hostname

If you need to change the hostname of a VTL server, right-click a server and select *System Maintenance* --> *Set Hostname*. The server will automatically reboot when the hostname is changed.

Set date and time

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.

You can also access these setting by double-clicking the time that appears at the bottom right of the console.

> **Note:** We recommend restarting the VTL services if you change the date and time.

Restart server

Right-click a server and select *System Maintenance* --> *Restart VTL* to restart the server processes.

Restart network

Right-click a server and select *System Maintenance* --> *Restart Network* to restart your local network configuration.

Reboot

Right-click a server and select *System Maintenance* --> *Reboot* to reboot your server.

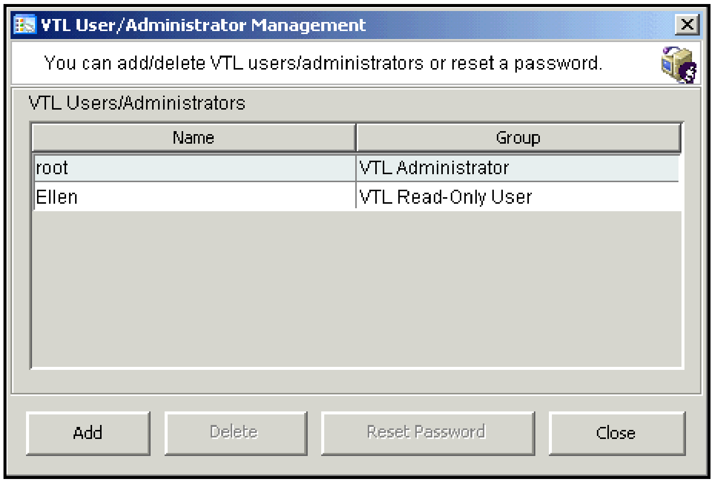
Halt

Right-click a server and select *System Maintenance* --> *Halt* 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*.



You can add/delete VTL users/administrators or reset a password.

Name	Group
root	VTL Administrator
Ellen	VTL Read-Only User

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.

Note: 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	**I**: This is an informational message. No action is required. **W**: This is a warning message that states that something occurred that may require maintenance or corrective action. However, the VTL system is still operational. **E**: This is an error that indicates a failure has occurred such that a device is not available, an operation has failed, or a licensing violation. Corrective action should be taken to resolve the cause of the error. **C**: These are critical errors that stop the system from operating properly.
Date & 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
Server Throughput Report - Provides information about the overall throughput of the VTL server for a specific date or range of dates.	VTL Prime	Yes
SCSI/Fibre Channel Throughput Report - 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
SCSI Device Throughput Report - 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
Physical Resources Configuration Report - Lists the physical resources on the VTL server, including the physical adapters and physical devices.	VTL Prime	No
Disk Space Usage Report - Displays information about the amount of disk space that each SCSI adapter is currently using and how much is available.	VTL Prime	Yes
Disk Space Usage History Report - 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
LUN Report - Displays all of the virtual tapes that are allocated on one or all LUNs.	VTL Prime	Yes
Physical Resources Allocation Report - 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
Physical Resource Allocation Report - 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
Fibre Channel Adapters Configuration Report - 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
Replication Status Report - 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
Virtual Library Information Report - Displays information about each library being emulated, including drives, tapes and slots.	VTL Prime	No
Virtual Tape Information Report - 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
Job Report - 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
Deduplication Status Report - 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
Deduplication Tape Usage Report - Provides statistics for all deduplication tapes and includes detailed information about each of the deduplication tapes.	VTL Prime	No
Deduplication Detailed Status Report - 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
Deduplication Tape Activity Report - 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*.

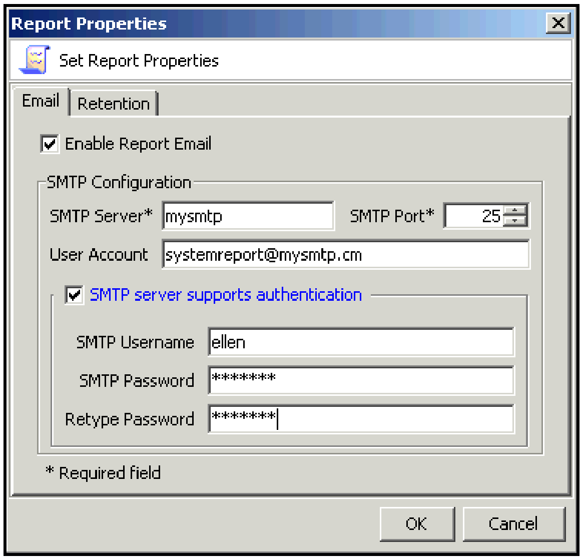
Set report properties

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.



☑ Enable Report Email

SMTP Configuration

SMTP Server* mysmtp

SMTP Port* 25

User Account systemreport@mysmtp.cm

☑ SMTP server supports authentication

SMTP Username ellen

SMTP Password ********

Retype Password ********

* Required field

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

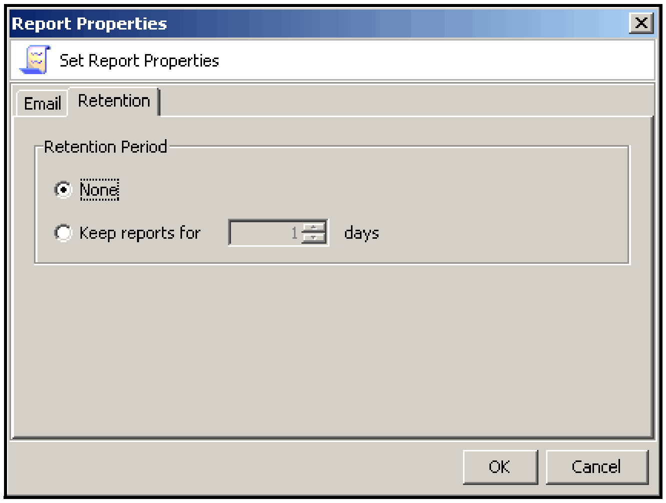
SMTP Port - Specify the mail server port that should be used.

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.



Retention Period

● None

○ Keep reports for 1 days

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.*

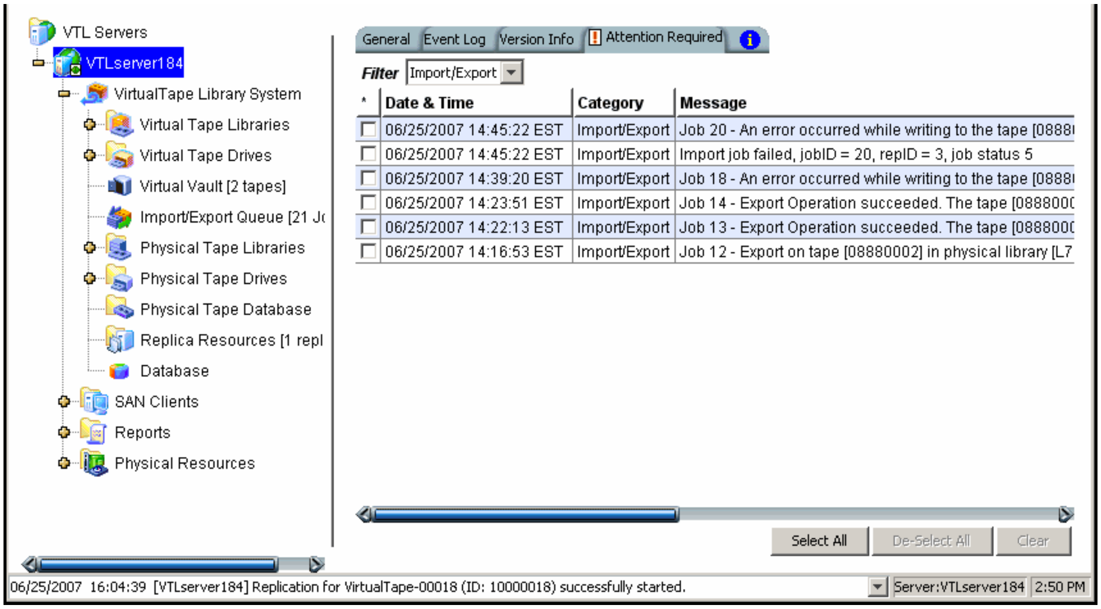
Delete a report

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



Filter: Import/Export

*	Date & Time	Category	Message
□	06/25/2007 14:45:22 EST	Import/Export	Job 20 - An error occurred while writing to the tape [0888
□	06/25/2007 14:45:22 EST	Import/Export	Import job failed, jobID = 20, repID = 3, job status 5
□	06/25/2007 14:39:20 EST	Import/Export	Job 18 - An error occurred while writing to the tape [0888
□	06/25/2007 14:23:51 EST	Import/Export	Job 14 - Export Operation succeeded. The tape [088800
□	06/25/2007 14:22:13 EST	Import/Export	Job 13 - Export Operation succeeded. The tape [088800
□	06/25/2007 14:16:53 EST	Import/Export	Job 12 - Export on tape [08880002] in physical library [L7

06/25/2007 16:04:39 [VTLserver184] Replication for VirtualTape-00018 (ID: 10000018) successfully started.

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. VTL

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

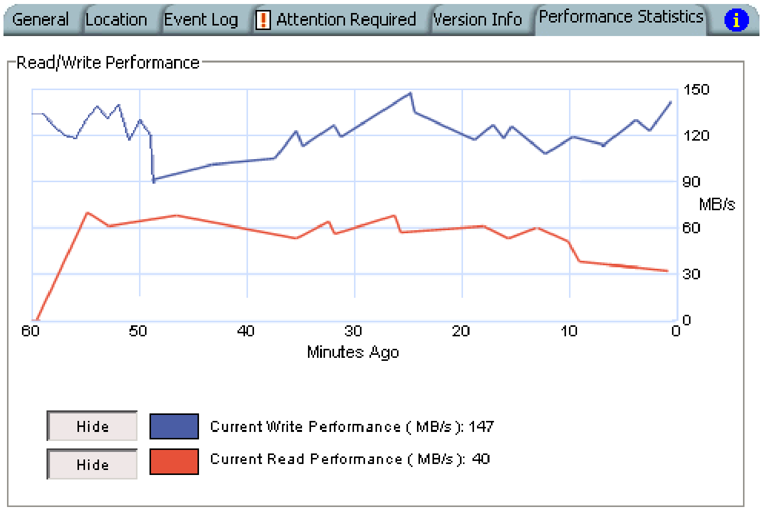
After you have resolved an issue, you can click the check box next to it and click the *Clear* button. You can clear individual issues or you can clear all listed issues by clicking *Select All* and then *Clear*.

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.



🟦 Current Write Performance (MB/s): 147

🟥 Current Read Performance (MB/s): 40

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.

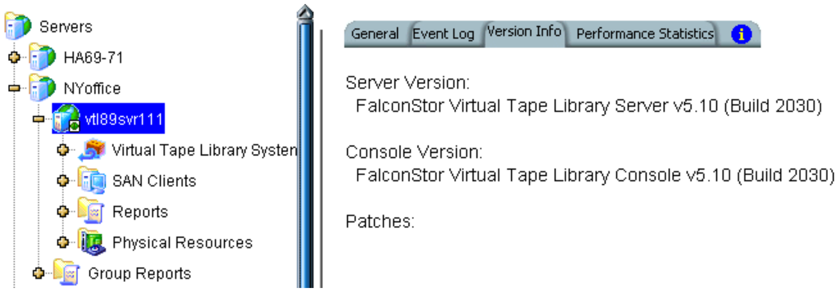
   Refer to 'SNMP traps' for more information.
4. On the *Storage Monitoring* tab, enter the maximum amount of storage that can be used by VTL before you should be alerted.

   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.



Server Version:
FalconStor Virtual Tape Library Server v5.10 (Build 2030)

Console Version:
FalconStor Virtual Tape Library Console v5.10 (Build 2030)

Patches:

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.
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.

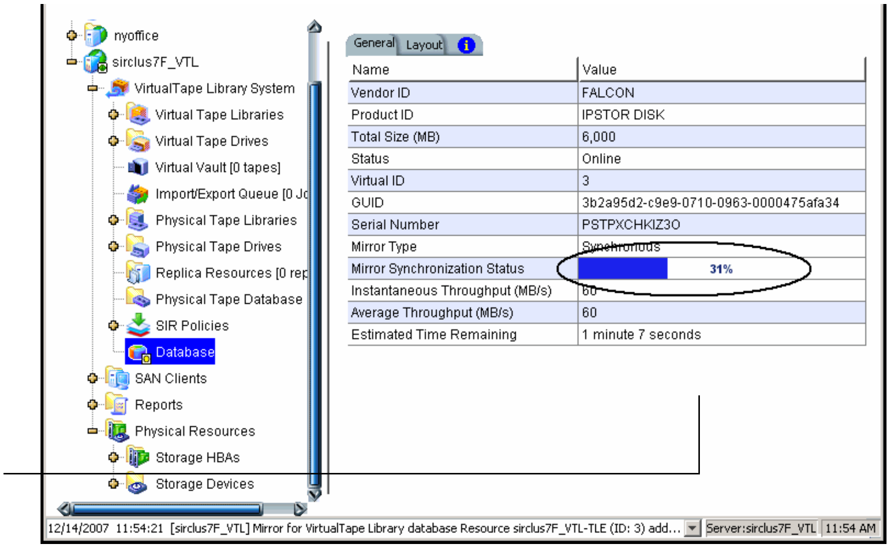
In order to mirror the database, you must have at least two physical devices (preferably on different controllers) because the mirror cannot be on the same disk as the VTL database.

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	PSTPXCHKIZ3O
Mirror Type	Synchronous
Mirror Synchronization Status	31%
Instantaneous Throughput (MB/s)	60
Average Throughput (MB/s)	60
Estimated Time Remaining	1 minute 7 seconds

12/14/2007 11:54:21 [sirclus7F_VTL] Mirror for VirtualTape Library database Resource sirclus7F_VTL-TLE (ID: 3) add... Server:sirclus7F_VTL 11:54 AM

Current status of mirroring configuration.

- *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

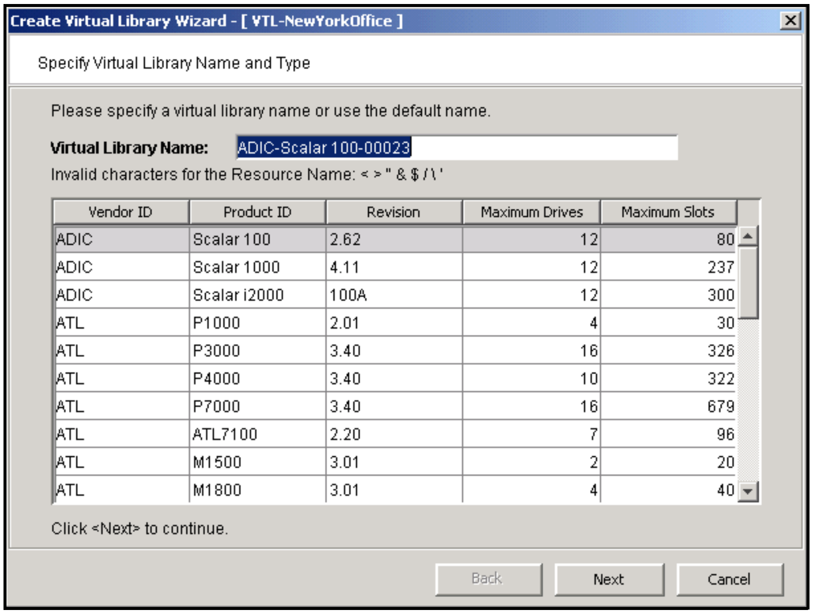
Create virtual tape libraries

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*.

Note: If you have recently added additional storage to your VTL system, before you can use it to create a virtual tape library, you must reserve it for virtual use. To do this: Right-click *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.



Create Virtual Library Wizard - [VTL-NewYorkOffice]

Specify Virtual Library Name and Type

Please specify a virtual library name or use the default name.

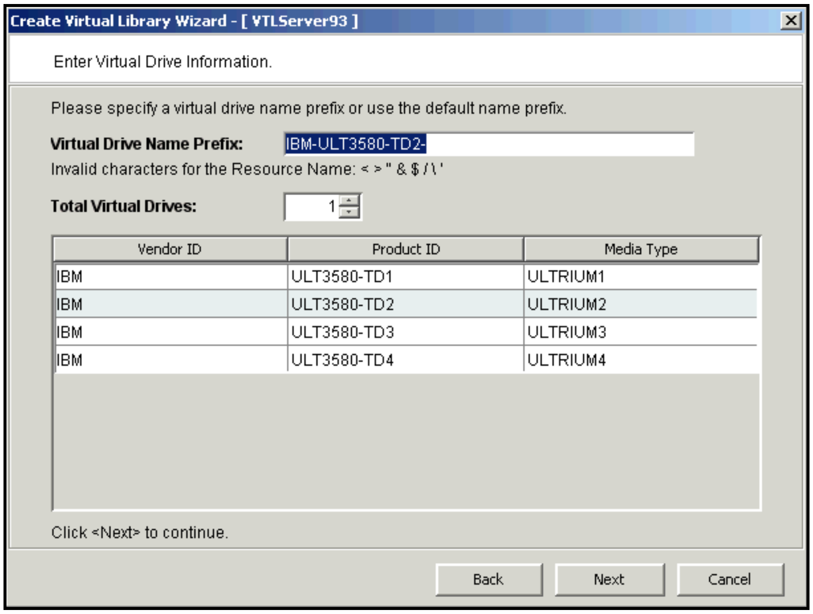
Virtual Library Name: ADIC-Scalar 100-00023

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

Vendor ID	Product ID	Revision	Maximum Drives	Maximum Slots
ADIC	Scalar 100	2.62	12	80
ADIC	Scalar 1000	4.11	12	237
ADIC	Scalar i2000	100A	12	300
ATL	P1000	2.01	4	30
ATL	P3000	3.40	16	326
ATL	P4000	3.40	10	322
ATL	P7000	3.40	16	679
ATL	ATL7100	2.20	7	96
ATL	M1500	3.01	2	20
ATL	M1800	3.01	4	40

Click <Next> to continue.

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



Create Virtual Library Wizard - [VTLServer93]

Enter Virtual Drive Information.

Please specify a virtual drive name prefix or use the default name prefix.

Virtual Drive Name Prefix: IBM-ULT3580-TD2-

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

Total Virtual Drives: 1

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

Click <Next> to continue.

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

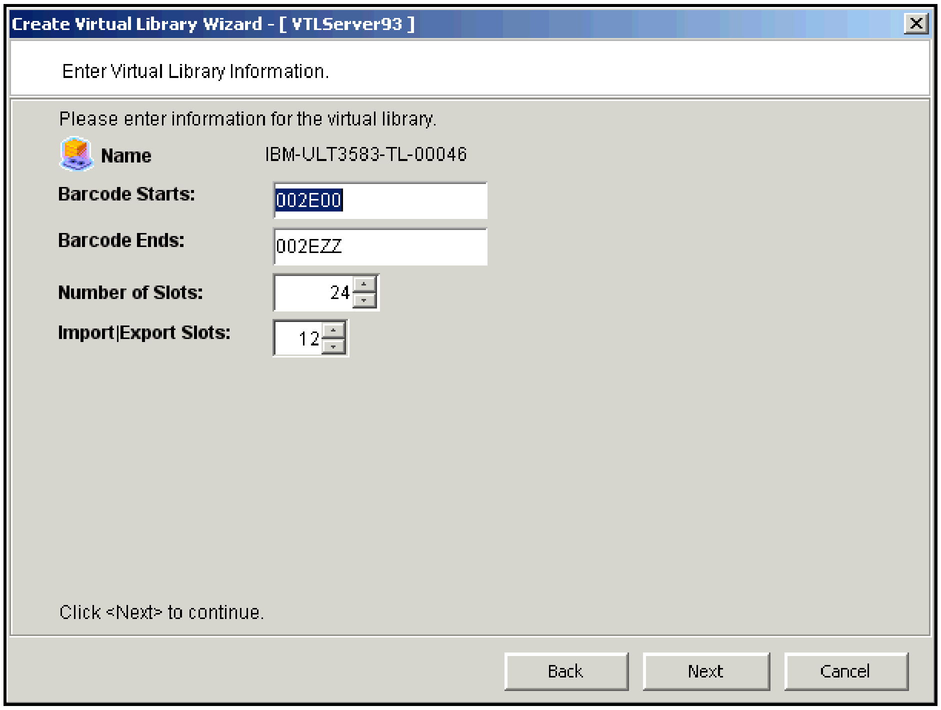
Total Virtual Drives - Determines the number of virtual tape drives available. This translates into the number of concurrent backup jobs that can run. Backup software licensing considerations may affect the number of tape drives you wish to present to each client server. This number can exceed the standard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

Note: 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.



Create Virtual Library Wizard - [VTLServer93]

Enter Virtual Library Information.

Please enter information for the virtual library.

Name IBM-ULT3583-TL-00046

Barcode Starts: 002E00

Barcode Ends: 002EZZ

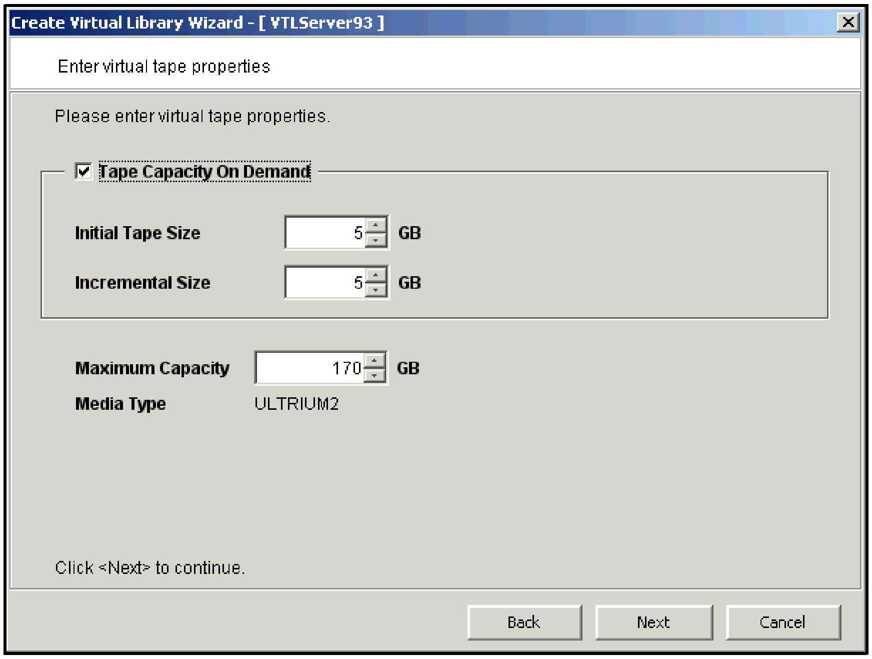
Number of Slots: 24

Import|Export Slots: 12

Click <Next> to continue.

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.



Create Virtual Library Wizard - [VTLServer93]

Enter virtual tape properties

Please enter virtual tape properties.

☑ Tape Capacity On Demand

Initial Tape Size 5 GB

Incremental Size 5 GB

Maximum Capacity 170 GB

Media Type ULTRIUM2

Click <Next> to continue.

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.

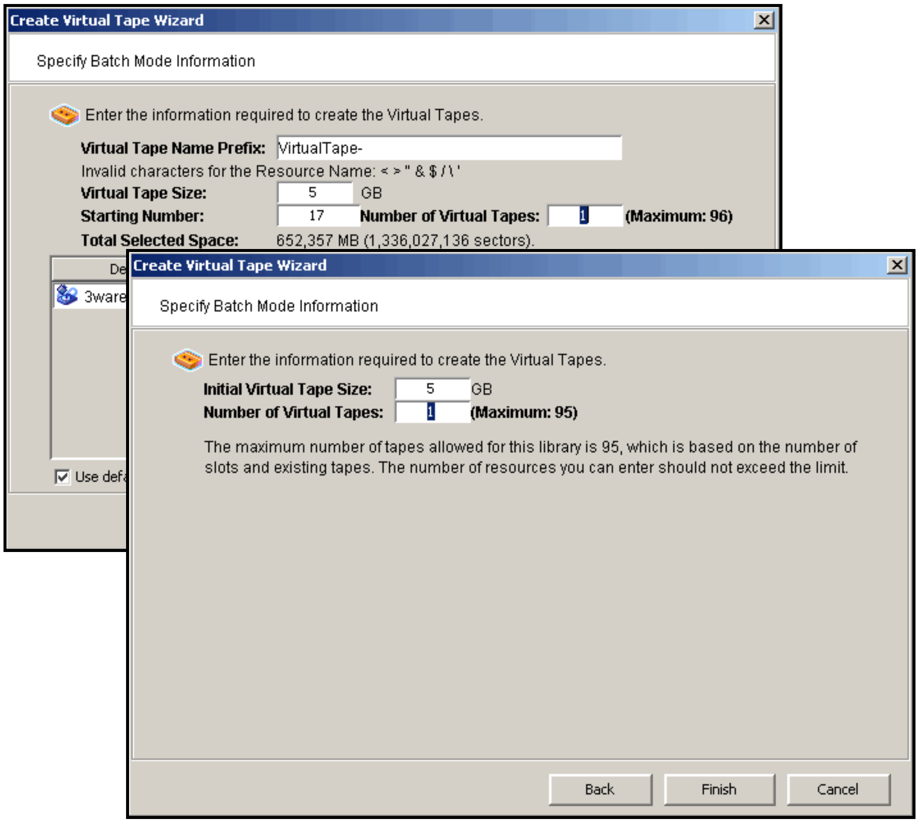
   Storage space is allocated from the local server even if this server is part of a multi-node group.

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.

4. 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.

Create Virtual Tape Wizard

Specify Batch Mode Information

Enter the information required to create the Virtual Tapes.

Virtual Tape Name Prefix: VirtualTape-

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

Virtual Tape Size: 5 GB

Starting Number: 17 **Number of Virtual Tapes:** 1 **(Maximum: 96)**

Total Selected Space: 652,357 MB (1,336,027,136 sectors).

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

Create Virtual Tape Wizard

Specify Batch Mode Information

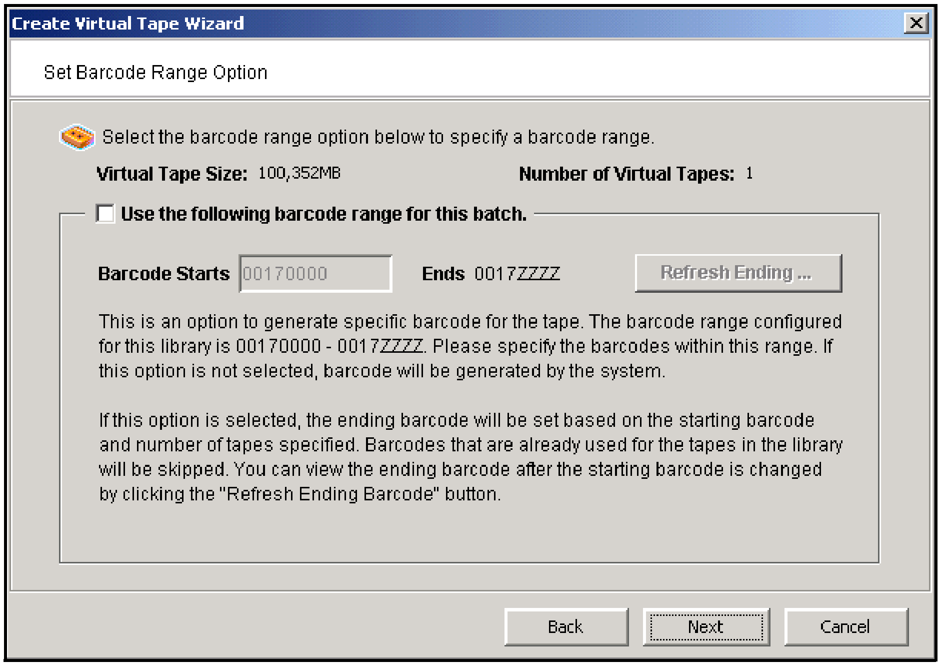
Enter the information required to create the Virtual Tapes.

Initial Virtual Tape Size: 5 GB

Number of Virtual Tapes: 1 **(Maximum: 95)**

The maximum number of tapes allowed for this library is 95, which is based on the number of slots and existing tapes. The number of resources you can enter should not exceed the limit.

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



Create Virtual Tape Wizard

Set Barcode Range Option

Select the barcode range option below to specify a barcode range.

Virtual Tape Size: 100,352MB **Number of Virtual Tapes:** 1

☐ **Use the following barcode range for this batch.**

Barcode Starts 00170000 **Ends** 0017ZZZZ

This is an option to generate specific barcode for the tape. The barcode range configured for this library is 00170000 - 0017ZZZZ. Please specify the barcodes within this range. If this option is not selected, barcode will be generated by the system.

If this option is selected, the ending barcode will be set based on the starting barcode and number of tapes specified. Barcodes that are already used for the tapes in the library will be skipped. You can view the ending barcode after the starting barcode is changed by clicking the "Refresh Ending Barcode" button.

6. 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.

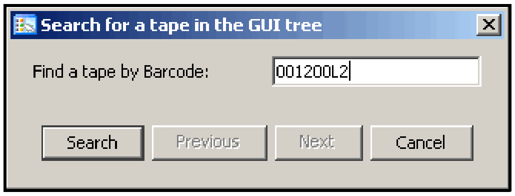
Locate and display virtual tapes in the console

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.*



Search for a tape in the GUI tree

Find a tape by Barcode: 001200L2

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:

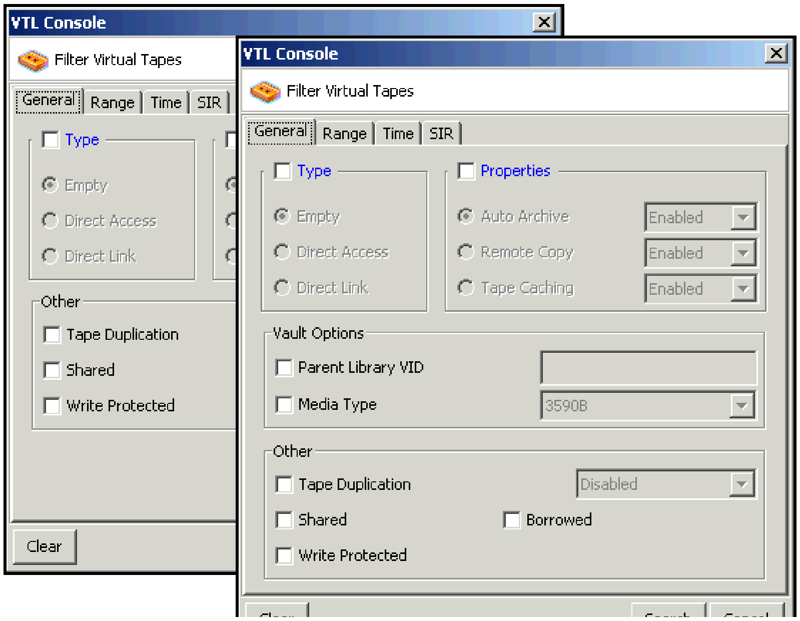
1. Select *Barcode* or *Name*.
2. Indicate whether they should be sorted in *Ascending* or *Descending* order.

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.

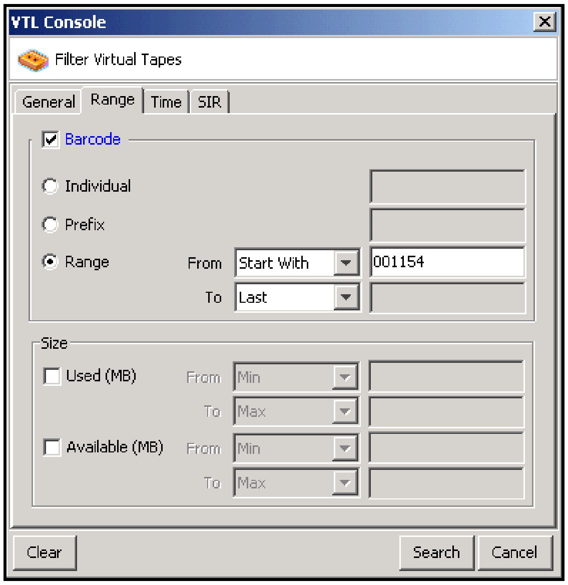
You will see this dialog if you started from the *Tapes* object.



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.


VTL Console

Filter Virtual Tapes

General | Range | Time | SIR

☑ Barcode

○ Individual

○ Prefix

● Range From Start With 001154

To Last

Size

☐ Used (MB) From Min

To Max

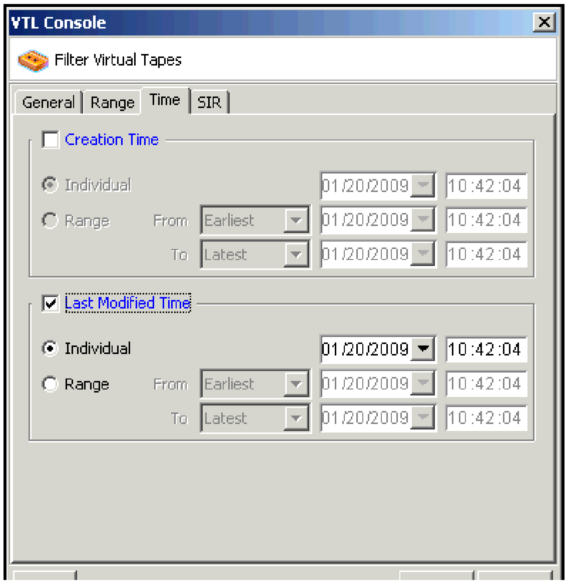
☐ Available (MB) From Min

To Max

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.


VTL Console

Filter Virtual Tapes

General | Range | Time | SIR

☐ Creation Time

● Individual 01/20/2009 10:42:04

○ Range From Earliest 01/20/2009 10:42:04

To Latest 01/20/2009 10:42:04

☑ Last Modified Time

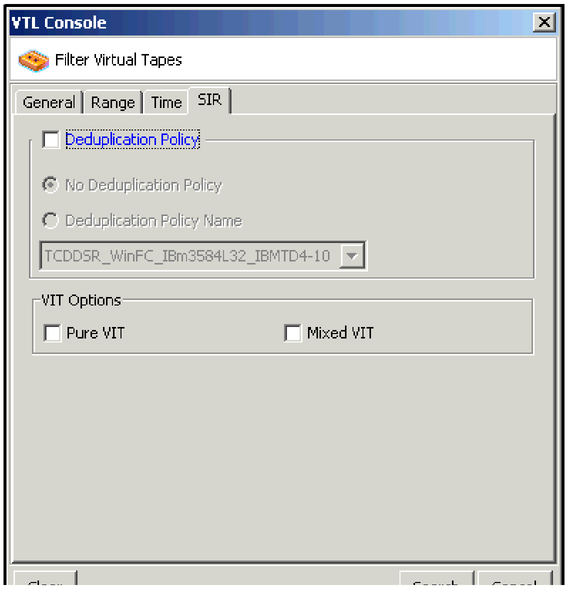
● Individual 01/20/2009 10:42:04

○ Range From Earliest 01/20/2009 10:42:04

To Latest 01/20/2009 10:42:04

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.



□ Deduplication Policy

● No Deduplication Policy

○ Deduplication Policy Name

TCDDSR_WinFC_IBm3584L32_IBMTD4-10

VIT Options

□ Pure VIT □ Mixed VIT

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)

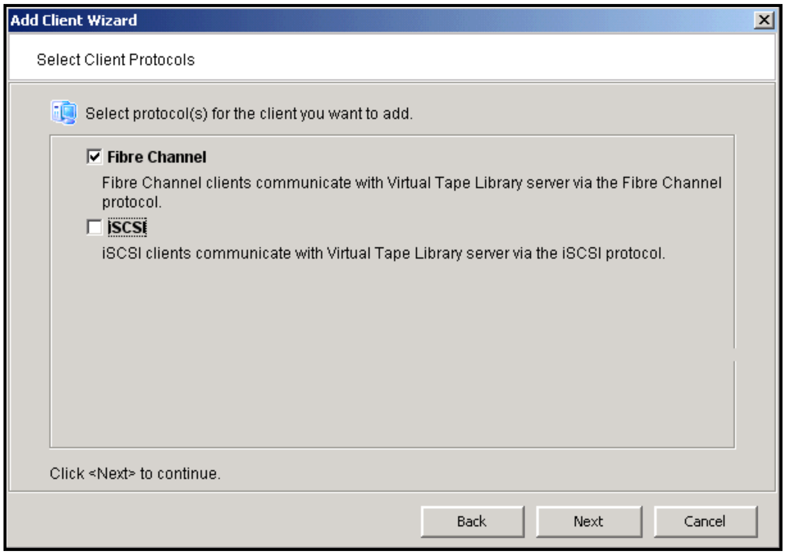
You can add SAN Clients in the following two ways:

- 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.



Add Client Wizard

Select Client Protocols

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

☑ **Fibre Channel**

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

☐ **iSCSI**

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

Click <Next> to continue.

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.

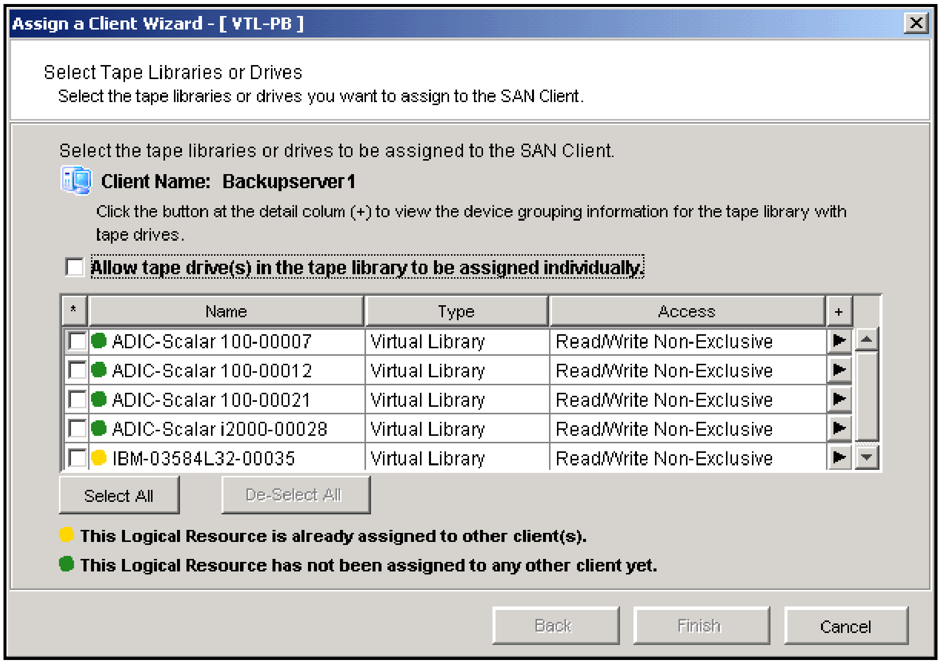
  Note: The *Everyone* generic client is not a supported option for SUN VTL. It may be used in a test environment but for security purposes it should not be used in a production environment. For security purposes, you should assign specific WWPNs to specific clients.

  Note:

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.



Assign a Client Wizard - [VTL-PB]

Select Tape Libraries or Drives

Select the tape libraries or drives you want to assign to the SAN Client.

Select the tape libraries or drives to be assigned to the SAN Client.

Client Name: Backupserver1

Click the button at the detail colum (+) to view the device grouping information for the tape library with tape drives.

☐ **Allow tape drive(s) in the tape library to be assigned individually.**

*	Name	Type	Access	+
☐	● ADIC-Scalar 100-00007	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ADIC-Scalar 100-00012	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ADIC-Scalar 100-00021	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ADIC-Scalar i2000-00028	Virtual Library	Read/Write Non-Exclusive	▶
☐	● IBM-03584L32-00035	Virtual Library	Read/Write Non-Exclusive	▶

● **This Logical Resource is already assigned to other client(s).**

● **This Logical Resource has not been assigned to any other client yet.**

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.

> **Note:** 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.

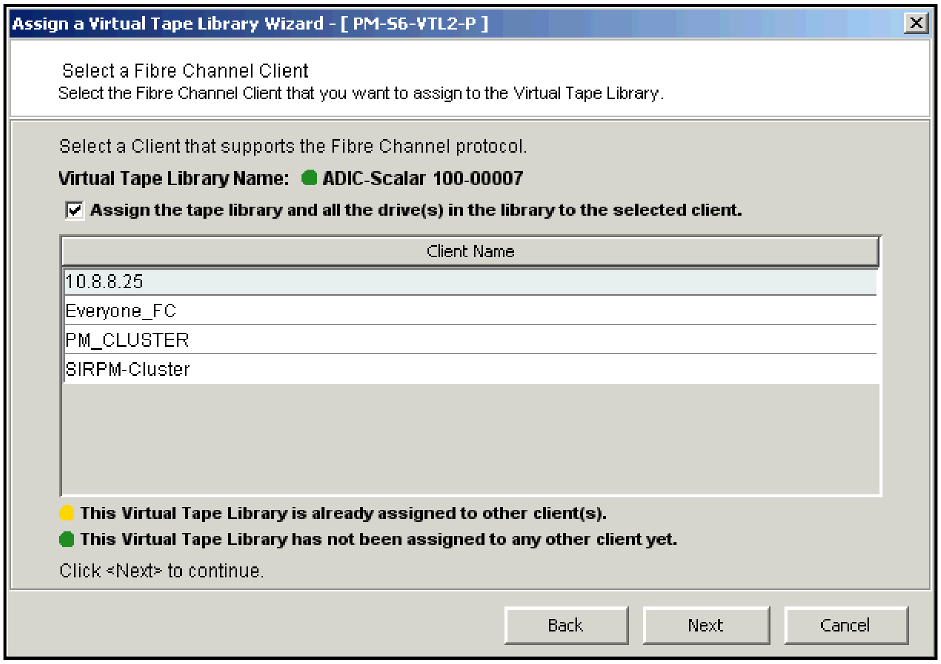
   For Windows, *Control Panel* --> *Computer Management* --> *Device Manager* --> right-click the device in the right pane --> *Scan for hardware changes*.
4. Use your backup software to discover the library.

   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.



Assign a Virtual Tape Library Wizard - [PM-S6-VTL2-P]

Select a Fibre Channel Client

Select the Fibre Channel Client that you want to assign to the Virtual Tape Library.

Select a Client that supports the Fibre Channel protocol.

Virtual Tape Library Name: ● **ADIC-Scalar 100-00007**

☑ **Assign the tape library and all the drive(s) in the library to the selected client.**

Client Name
10.8.8.25
Everyone_FC
PM_CLUSTER
SIRPM-Cluster

● **This Virtual Tape Library is already assigned to other client(s).**

● **This Virtual Tape Library has not been assigned to any other client yet.**

Click <Next> to continue.

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.

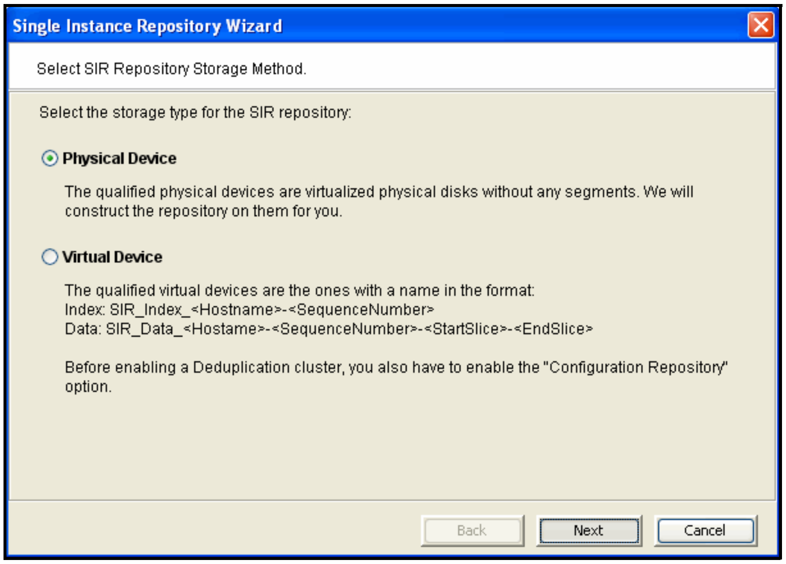
When replication is configured as part of a deduplication policy, the deduplication repository and metadata are replicated.

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*.



Single Instance Repository Wizard

Select SIR Repository Storage Method.

Select the storage type for the SIR repository:

● Physical Device

The qualified physical devices are virtualized physical disks without any segments. We will construct the repository on them for you.

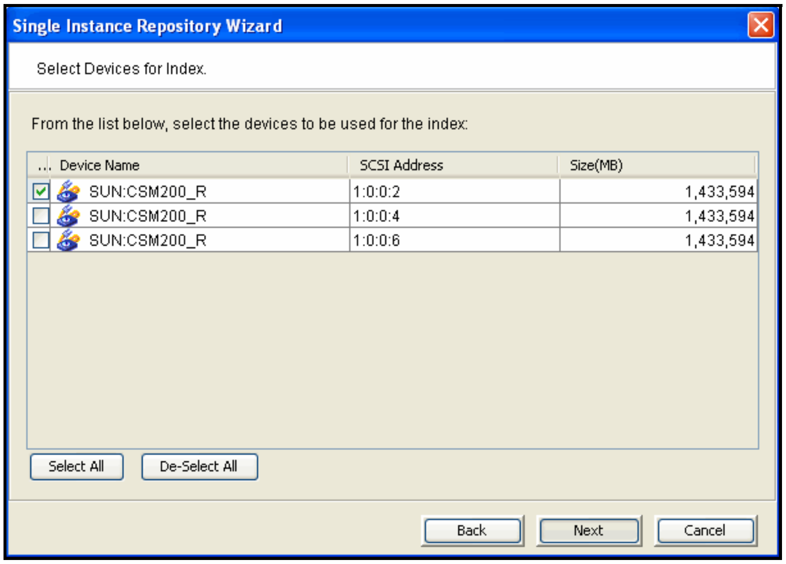
○ Virtual Device

The qualified virtual devices are the ones with a name in the format:
Index: SIR_Index_<Hostname>-<SequenceNumber>
Data: SIR_Data_<Hostame>-<SequenceNumber>-<StartSlice>-<EndSlice>

Before enabling a Deduplication cluster, you also have to enable the "Configuration Repository" option.

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.*



Single Instance Repository Wizard

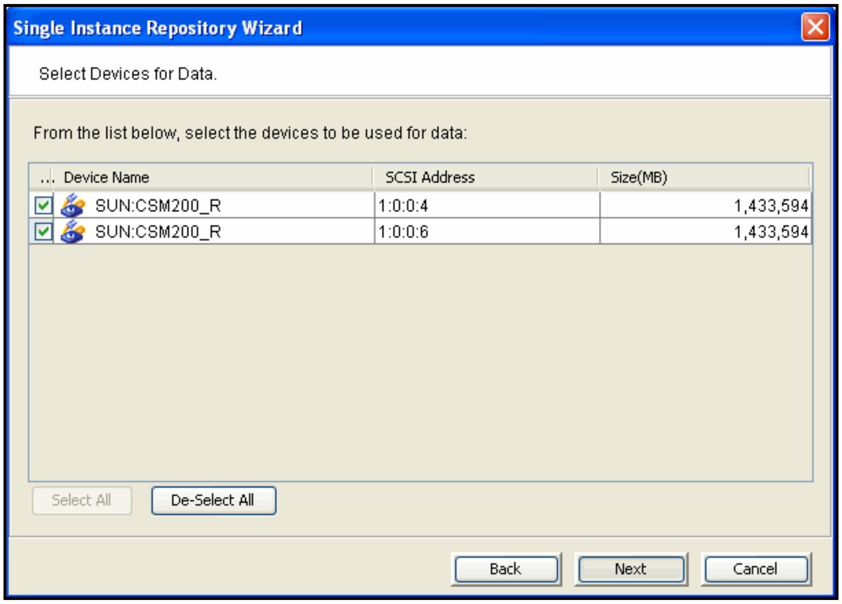
Select Devices for Index.

From the list below, select the devices to be used for the index:

...	Device Name	SCSI Address	Size(MB)
☑	SUN:CSM200_R	1:0:0:2	1,433,594
☐	SUN:CSM200_R	1:0:0:4	1,433,594
☐	SUN:CSM200_R	1:0:0:6	1,433,594

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.



Select Devices for Data.

From the list below, select the devices to be used for data:

...	Device Name	SCSI Address	Size(MB)
☑	SUN:CSM200_R	1:0:0:4	1,433,594
☑	SUN:CSM200_R	1:0:0:6	1,433,594

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.

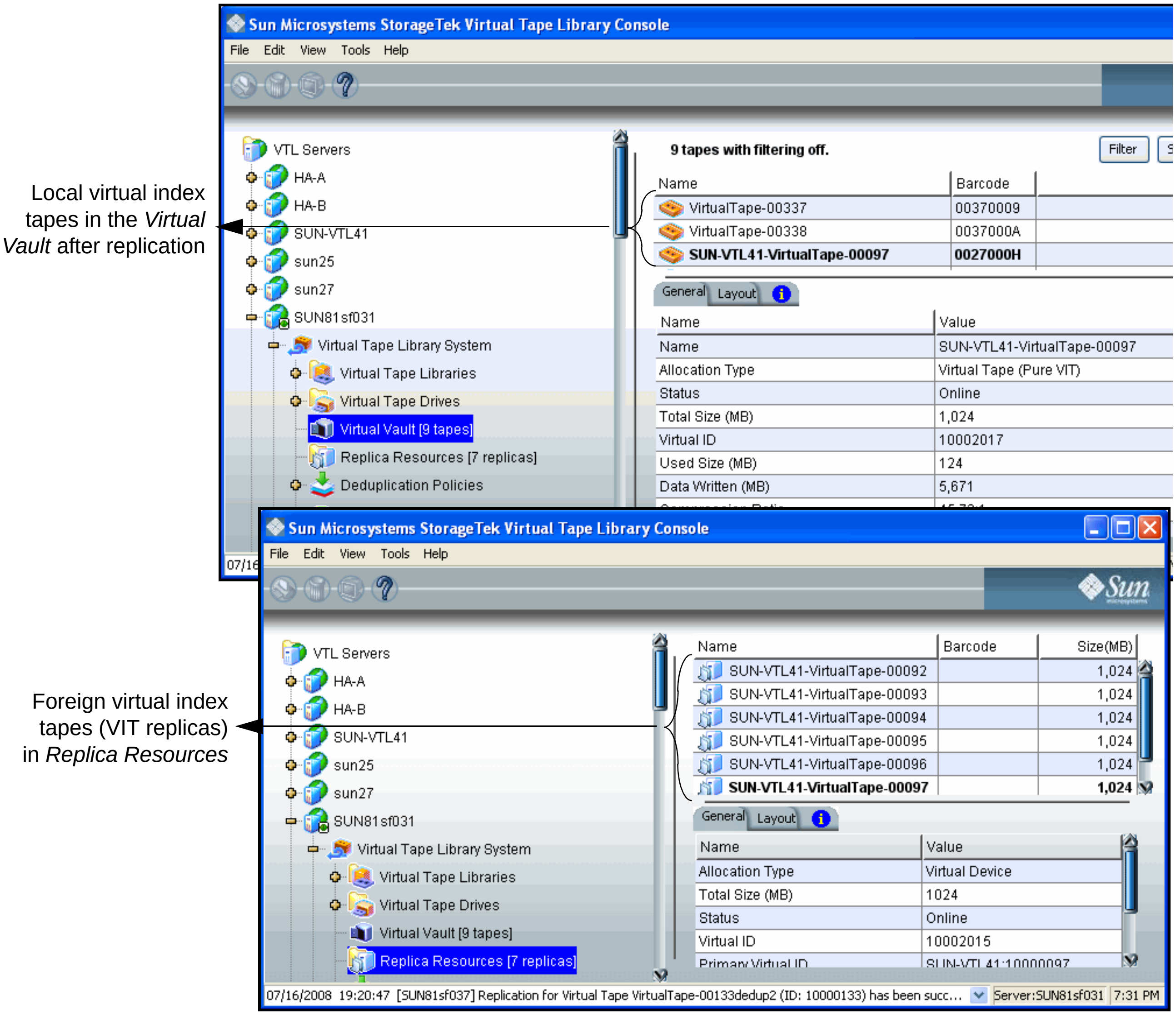
Replication from the source server to the target server occurs via Fibre Channel or iSCSI. The target server is usually located at a remote location. If a disaster occurs and the replica is needed, the administrator can move the replicated tape from the virtual vault to its virtual tape library so that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

Note: 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.



Local virtual index tapes in the *Virtual Vault* after replication

9 tapes with filtering off.

Name	Barcode
VirtualTape-00337	00370009
VirtualTape-00338	0037000A
SUN-VTL41-VirtualTape-00097	**0027000H**

Name	Value
Name	SUN-VTL41-VirtualTape-00097
Allocation Type	Virtual Tape (Pure VIT)
Status	Online
Total Size (MB)	1,024
Virtual ID	10002017
Used Size (MB)	124
Data Written (MB)	5,671

Foreign virtual index tapes (VIT replicas) in *Replica Resources*

Name	Barcode	Size(MB)
SUN-VTL41-VirtualTape-00092		1,024
SUN-VTL41-VirtualTape-00093		1,024
SUN-VTL41-VirtualTape-00094		1,024
SUN-VTL41-VirtualTape-00095		1,024
SUN-VTL41-VirtualTape-00096		1,024
SUN-VTL41-VirtualTape-00097		**1,024**

Name	Value
Allocation Type	Virtual Device
Total Size (MB)	1024
Status	Online
Virtual ID	10002015
Primary Virtual ID	SUN-VTL41:10000097

07/16/2008 19:20:47 [SUN81sf037] Replication for Virtual Tape VirtualTape-00133dedup2 (ID: 10000133) has been succ... Server:SUN81sf031 7:31 PM

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.

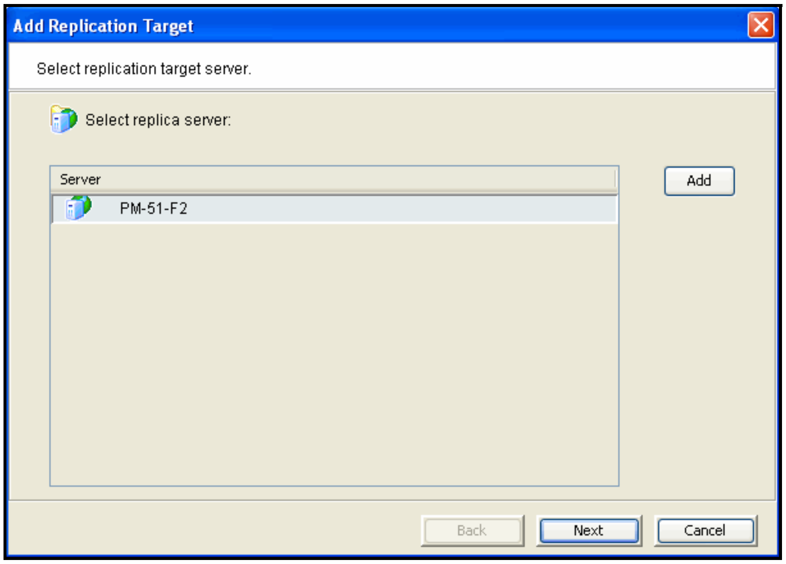
While most customers choose to use a Fibre Channel switch to connect their VTL and deduplication appliances, it is also possible to direct-connect the appliances. If you are using an iSCSI connection, the iSCSI option must be enabled on both servers. If you are direct-connecting the appliances, the source 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).

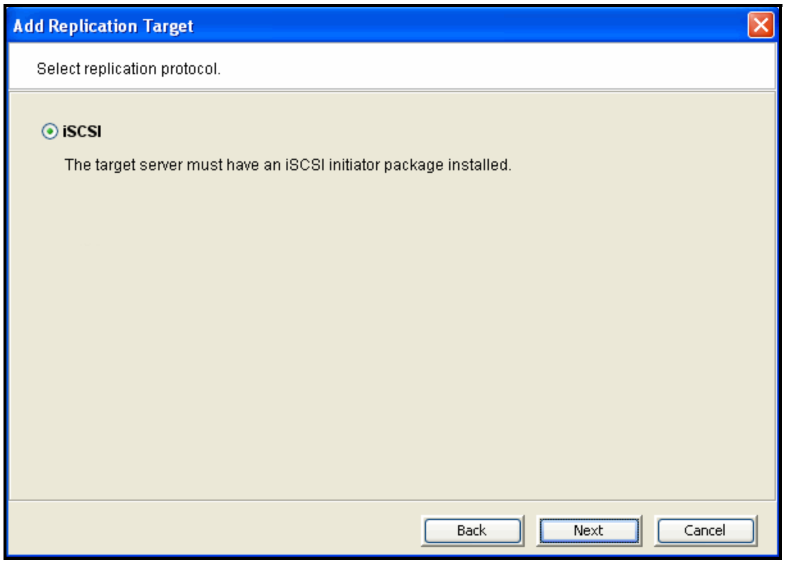


3. If the server is not listed, select *Add*.

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.



Add Replication Target

Select replication protocol.

● iSCSI

The target server must have an iSCSI initiator package installed.

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

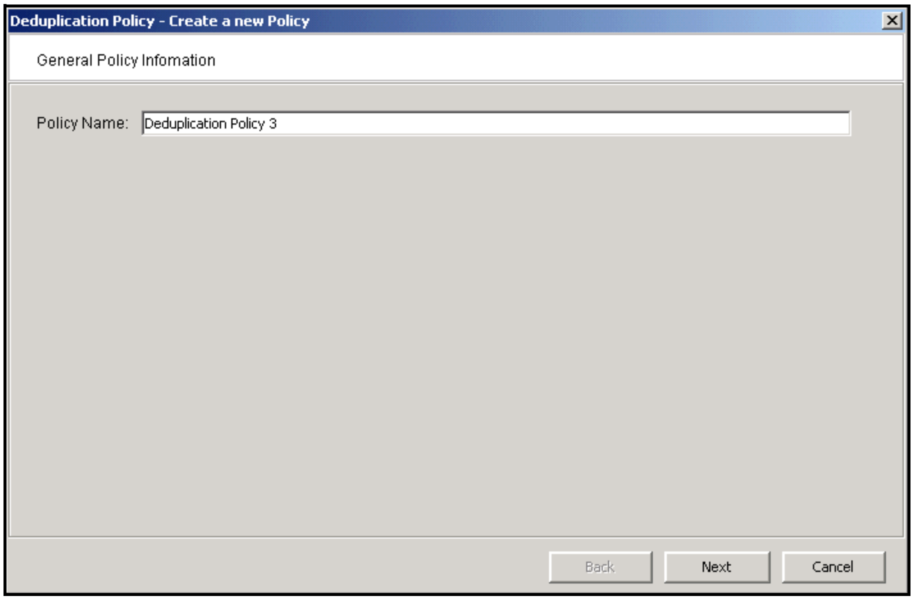
Add deduplication policies

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.

Note: 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.

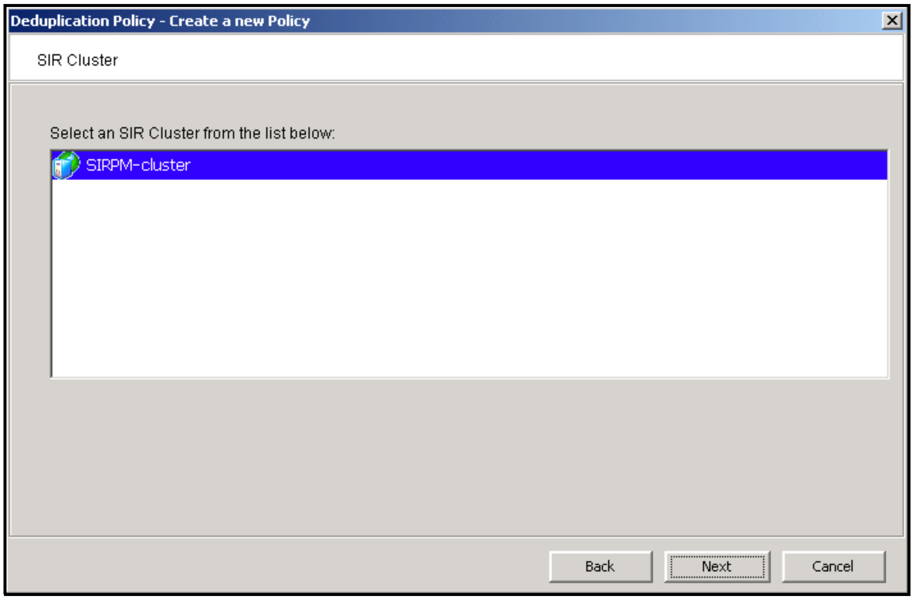
1. On your VTL server, right-click on the *Deduplication Policies* object and select *New*.

2. For a new policy, enter a name for the policy.


Deduplication Policy - Create a new Policy
General Policy Infomation
Back
Next
Cancel

Policy Name: Deduplication Policy 3

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



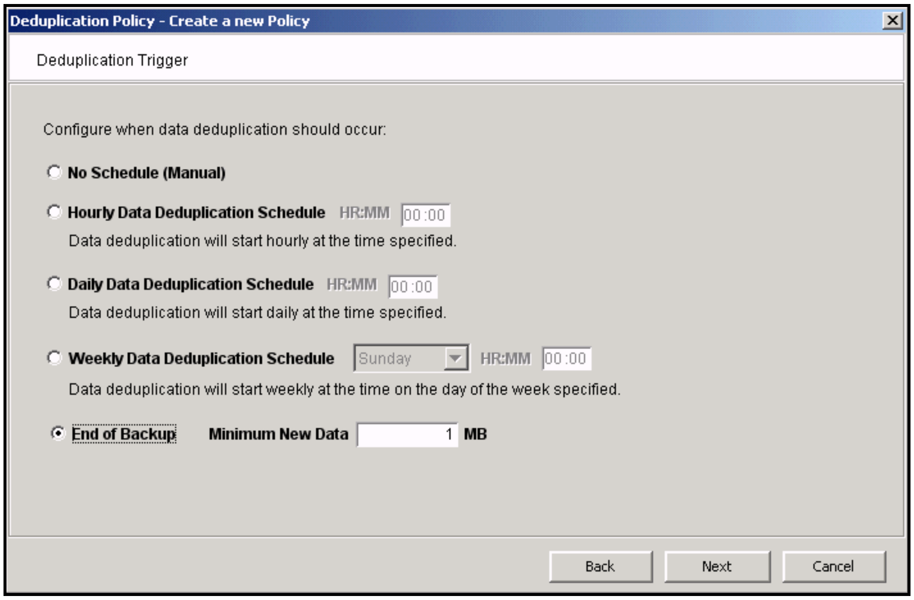
Deduplication Policy - Create a new Policy

SIR Cluster

Select an SIR Cluster from the list below:

SIRPM-cluster

4. Indicate how often deduplication should occur.



Deduplication Policy - Create a new Policy

Deduplication Trigger

Configure when data deduplication should occur:

○ No Schedule (Manual)

○ Hourly Data Deduplication Schedule HR:MM 00:00
Data deduplication will start hourly at the time specified.

○ Daily Data Deduplication Schedule HR:MM 00:00
Data deduplication will start daily at the time specified.

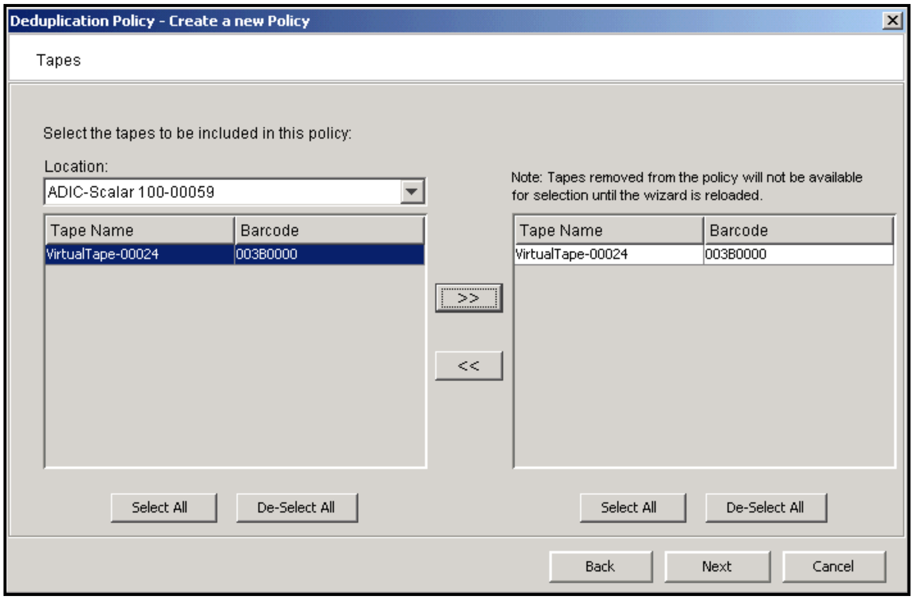
○ Weekly Data Deduplication Schedule Sunday HR:MM 00:00
Data deduplication will start weekly at the time on the day of the week specified.

● End of Backup Minimum New Data 1 MB

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.

Note: 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.



Deduplication Policy - Create a new Policy

Tapes

Select the tapes to be included in this policy:

Location: ADIC-Scalar 100-00059

Note: Tapes removed from the policy will not be available for selection until the wizard is reloaded.

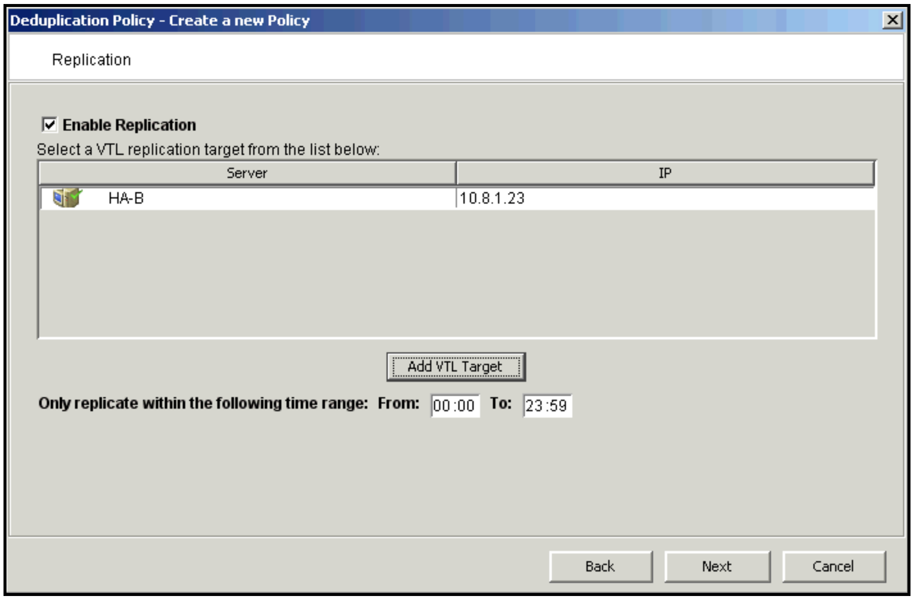
Tape Name	Barcode
VirtualTape-00024	003B0000

Tape Name	Barcode
VirtualTape-00024	003B0000

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.



Deduplication Policy - Create a new Policy

Replication

☑ **Enable Replication**

Select a VTL replication target from the list below:

Server	IP
HA-B	10.8.1.23

Only replicate within the following time range: From: 00:00 **To:** 23:59

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

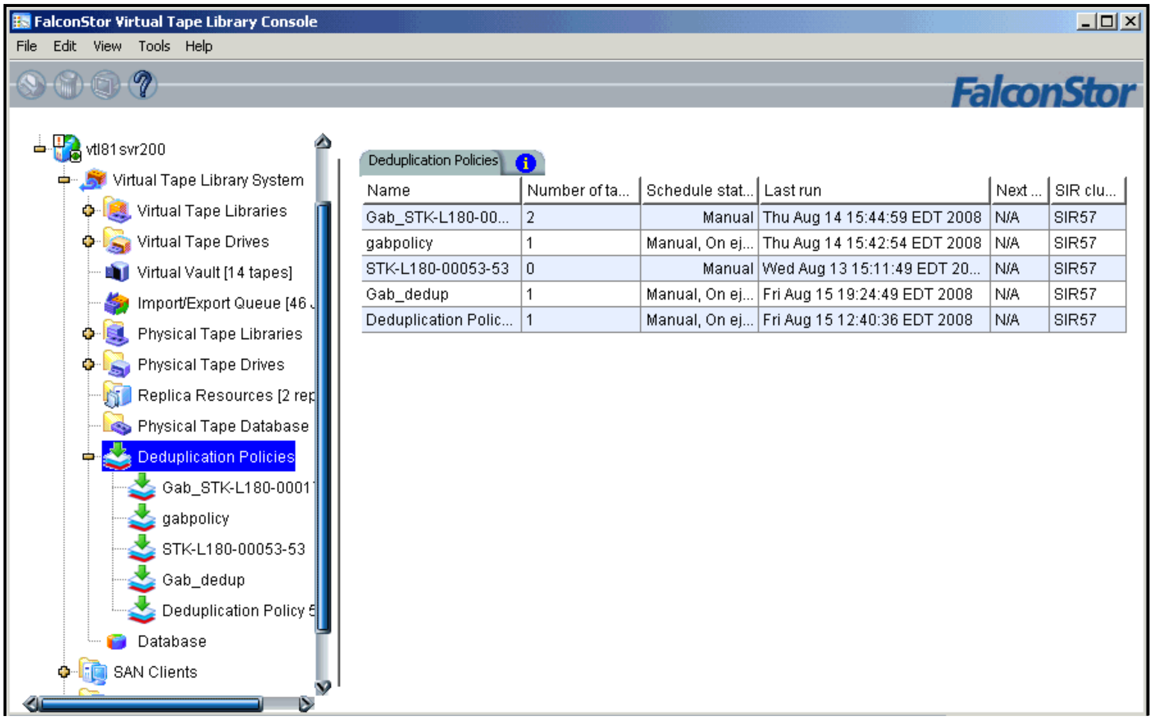
From the console, you can view the following:

- 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.



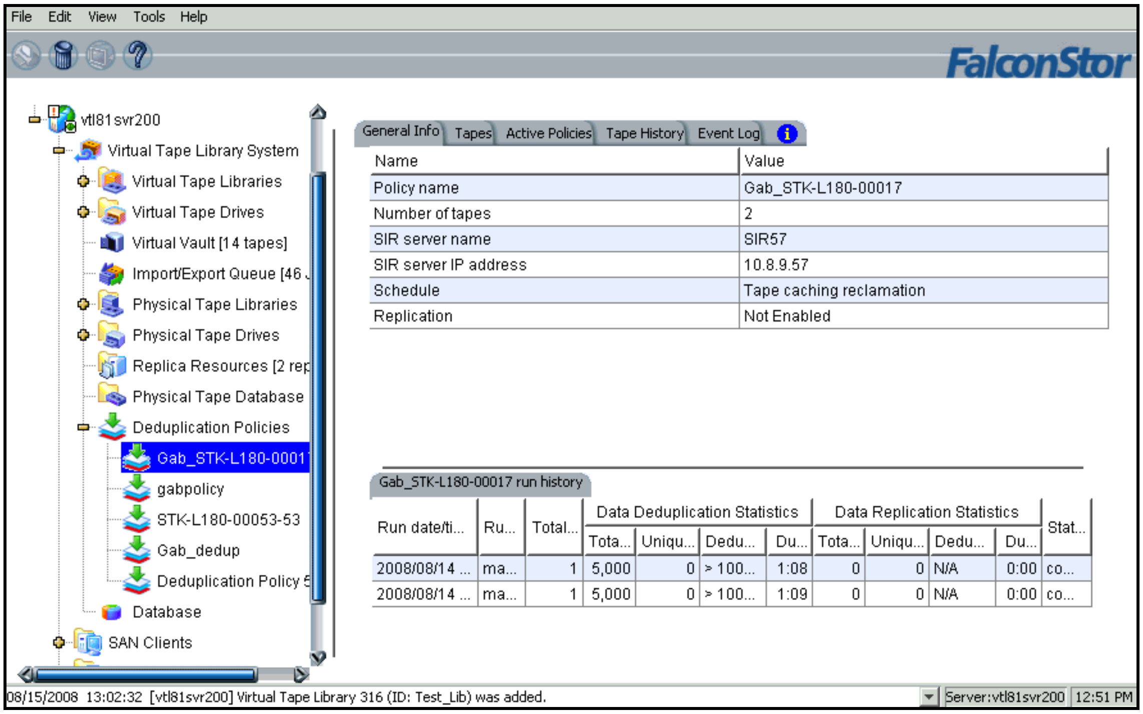
Name	Number of ta...	Schedule stat...	Last run	Next ...	SIR clu...
Gab_STK-L180-00...	2	Manual	Thu Aug 14 15:44:59 EDT 2008	N/A	SIR57
gabpolicy	1	Manual, On ej...	Thu Aug 14 15:42:54 EDT 2008	N/A	SIR57
STK-L180-00053-53	0	Manual	Wed Aug 13 15:11:49 EDT 20...	N/A	SIR57
Gab_dedup	1	Manual, On ej...	Fri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

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.



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

Gab_STK-L180-00017 run history

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...

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 then 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.

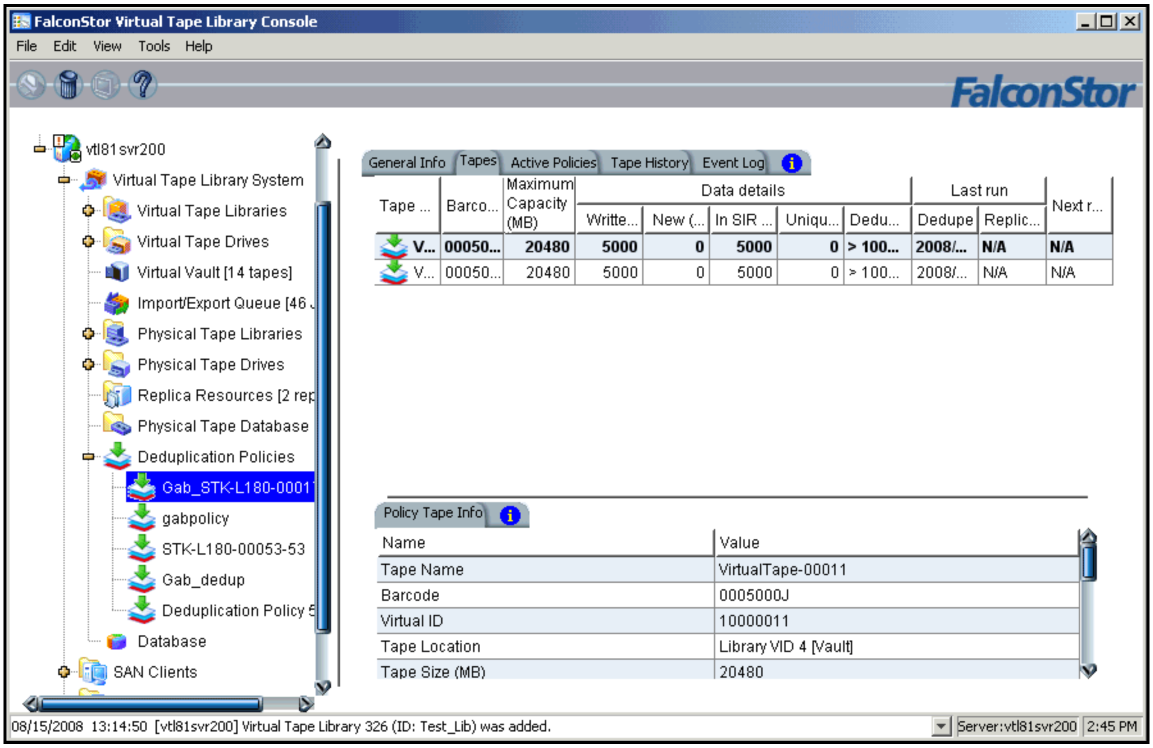
Dedupe ratio - The ratio between the data moved to deduplication and the unique data.

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...
			Writte...	New (...	In SIR ...	Uniqu...	Dedu...	Dedupe	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

08/15/2008 13:14:50 [vtl81svr200] Virtual Tape Library 326 (ID: Test_Lib) was added.

Server:vtl81svr200 2:45 PM

Virtual ID - The tape's virtual ID.

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

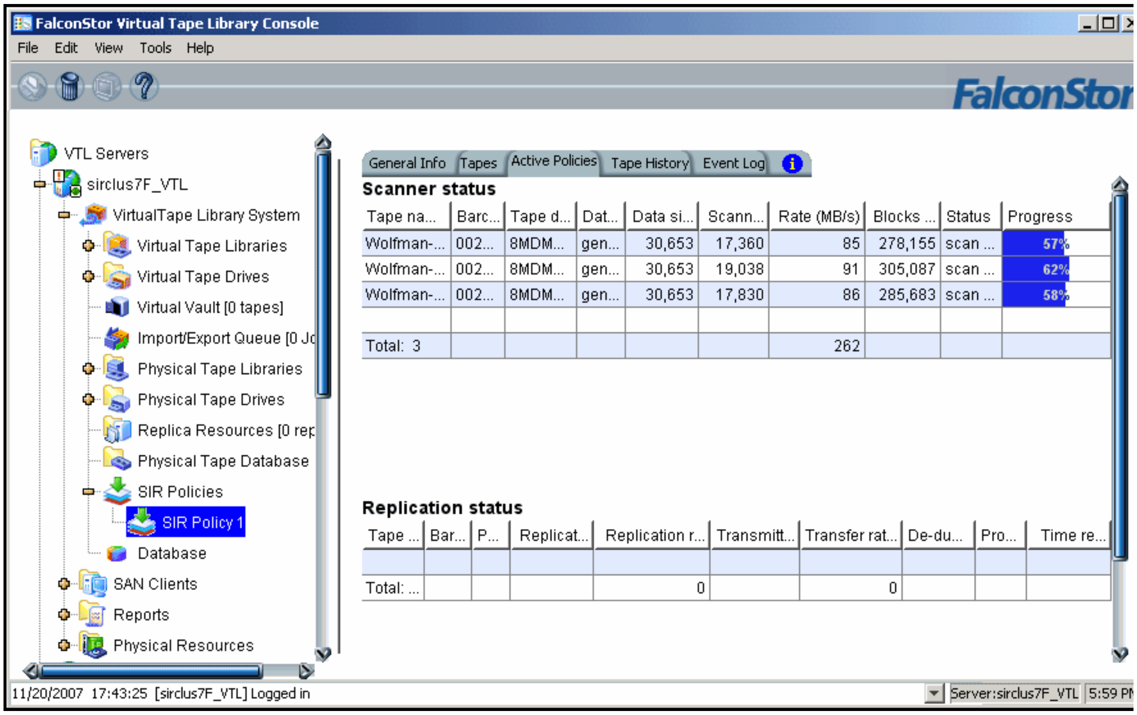
Physical allocation - The physical size of the tape.

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.



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	85	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 ...	58%
Total: 3						262			

Replication status

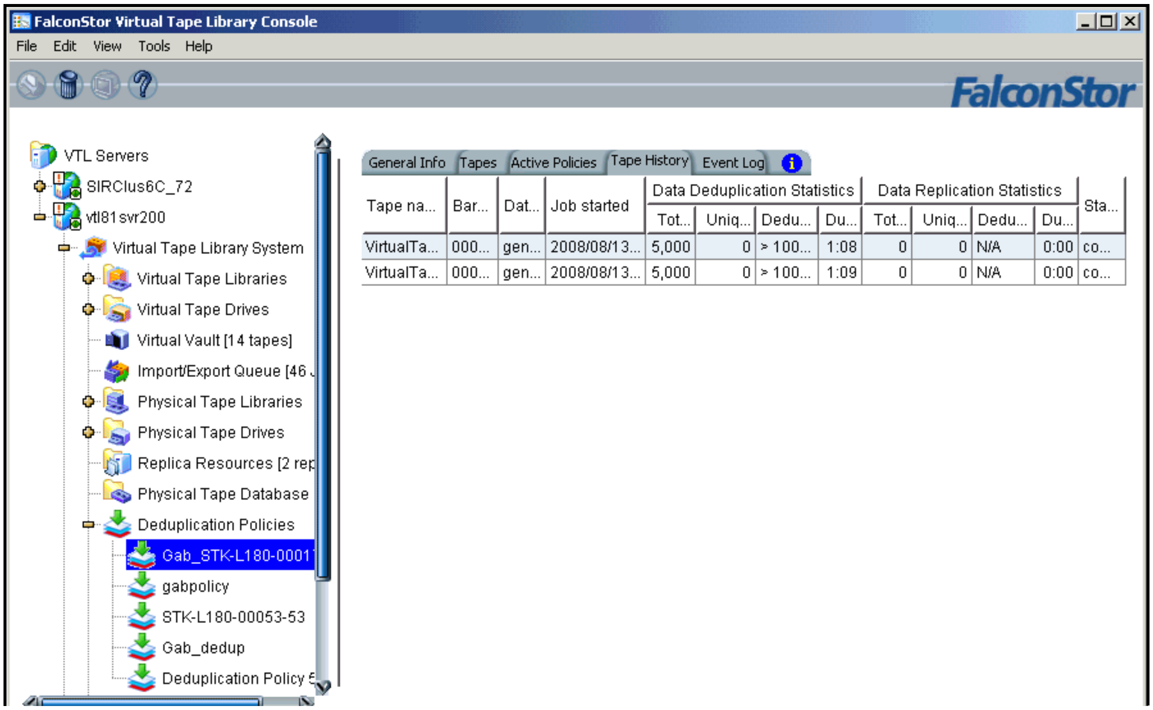
Tape ...	Bar...	P...	Replicat...	Replication r...	Transmitt...	Transfer rat...	De-du...	Pro...	Time re...
Total: ...				0		0			

11/20/2007 17:43:25 [sirclus7F_VTL] Logged in

Server:sirclus7F_VTL 5:59 PM

Tape History tab

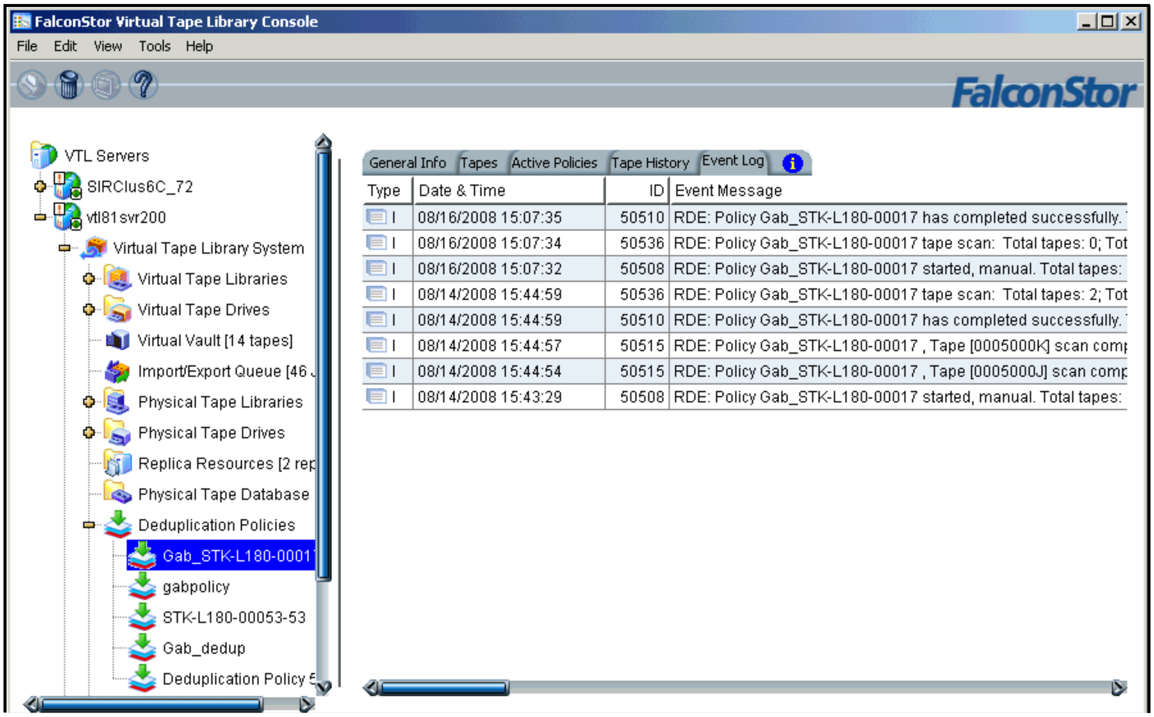
The *Tape History* tab lists all of the deduplication and replication jobs that have run and provides statistics for each.



Tape na...	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

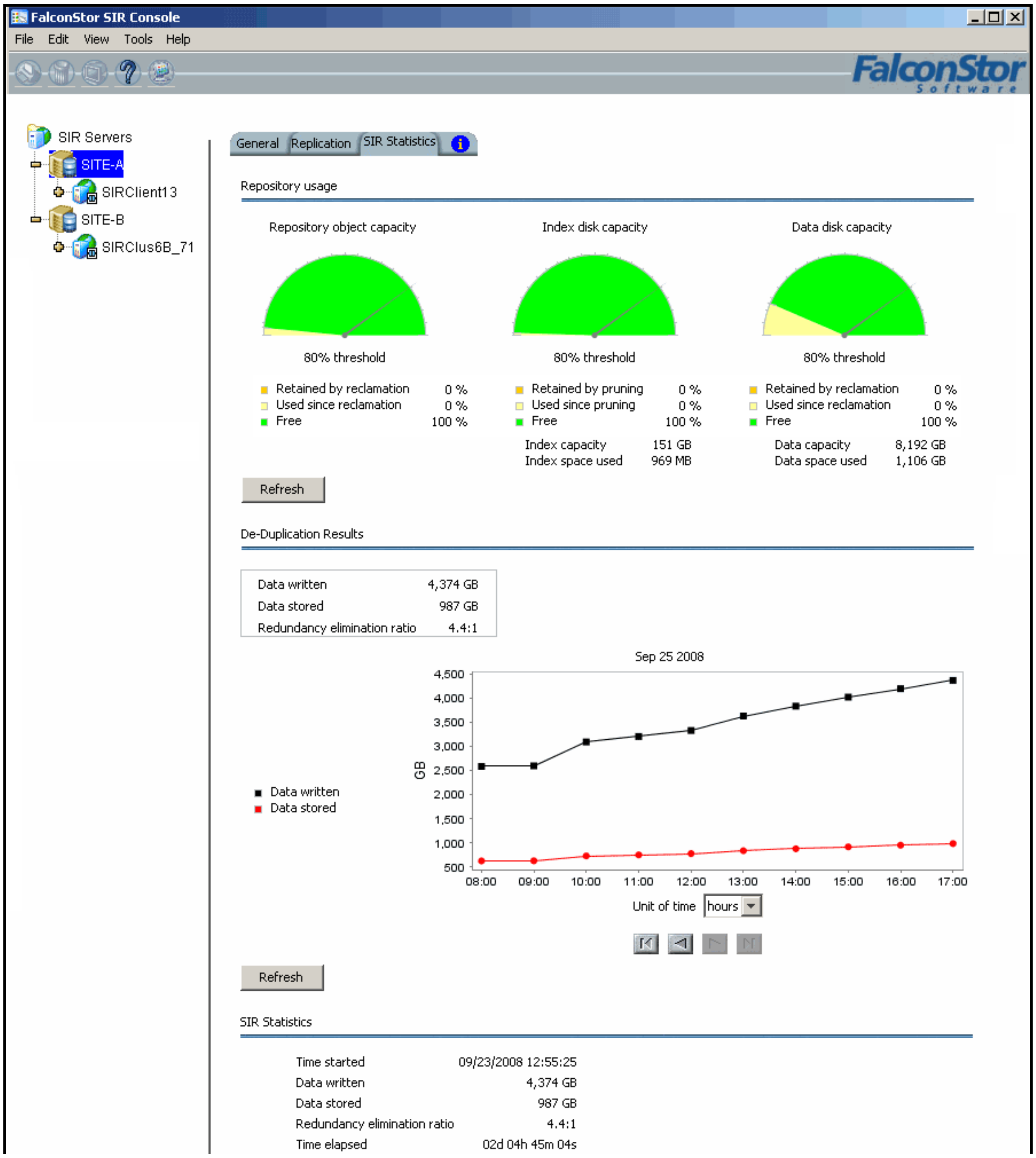
The *Event Log* tab displays informational events and errors pertaining to this policy.



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.



Repository usage

Repository object capacity		Index disk capacity		Data disk capacity	
80% threshold		80% threshold		80% threshold	
🟨 Retained by reclamation	0 %	🟨 Retained by pruning	0 %	🟨 Retained by reclamation	0 %
□ Used since reclamation	0 %	□ Used since pruning	0 %	□ Used since reclamation	0 %
🟩 Free	100 %	🟩 Free	100 %	🟩 Free	100 %
		Index capacity	151 GB	Data capacity	8,192 GB
		Index space used	969 MB	Data space used	1,106 GB

De-Duplication Results

Data written	4,374 GB
Data stored	987 GB
Redundancy elimination ratio	4.4:1

SIR Statistics

Time started	09/23/2008 12:55:25
Data written	4,374 GB
Data stored	987 GB
Redundancy elimination ratio	4.4:1
Time elapsed	02d 04h 45m 04s

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: [(data scanned)÷(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.

Note: 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 data repository 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 VTL console.

When a VIT is eliminated, the pointers to deduplication storage are deleted but the actual deduplicated data is not.

The *Space Reclamation* option allows you to delete the deduplicated data and free up the associated disk space from the data repository. To do this right-click on the VTL server object and then select *Options/Deduplication/Run Space Reclamation.*

Note: 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.

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.

Note: 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 *on demand.*
Replication of virtual tapes	Automatic	Replicates *changed* 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 *changed* 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.

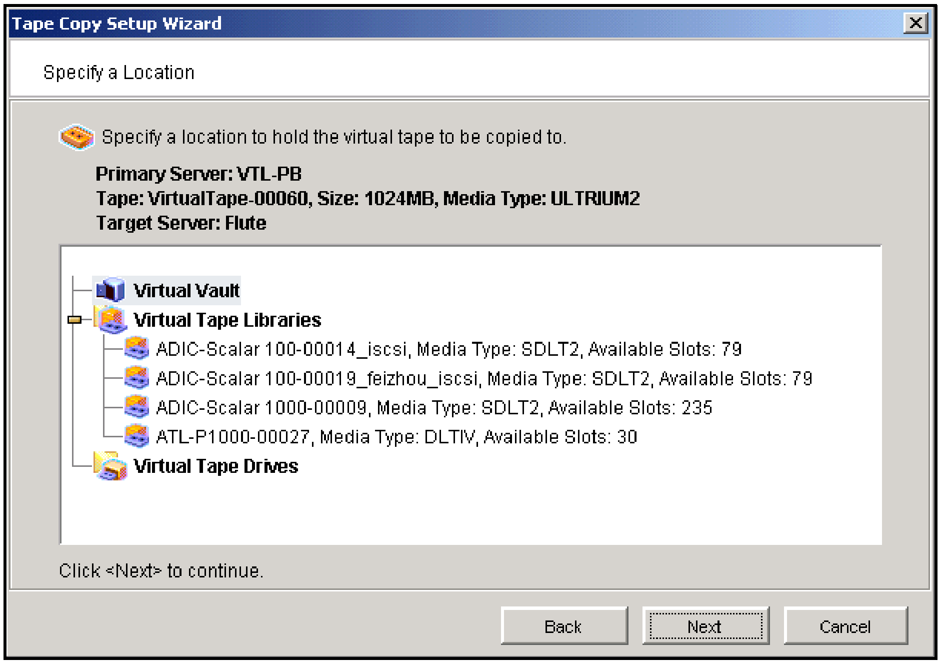
Remote Copy

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.

> **Note:** 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.



Tape Copy Setup Wizard

Specify a Location

Specify a location to hold the virtual tape to be copied to.

Primary Server: VTL-PB
Tape: VirtualTape-00060, Size: 1024MB, Media Type: ULTRIUM2
Target Server: Flute

- Virtual Vault
- Virtual Tape Libraries
  - ADIC-Scalar 100-00014_iscsi, Media Type: SDLT2, Available Slots: 79
  - ADIC-Scalar 100-00019_feizhou_iscsi, Media Type: SDLT2, Available Slots: 79
  - ADIC-Scalar 1000-00009, Media Type: SDLT2, Available Slots: 235
  - ATL-P1000-00027, Media Type: DLTIV, Available Slots: 30
- Virtual Tape Drives

Click <Next> to continue.

   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.

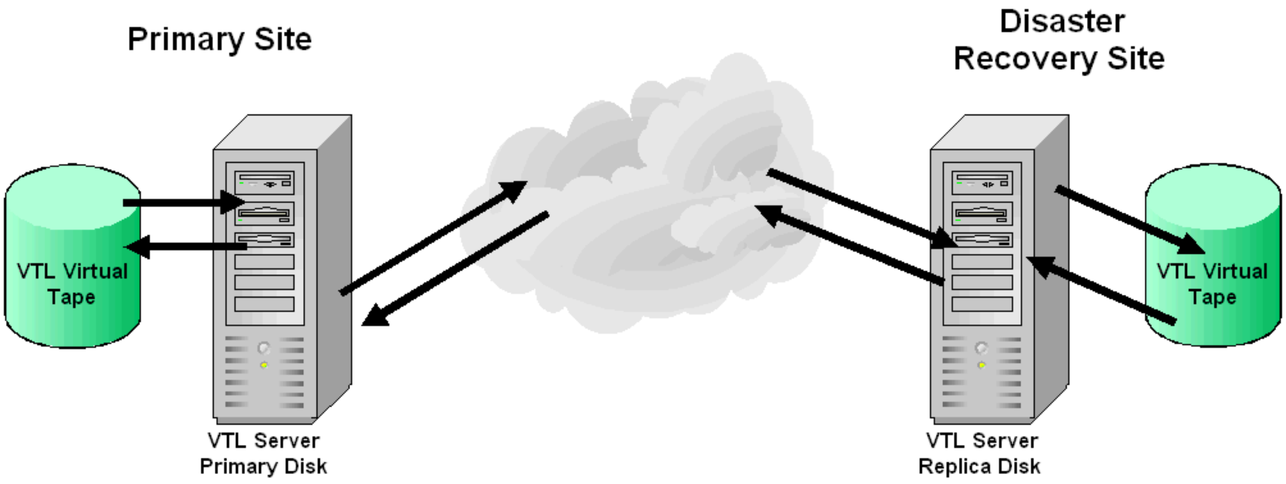
If a disaster occurs and the replica is needed, the administrator can *promote* the replica to become the primary virtual tape so that clients can access it.

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.

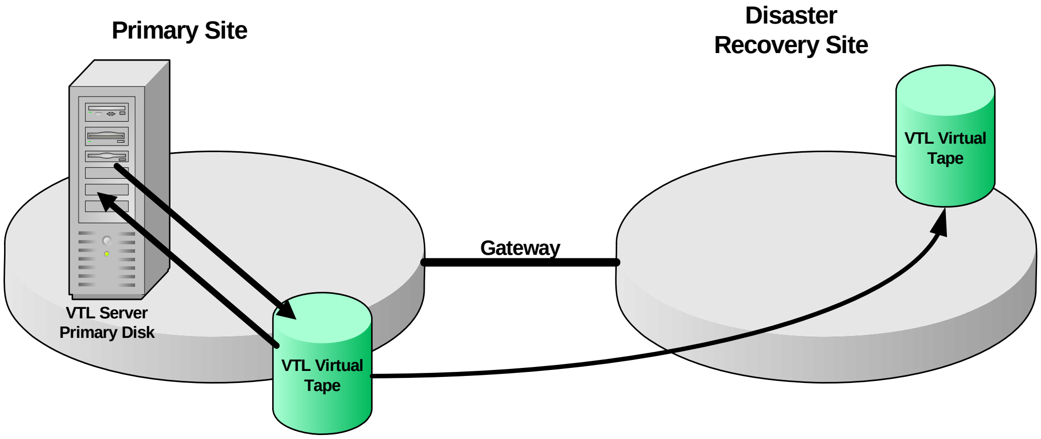


Local Replication

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.


Primary Site
Disaster Recovery Site
VTL Server Primary Disk
VTL Virtual Tape
Gateway
VTL Virtual Tape

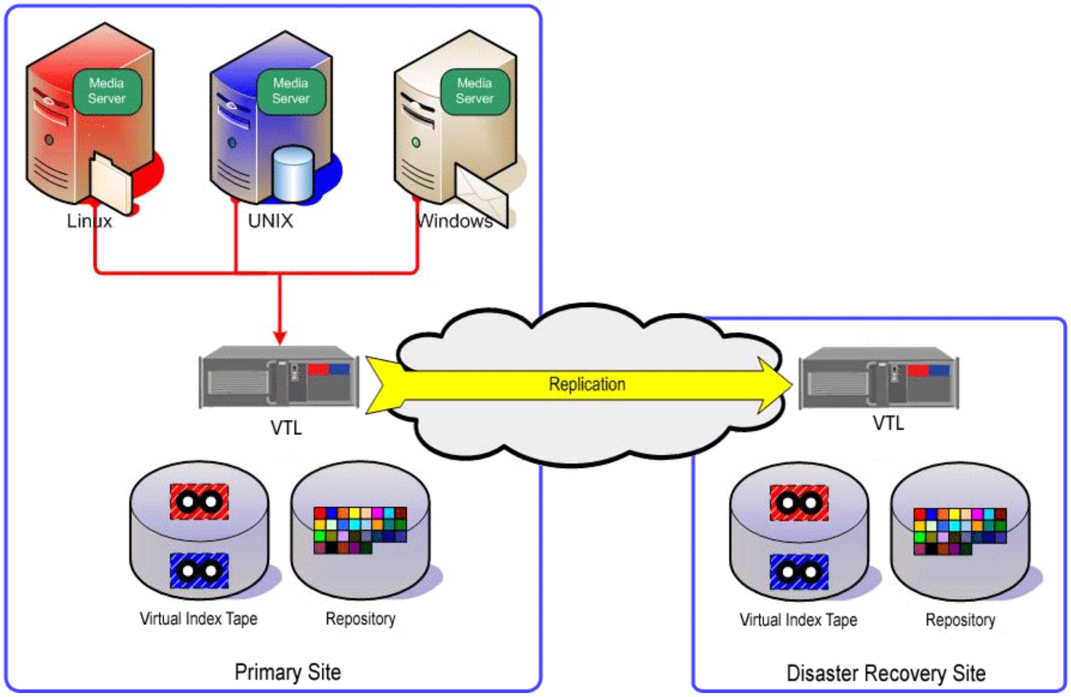
Replication of deduplicated tapes

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.

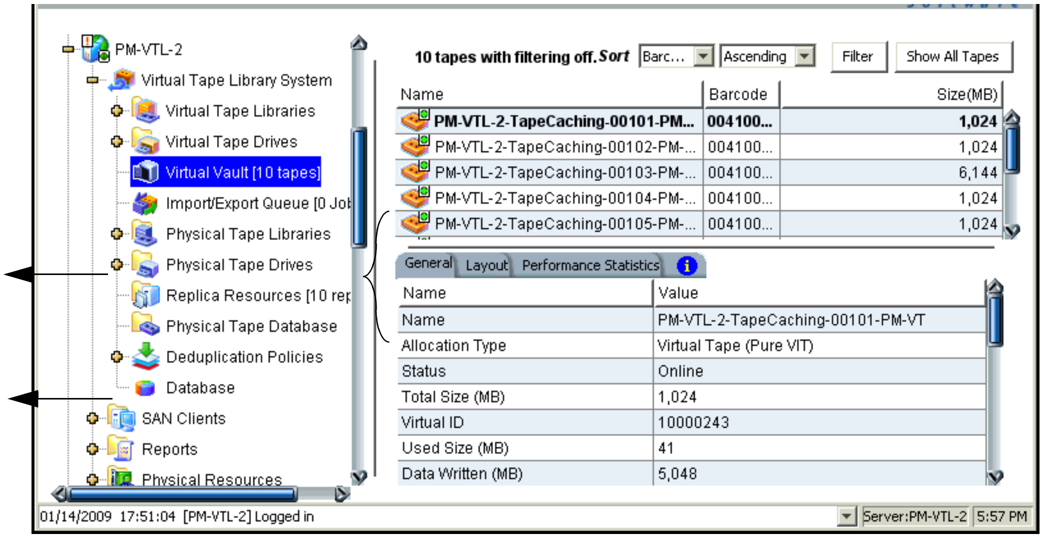


Replication of deduplicated data occurs in two phases, which you can see identified in replication status displays in the VTL console:

- 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.



Local virtual index tapes in the *Virtual Vault* after replication

Foreign virtual index tapes (VIT replicas) in *Replica Resources*

10 tapes with filtering off. ***Sort***

Name	Barcode	Size(MB)
PM-VTL-2-TapeCaching-00101-PM...	**004100...**	**1,024**
PM-VTL-2-TapeCaching-00102-PM-...	004100...	1,024
PM-VTL-2-TapeCaching-00103-PM-...	004100...	6,144
PM-VTL-2-TapeCaching-00104-PM-...	004100...	1,024
PM-VTL-2-TapeCaching-00105-PM-...	004100...	1,024

Name	Value
Name	PM-VTL-2-TapeCaching-00101-PM-VT
Allocation Type	Virtual Tape (Pure VIT)
Status	Online
Total Size (MB)	1,024
Virtual ID	10000243
Used Size (MB)	41
Data Written (MB)	5,048

01/14/2009 17:51:04 [PM-VTL-2] Logged in | Server:PM-VTL-2 | 5:57 PM

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.

Note: 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*.

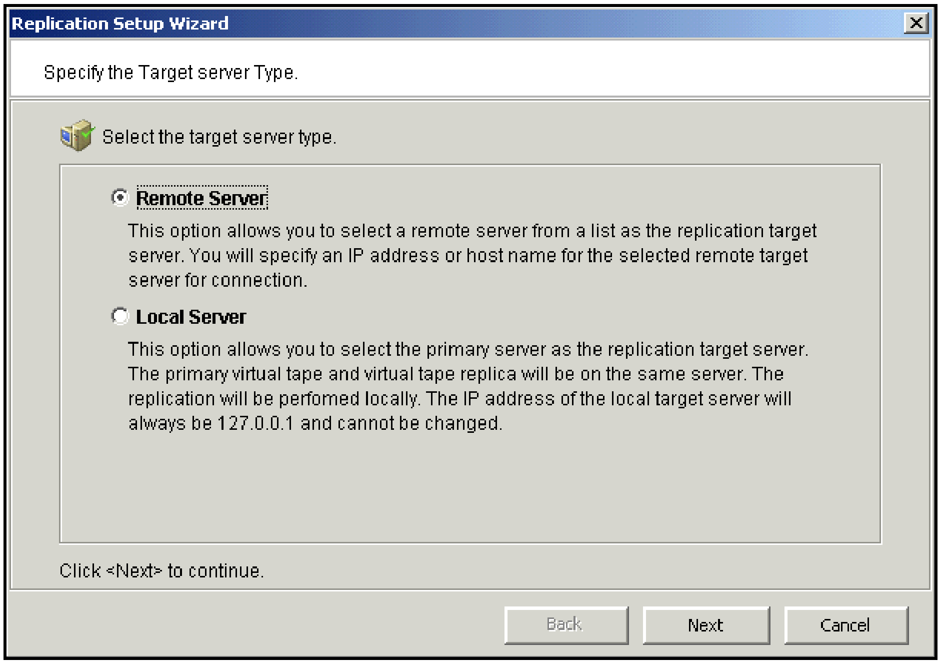
   To enable replication for multiple virtual tapes in the same virtual tape library, right-click the virtual tape library and select *Replication* --> *Add.*

   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.

   Note: 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.



Specify the Target server Type.

Select the target server type.

● Remote Server

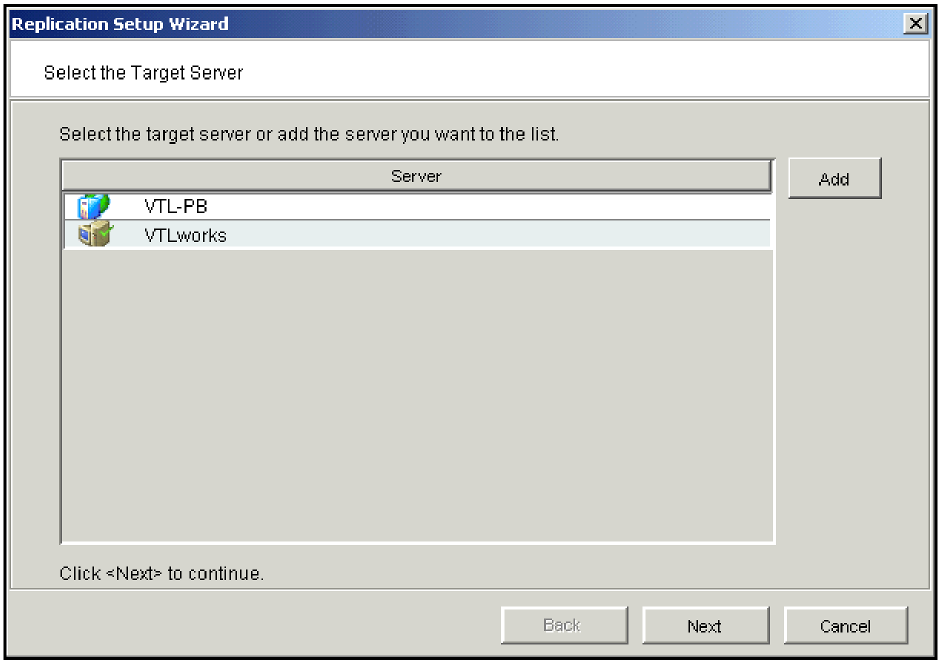
This option allows you to select a remote server from a list as the replication target server. You will specify an IP address or host name for the selected remote target server for connection.

○ Local Server

This option allows you to select the primary server as the replication target server. The primary virtual tape and virtual tape replica will be on the same server. The replication will be perfomed locally. The IP address of the local target server will always be 127.0.0.1 and cannot be changed.

Click <Next> to continue.

3. Select the server that will contain the replica.



Replication Setup Wizard

Select the Target Server

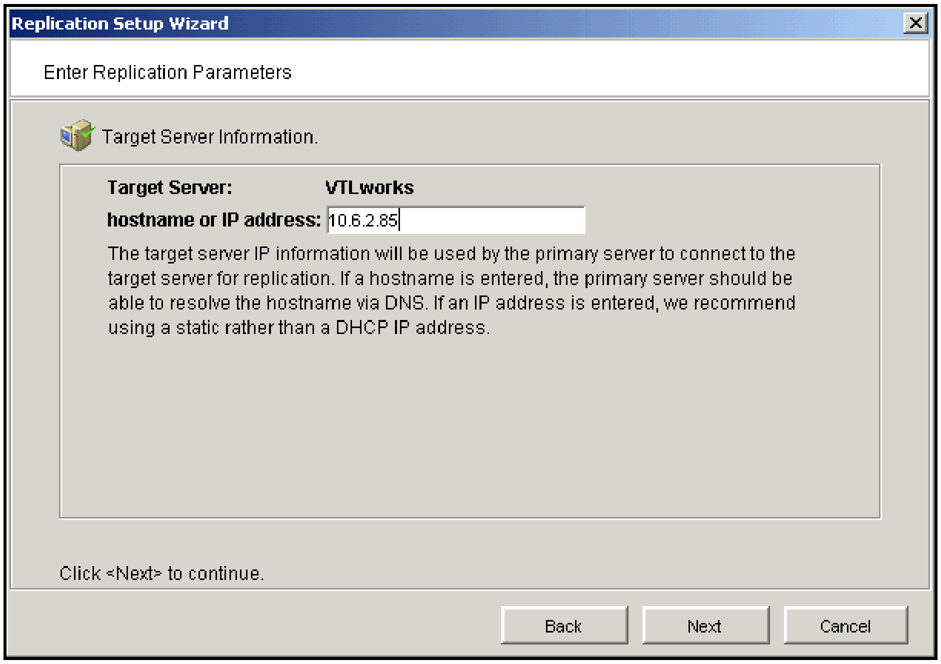
Select the target server or add the server you want to the list.

Server
VTL-PB
VTLworks

Click <Next> to continue.

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

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



Replication Setup Wizard

Enter Replication Parameters

Target Server Information.

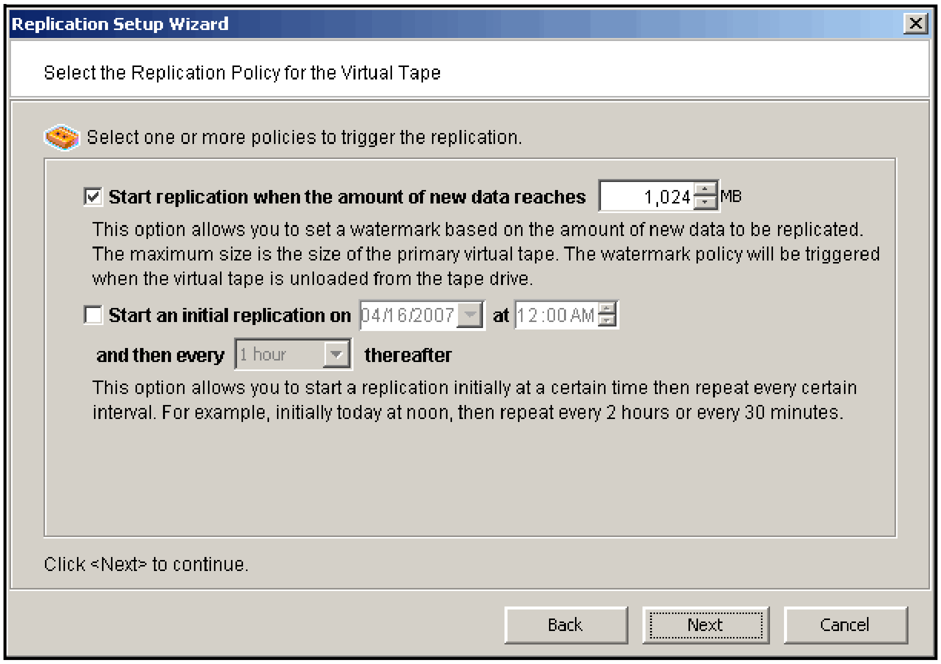
Target Server: **VTLworks**

hostname or IP address: 10.6.2.85

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

Click <Next> to continue.

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



Select the Replication Policy for the Virtual Tape

Select one or more policies to trigger the replication.

☑ **Start replication when the amount of new data reaches** 1,024 MB

This option allows you to set a watermark based on the amount of new data to be replicated. The maximum size is the size of the primary virtual tape. The watermark policy will be triggered when the virtual tape is unloaded from the tape drive.

☐ **Start an initial replication on** 04/16/2007 **at** 12:00 AM

and then every 1 hour **thereafter**

This option allows you to start a replication initially at a certain time then repeat every certain interval. For example, initially today at noon, then repeat every 2 hours or every 30 minutes.

Click <Next> to continue.

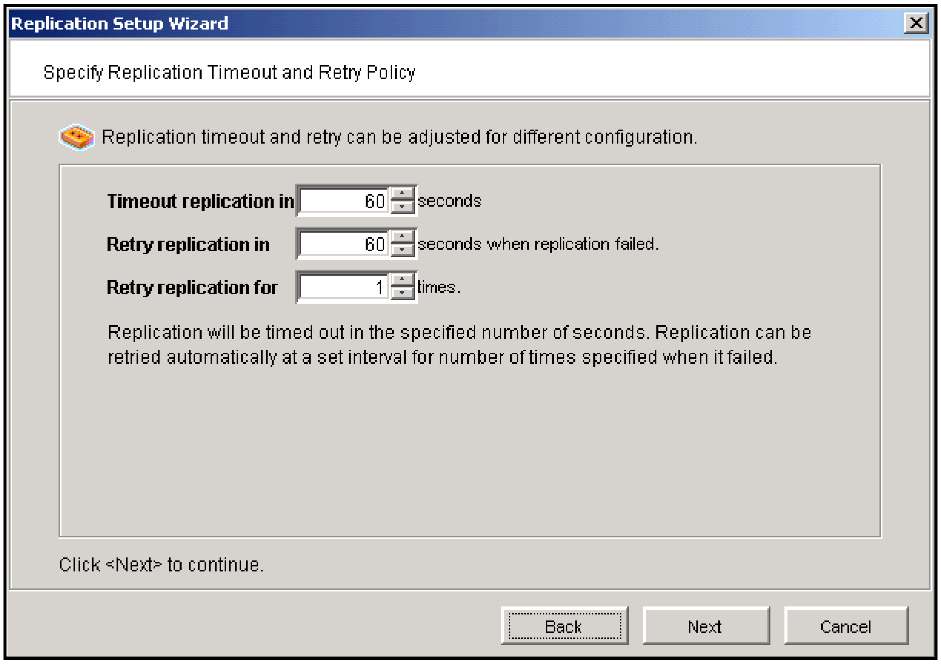
You must select at least one policy, but you can have multiple.

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.



Specify Replication Timeout and Retry Policy

Replication timeout and retry can be adjusted for different configuration.

Timeout replication in 60 seconds

Retry replication in 60 seconds when replication failed.

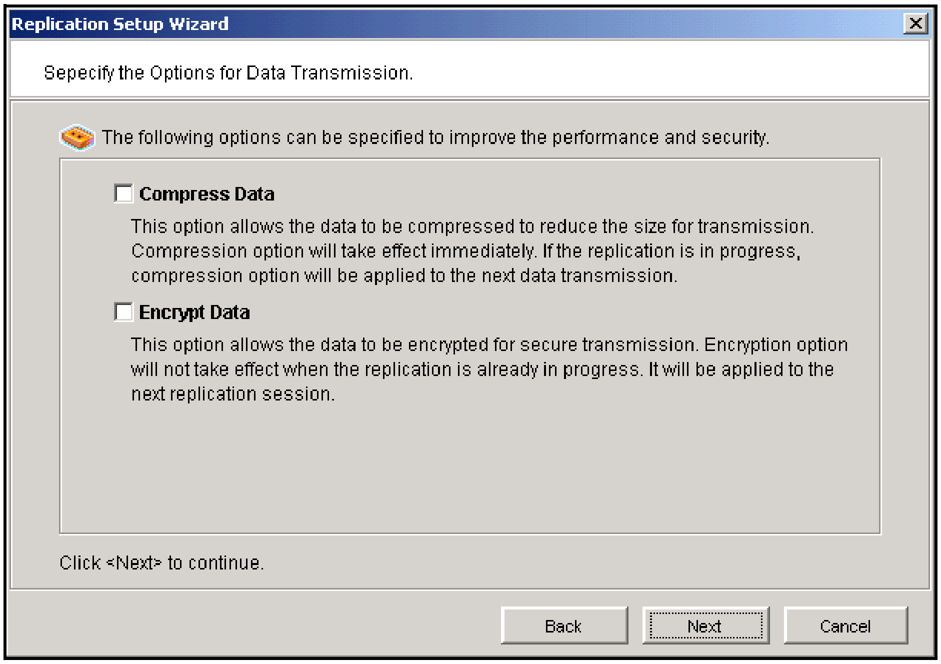
Retry replication for 1 times.

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

Click <Next> to continue.

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*.



Sepecify the Options for Data Transmission.

The following options can be specified to improve the performance and security.

☐ Compress Data

This option allows the data to be compressed to reduce the size for transmission. Compression option will take effect immediately. If the replication is in progress, compression option will be applied to the next data transmission.

☐ Encrypt Data

This option allows the data to be encrypted for secure transmission. Encryption option will not take effect when the replication is already in progress. It will be applied to the next replication session.

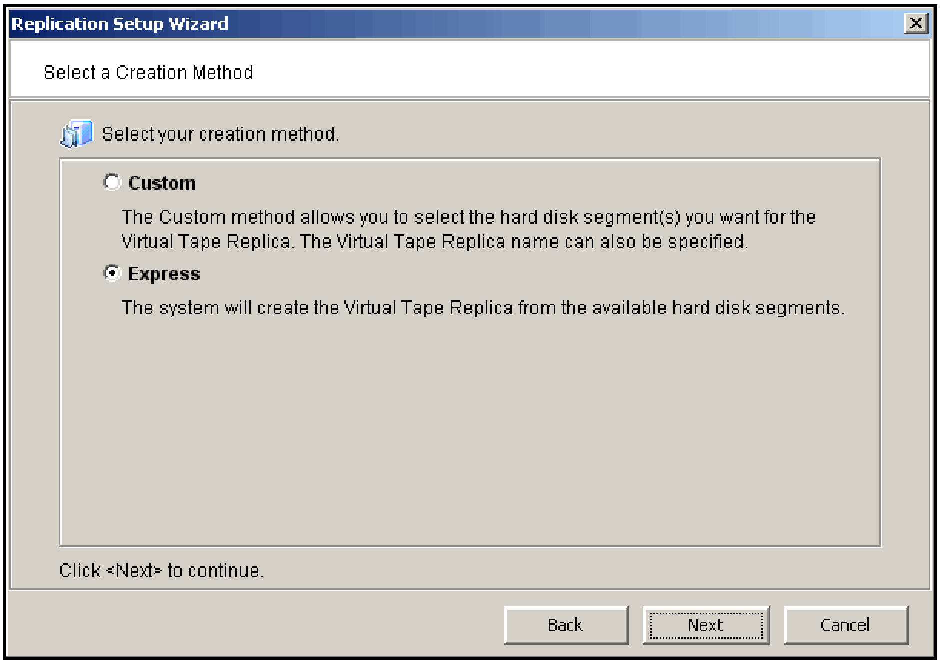
Click <Next> to continue.

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.



Replication Setup Wizard

Select a Creation Method

Select your creation method.

○ **Custom**

The Custom method allows you to select the hard disk segment(s) you want for the Virtual Tape Replica. The Virtual Tape Replica name can also be specified.

● **Express**

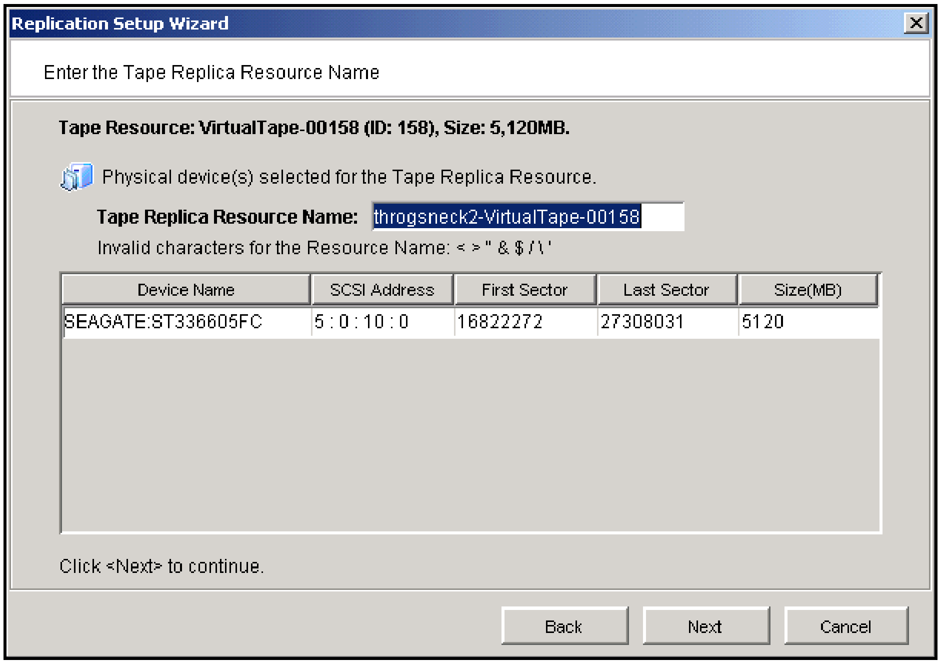
The system will create the Virtual Tape Replica from the available hard disk segments.

Click <Next> to continue.

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

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

9. Enter a name for the replica resource.



Replication Setup Wizard

Enter the Tape Replica Resource Name

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

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

Tape Replica Resource Name: throgsneck2-VirtualTape-00158

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

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

Click <Next> to continue.

The name is not case sensitive and is limited to a maximum of 32 characters.

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

Configure replication for deduplicated tapes

Notes:

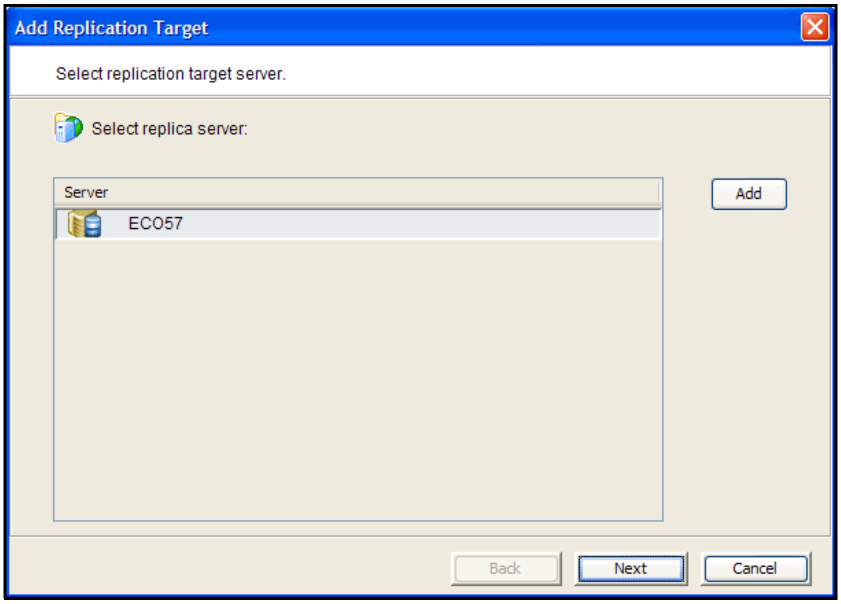
- If you need to change the IP address or hostname of your VTL appliance, you must do so before configuring replication for tapes in a deduplication policy.
- By default, replication uses eth0. If you want to replicate using eth1, you will need to configure your systems accordingly. Refer to 'Replicating 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.


Add Replication Target

Select replication target server.

Select replica server:

Server
ECO57

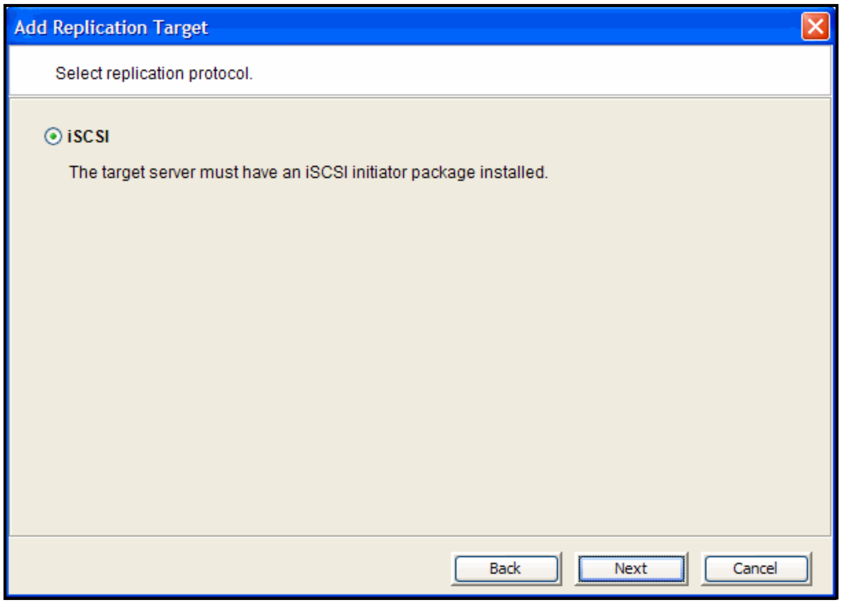
4. Enter login information for the target server.

   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.



Add Replication Target

Select replication protocol.

● iSCSI

The target server must have an iSCSI initiator package installed.

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).

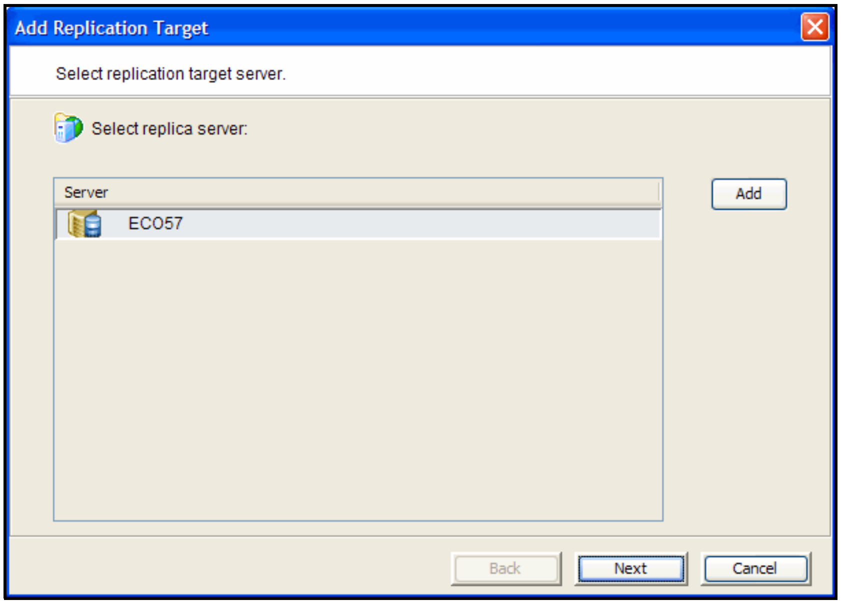
You can now configure replication for tapes included in a deduplication policy (refer to 'Add deduplication policies' for details).

Replicating deduplicated tapes from a server using an alternate NIC

1. Enable iSCSI protocol on the source serverby 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.



Add Replication Target

Select replication target server.

Select replica server:

Server
ECO57

4. Enter login information for the target server.

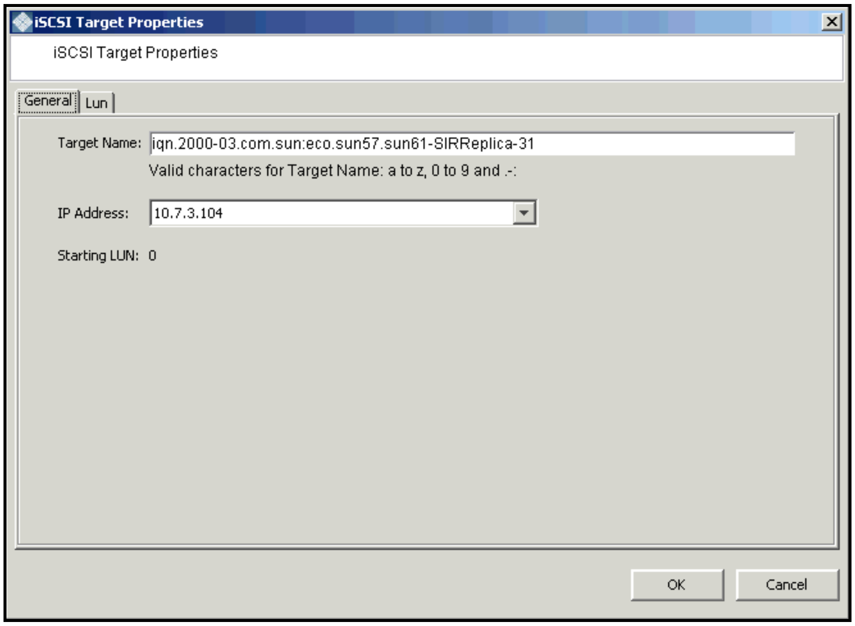
   If your target is another VTL standalone system, enter login information for the target VTL server.

   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.



iSCSI Target Properties

Target Name: iqn.2000-03.com.sun:eco.sun57.sun61-SIRReplica-31

Valid characters for Target Name: a to z, 0 to 9 and .-:

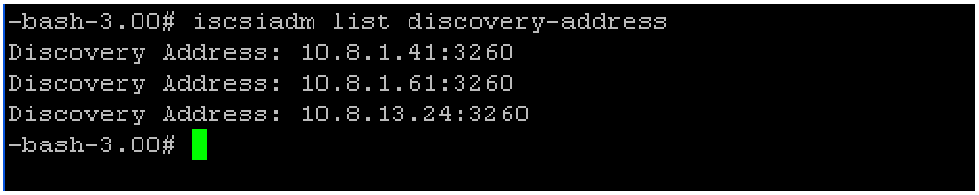
IP Address: 10.7.3.104

Starting LUN: 0

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:

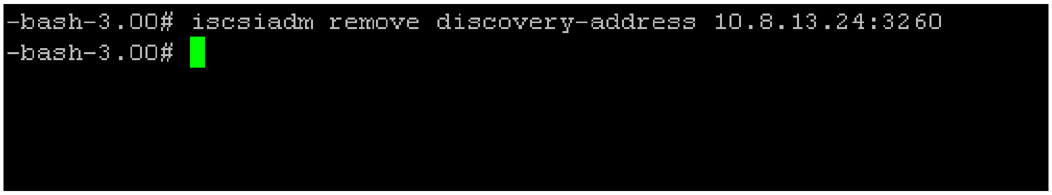
```
iscsiadm list discovery-address
```



```
-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:

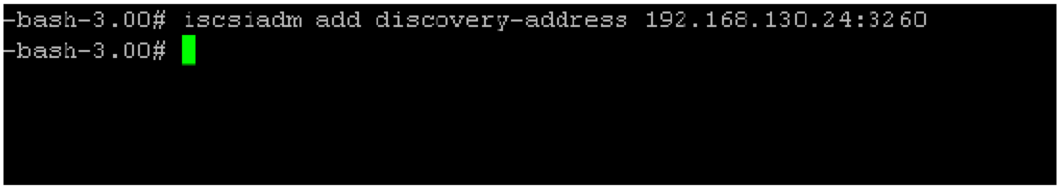
```
iscsiadm remove discovery-address <IP address>
```



```
-bash-3.00# iscsiadm remove discovery-address 10.8.13.24:3260
-bash-3.00#
```

- Add the alternate IP address as the discovery address:

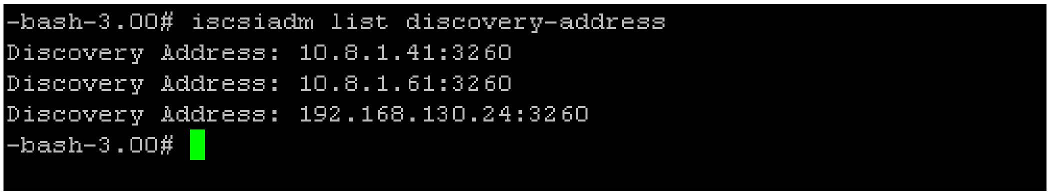
```
iscsiadm add discovery-address <IP address>
```



```
-bash-3.00# iscsiadm add discovery-address 192.168.130.24:3260
-bash-3.00# 
```

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

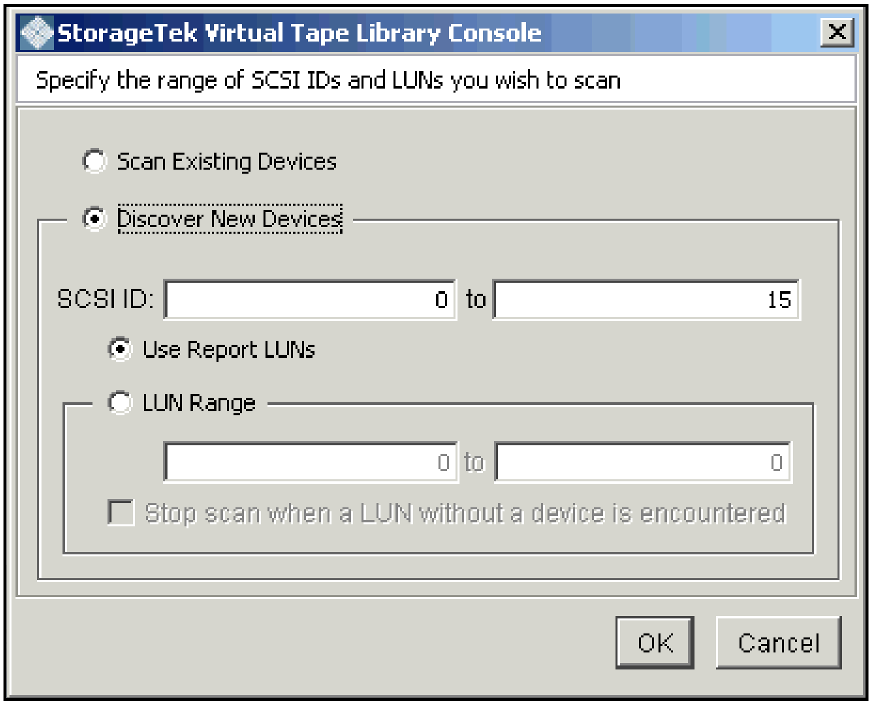
```
iscsiadm list discovery-address
```



```
-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.



StorageTek Virtual Tape Library Console

Specify the range of SCSI IDs and LUNs you wish to scan

○ Scan Existing Devices

● Discover New Devices

SCSI ID: 0 to 15

● Use Report LUNs

○ LUN Range

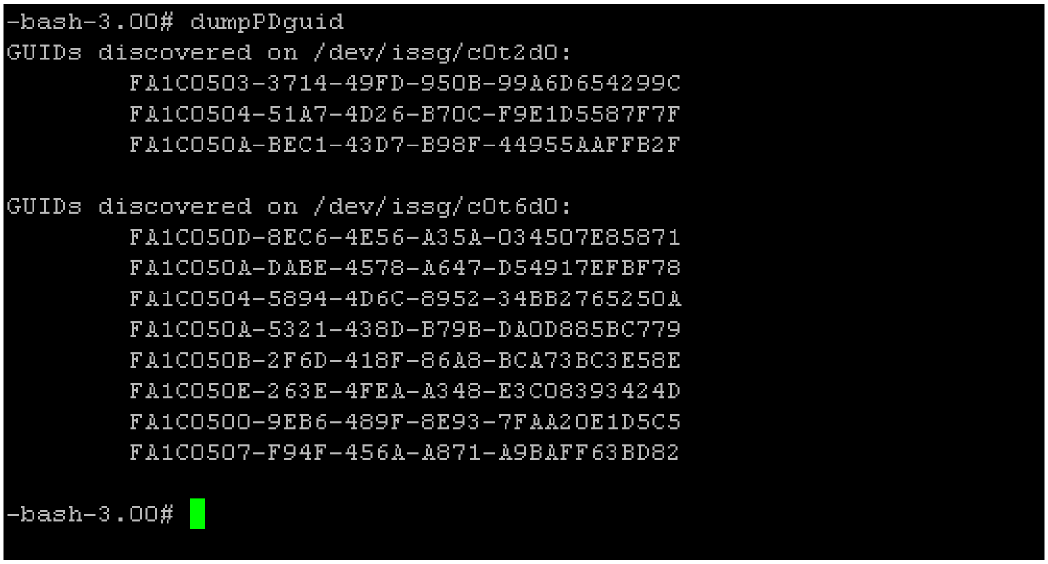
0 to 0

□ Stop scan when a LUN without a device is encountered

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:

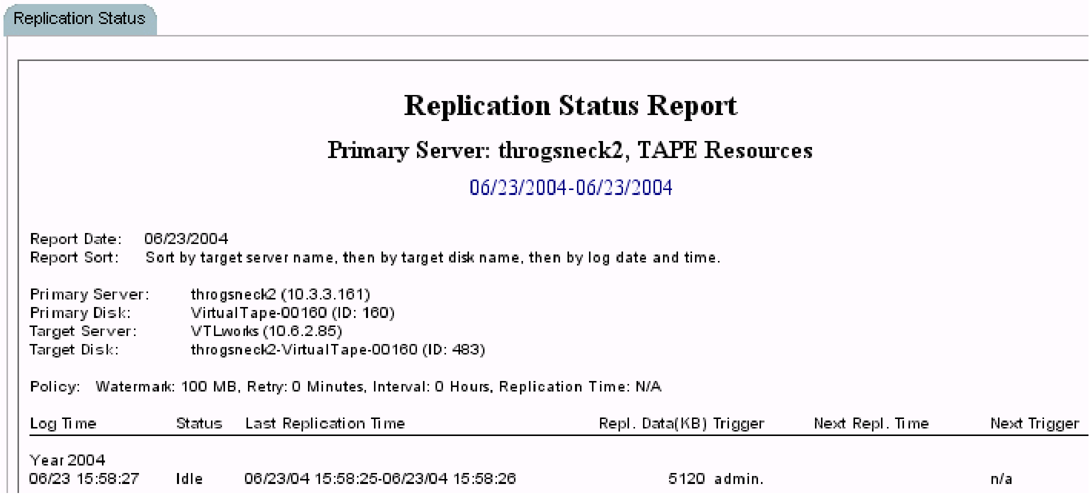


```
-bash-3.00# dumpPDguid
GUIDs discovered on /dev/issg/c0t2d0:
        FA1C0503-3714-49FD-950B-99A6D654299C
        FA1C0504-51A7-4D26-B70C-F9E1D5587F7F
        FA1C050A-BEC1-43D7-B98F-44955AAFFB2F

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 Report

Primary Server: throgsneck2, TAPE Resources

06/23/2004-06/23/2004

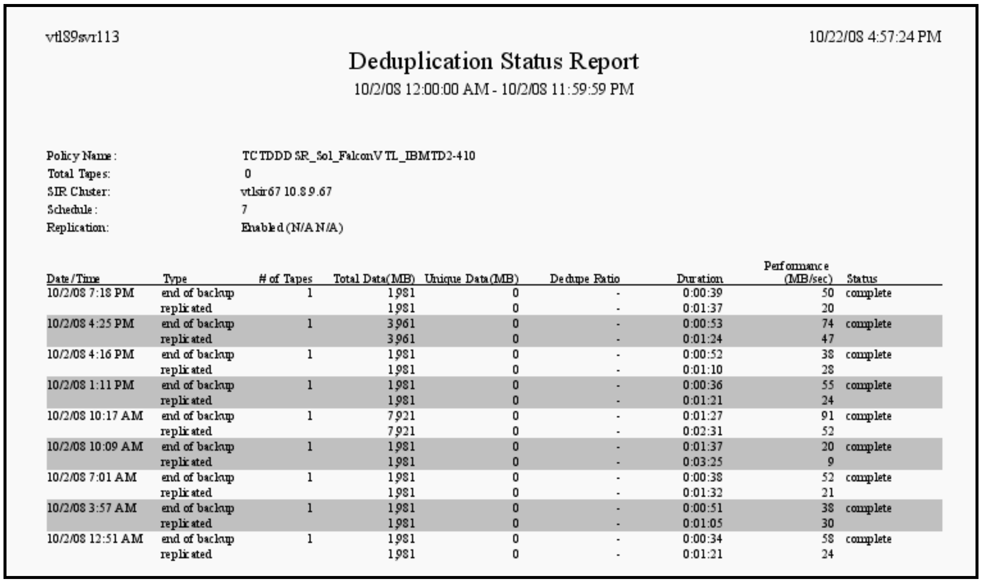
Report Date: 06/23/2004
Report Sort: Sort by target server name, then by target disk name, then by log date and time.

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

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

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

- 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*:



vtl89svr113 10/22/08 4:57:24 PM

Deduplication Status Report

10/2/08 12:00:00 AM - 10/2/08 11:59:59 PM

Policy Name :	TCTDDDSR_Sol_FalconVTL_IBMTD2-410
Total Tapes:	0
SIR Cluster:	vtlsir67 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	1,981	0	-	0:00:39	50	complete
	replicated		1,981	0	-	0:01:37	20	
10/2/08 4:25 PM	end of backup	1	3,961	0	-	0:00:53	74	complete
	replicated		3,961	0	-	0:01:24	47	
10/2/08 4:16 PM	end of backup	1	1,981	0	-	0:00:52	38	complete
	replicated		1,981	0	-	0:01:10	28	
10/2/08 1:11 PM	end of backup	1	1,981	0	-	0:00:36	55	complete
	replicated		1,981	0	-	0:01:21	24	
10/2/08 10:17 AM	end of backup	1	7,921	0	-	0:01:27	91	complete
	replicated		7,921	0	-	0:02:31	52	
10/2/08 10:09 AM	end of backup	1	1,981	0	-	0:01:37	20	complete
	replicated		1,981	0	-	0:03:25	9	
10/2/08 7:01 AM	end of backup	1	1,981	0	-	0:00:38	52	complete
	replicated		1,981	0	-	0:01:32	21	
10/2/08 3:57 AM	end of backup	1	1,981	0	-	0:00:51	38	complete
	replicated		1,981	0	-	0:01:05	30	
10/2/08 12:51 AM	end of backup	1	1,981	0	-	0:00:34	58	complete
	replicated		1,981	0	-	0:01:21	24	

Promote a replica resource

Note: 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

> **Note:** 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

Note: This is valid only for virtual tapes, not for Virtual Index Tapes (VITs).

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

Note: 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.

Note: 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.

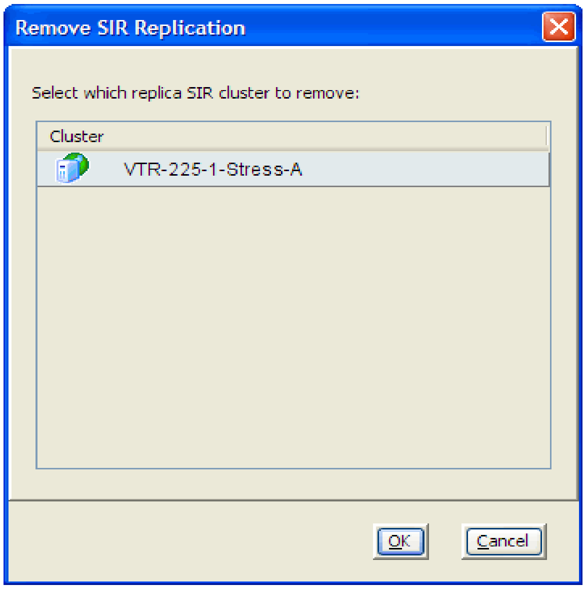
> **Note:** If you need to change the IP address or a hostname of a VTL appliance that has replication configured for deduplicated tapes, you must complete this procedure before changing either the IP address or hostname, and then reconfigure replication afterward.

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.

   > **Note:** 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.



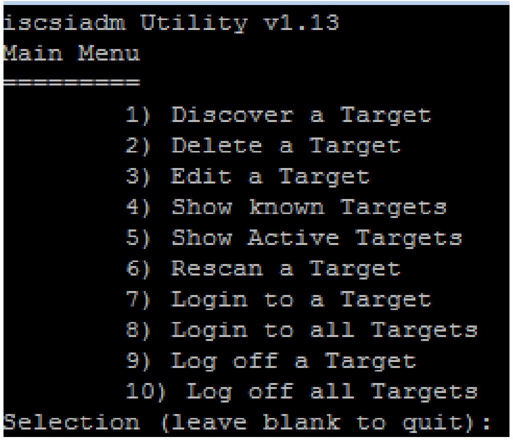
Remove SIR Replication

Select which replica SIR cluster to remove:

Cluster
VTR-225-1-Stress-A

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.

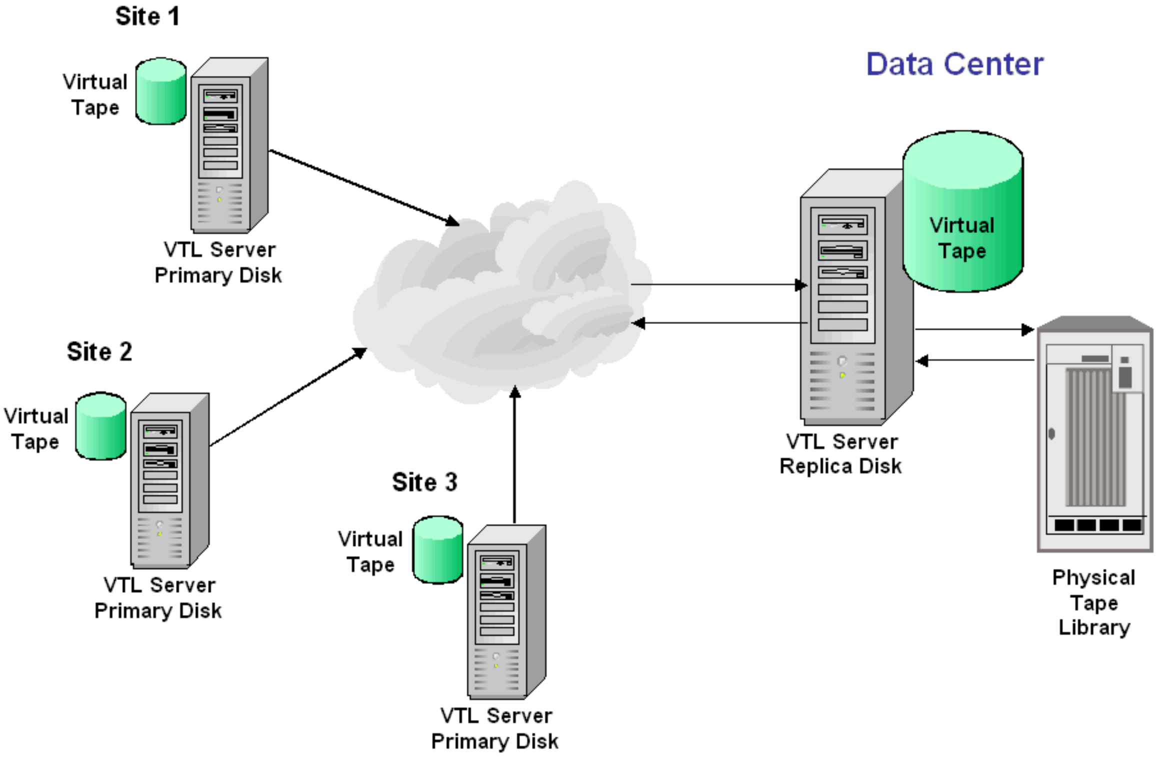
4. Locate the file `$ISHOME/etc/hostname/ecocluster.conf`.

   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.

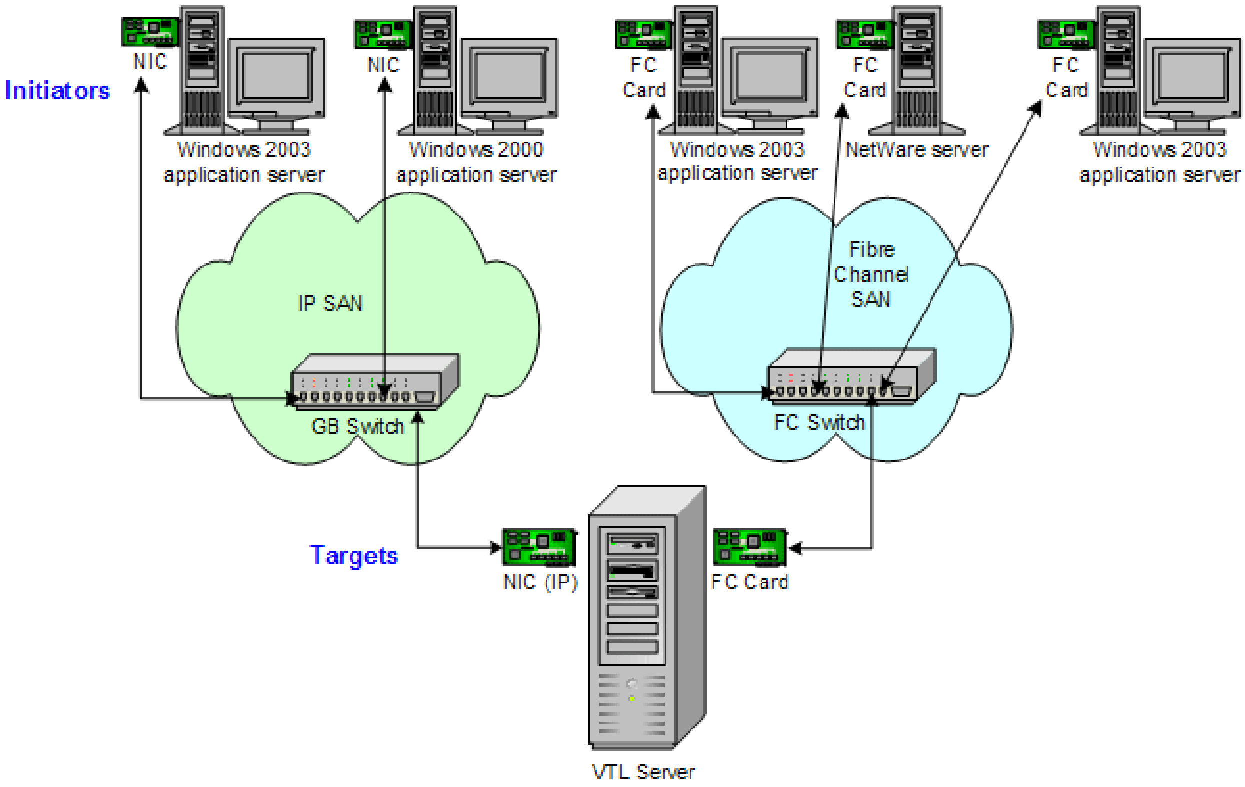
In this environment, if you will be exporting tapes from the remote VTL server to the physical tape library, you want to make sure that when you create tapes on the primary servers (at the multiple VTL locations *without* physical tape libraries), you match the barcodes of the tapes on the physical library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


Initiators
NIC
Windows 2003 application server
NIC
Windows 2000 application server
FC Card
Windows 2003 application server
FC Card
NetWare server
FC Card
Windows 2003 application server
IP SAN
GB Switch
Fibre Channel SAN
FC Switch
Targets
NIC (IP)
FC Card
VTL Server

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*.

     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.

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.

   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.

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

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

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

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

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

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

For example, for the case of upstream (to 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 our website to see a complete list of certified cards.

Storage array

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

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

Backup servers

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

Configure a FC switch using soft zoning

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

1. Access the FC switch via its web interface and log in if necessary.
2. Access the Name Server Table.
3. Access the zoning configuration and log in if necessary.
4. Using previously recorded FC HBA information, look for the WWPNs for the adapters from the VTL appliance, storage array, and backup servers.
5. Create aliases for each WWPN.

   Note that some switches (i.e. McData) do not use aliasing.

6. Create zones for your configuration, for example:
   - Zone 1: VTL WWPN (initiator)->storage array WWPN (target)
   - Zone 2: VTL WWPN (initiator)->Tape Library WWPN (target)
   - Zone 3: VTL WWPN (target)->backup server WWPN (initiator)
7. Save the configuration.

Configure a FC switch using hard zoning

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

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.*

> **Note:** 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:\qlogic).
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.

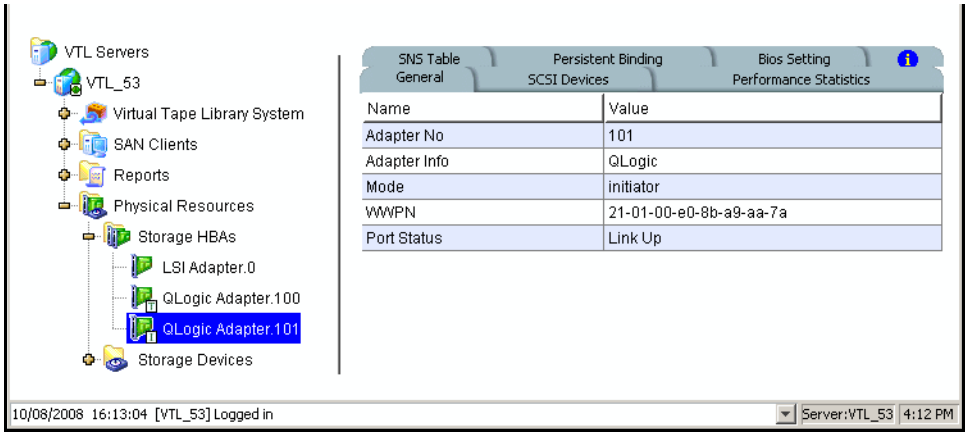
The *Port Down Retry Count* and *Link Down Retry* is configurable in the BIOS whereas the */XRetry, /XTimeout*, and */PortDown* values are configured by the driver. The *Port Down Retry Count* and the */Portdown* values combined will approximately be the total disk timeout.

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.

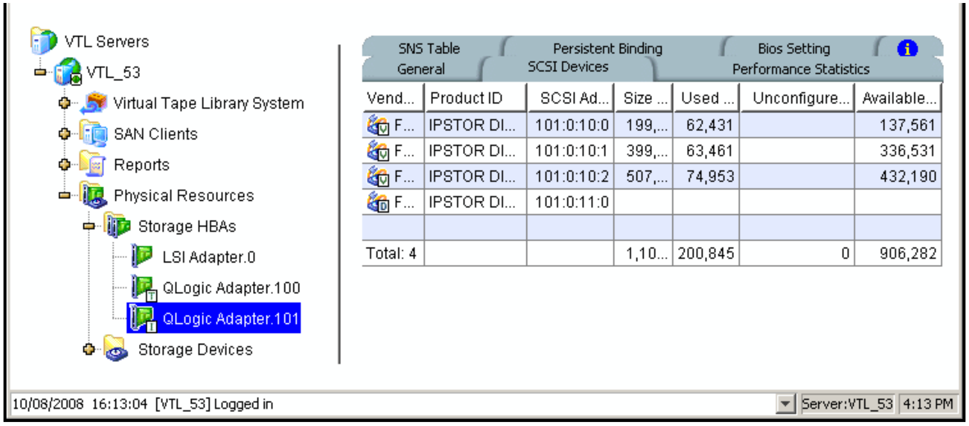


Name	Value
Adapter No	101
Adapter Info	QLogic
Mode	initiator
WWPN	21-01-00-e0-8b-a9-aa-7a
Port Status	Link Up

10/08/2008 16:13:04 [VTL_53] Logged in   Server:VTL_53   4:12 PM

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*.

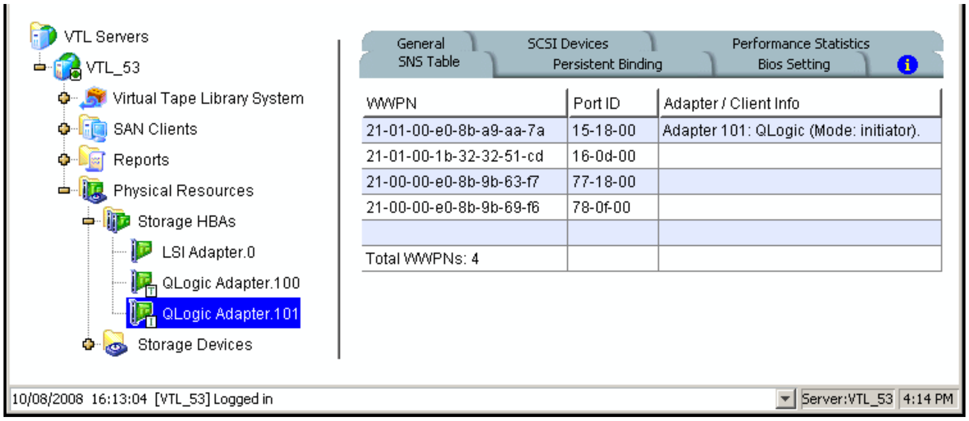


Vend...	Product ID	SCSI Ad...	Size ...	Used ...	Unconfigure...	Available...
F...	IPSTOR DI...	101:0:10:0	199,...	62,431		137,561
F...	IPSTOR DI...	101:0:10:1	399,...	63,461		336,531
F...	IPSTOR DI...	101:0:10:2	507,...	74,953		432,190
F...	IPSTOR DI...	101:0:11:0				
Total: 4			1,10...	200,845	0	906,282

10/08/2008 16:13:04 [VTL_53] Logged in   Server:VTL_53   4:13 PM

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.*



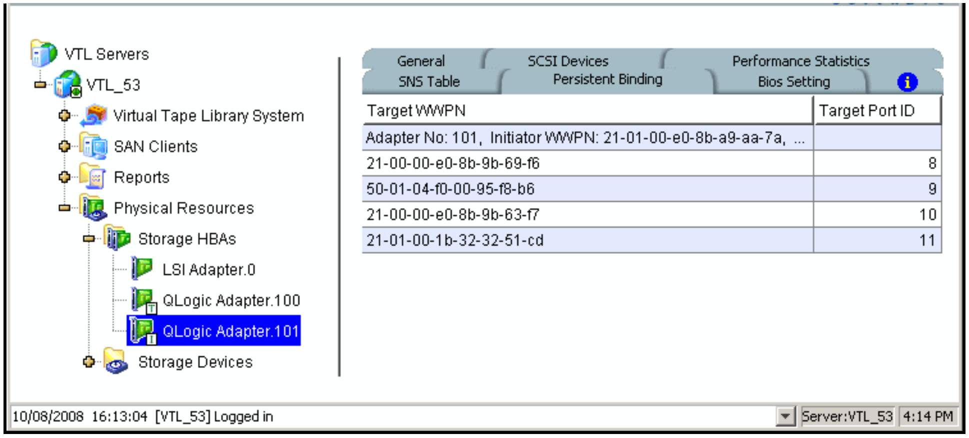
WWPN	Port ID	Adapter / Client Info
21-01-00-e0-8b-a9-aa-7a	15-18-00	Adapter 101: QLogic (Mode: initiator).
21-01-00-1b-32-32-51-cd	16-0d-00	
21-00-00-e0-8b-9b-63-f7	77-18-00	
21-00-00-e0-8b-9b-69-f6	78-0f-00	
Total WWPNs: 4		

10/08/2008 16:13:04 [VTL_53] Logged in

Server:VTL_53 4:14 PM

Persistent Binding tab

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



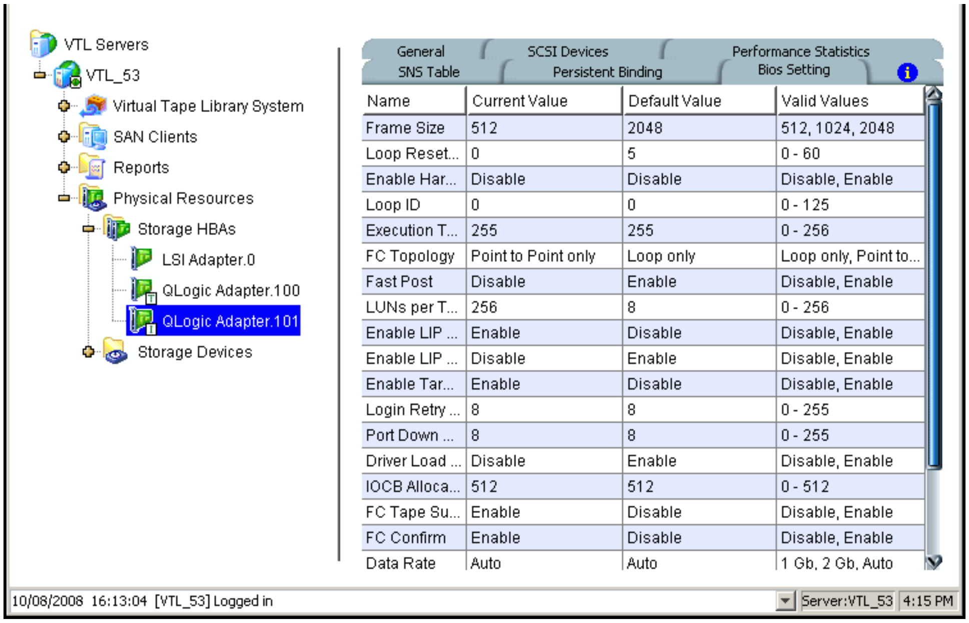
Target WWPN	Target Port ID
Adapter No: 101, Initiator WWPN: 21-01-00-e0-8b-a9-aa-7a, ...	
21-00-00-e0-8b-9b-69-f6	8
50-01-04-f0-00-95-f8-b6	9
21-00-00-e0-8b-9b-63-f7	10
21-01-00-1b-32-32-51-cd	11

10/08/2008 16:13:04 [VTL_53] Logged in

Server:VTL_53 4:14 PM

Bios Setting tab

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

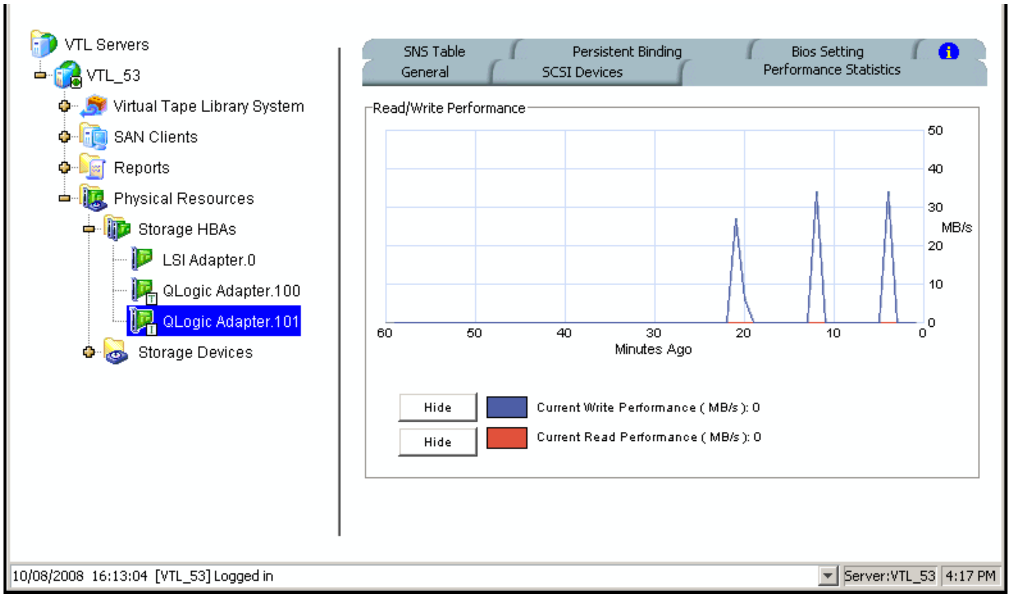


Name	Current Value	Default Value	Valid Values
Frame Size	512	2048	512, 1024, 2048
Loop Reset...	0	5	0 - 60
Enable Har...	Disable	Disable	Disable, Enable
Loop ID	0	0	0 - 125
Execution T...	255	255	0 - 256
FC Topology	Point to Point only	Loop only	Loop only, Point to...
Fast Post	Disable	Enable	Disable, 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

10/08/2008 16:13:04 [VTL_53] Logged in | Server:VTL_53 | 4:15 PM

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.



Current Write Performance (MB/s): 0

Current Read Performance (MB/s): 0

10/08/2008 16:13:04 [VTL_53] Logged in | Server:VTL_53 | 4:17 PM

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.

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

To set a port:

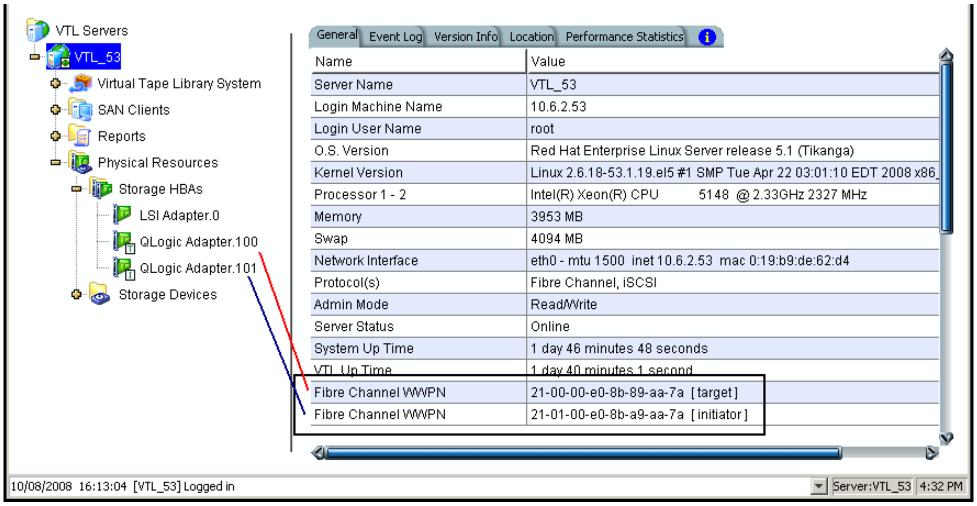
1. In the console, expand *Physical Resources*.

2. Right-click 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_
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]

10/08/2008 16:13:04 [VTL_53] Logged in | Server:VTL_53 | 4:32 PM

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.

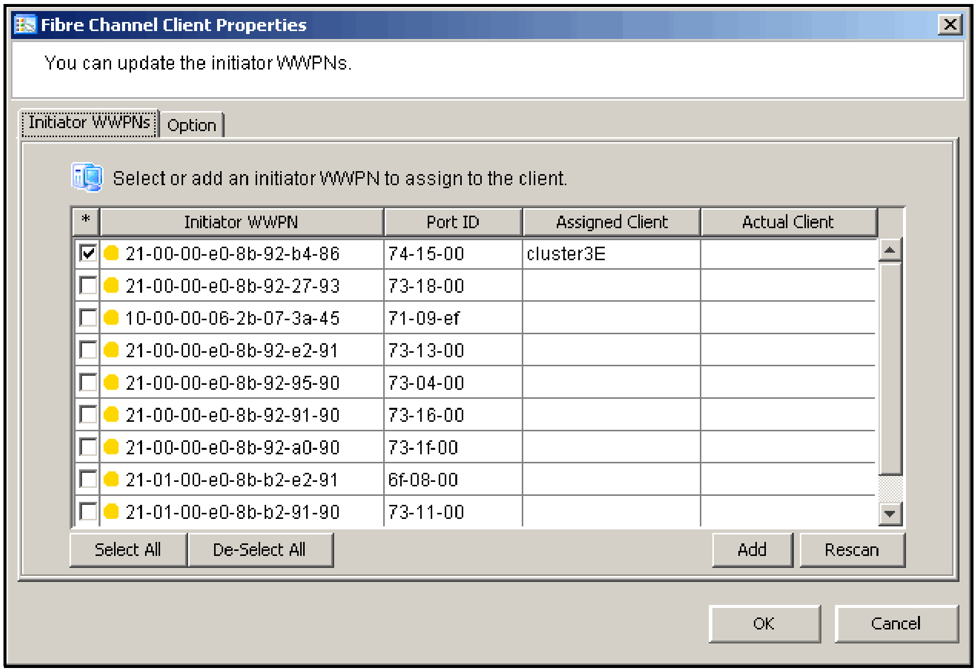
To simplify this process, when you enabled Fibre Channel, an *Everyone_FC* client was created under *SAN Clients*. This is a generic client that you can assign to all (or some) of your tape libraries/drives. It allows any WWPN not already associated with a Fibre Channel client to have read/write non-exclusive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

> **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.

Do the following for each client:

1. Highlight the Fibre Channel Client in the console.

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



You can update the initiator WWPNs.

Select or add an initiator WWPN to assign to the client.

*	Initiator WWPN	Port ID	Assigned Client	Actual Client
☑	● 21-00-00-e0-8b-92-b4-86	74-15-00	cluster3E	
□	● 21-00-00-e0-8b-92-27-93	73-18-00		
□	● 10-00-00-06-2b-07-3a-45	71-09-ef		
□	● 21-00-00-e0-8b-92-e2-91	73-13-00		
□	● 21-00-00-e0-8b-92-95-90	73-04-00		
□	● 21-00-00-e0-8b-92-91-90	73-16-00		
□	● 21-00-00-e0-8b-92-a0-90	73-1f-00		
□	● 21-01-00-e0-8b-b2-e2-91	6f-08-00		
□	● 21-01-00-e0-8b-b2-91-90	73-11-00		

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

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

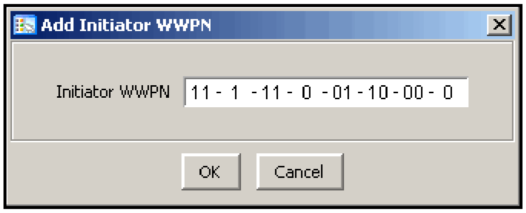
   - Most Fibre Channel switches allow administration of the switch through an Ethernet port. These administration applications have utilities to reveal or allow you to change the following: Configuration of each port on the switch, zoning configurations, the WWPNs of connected Fibre Channel cards, and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

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

   - The first time a new Client connects to the VTL Server, the following message appears on the server screen:
   FSQLtgt: New Client WWPN Found: 21 00 00 e0 8b 43 23 52

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

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



Initiator WWPN: 11 - 1 - 11 - 0 - 01 - 10 - 00 - 0

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.

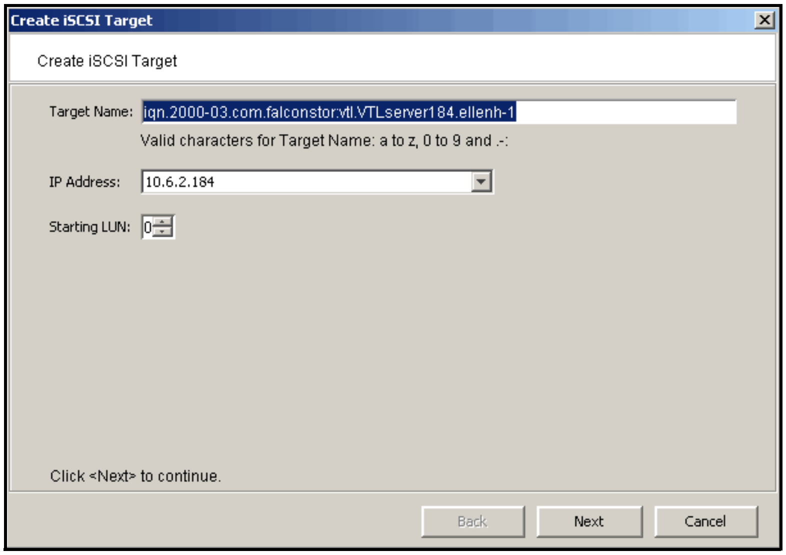
   More than one username/password pair can be assigned to the client, but they will be useful only when coming from the machine with an authorized initiator name.

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*.



Target Name: iqn.2000-03.com.falconstor:vtl.VTLserver184.ellenh-1

Valid characters for Target Name: a to z, 0 to 9 and .-:

IP Address: 10.6.2.184

Starting LUN: 0

Click <Next> to continue.

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.

   Note: 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.

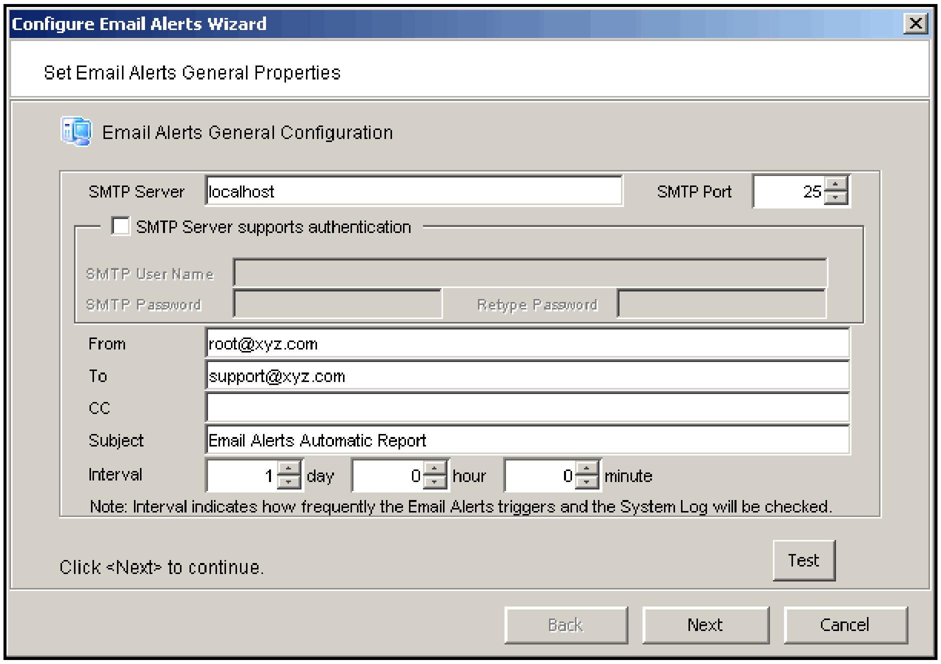
When an error is triggered, Email Alerts generates an email and sends it to a system administrator.

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.

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.

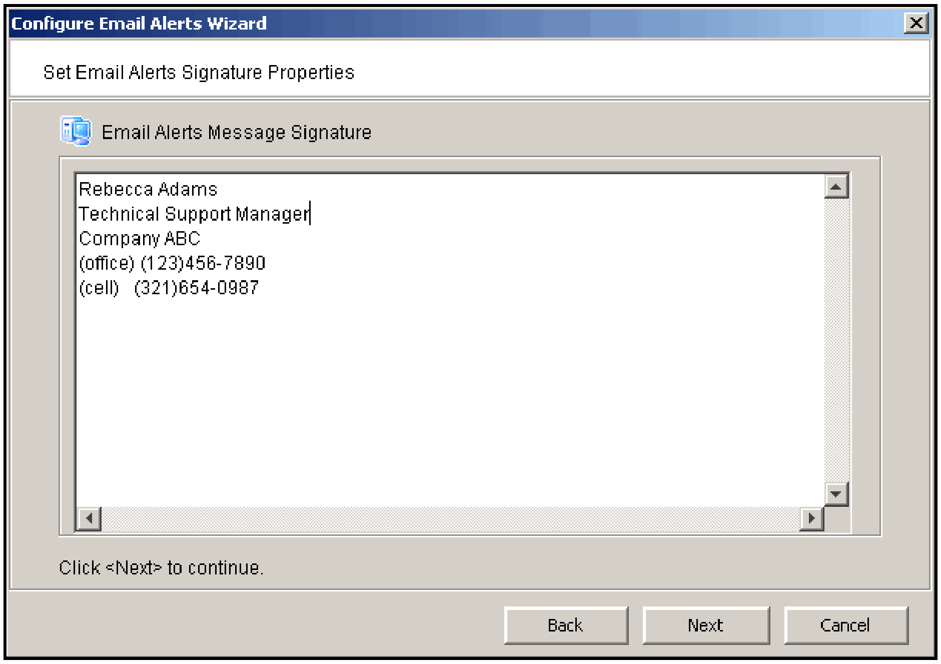
CC - Specify any other email accounts that should receive emails from Email Alerts.

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.

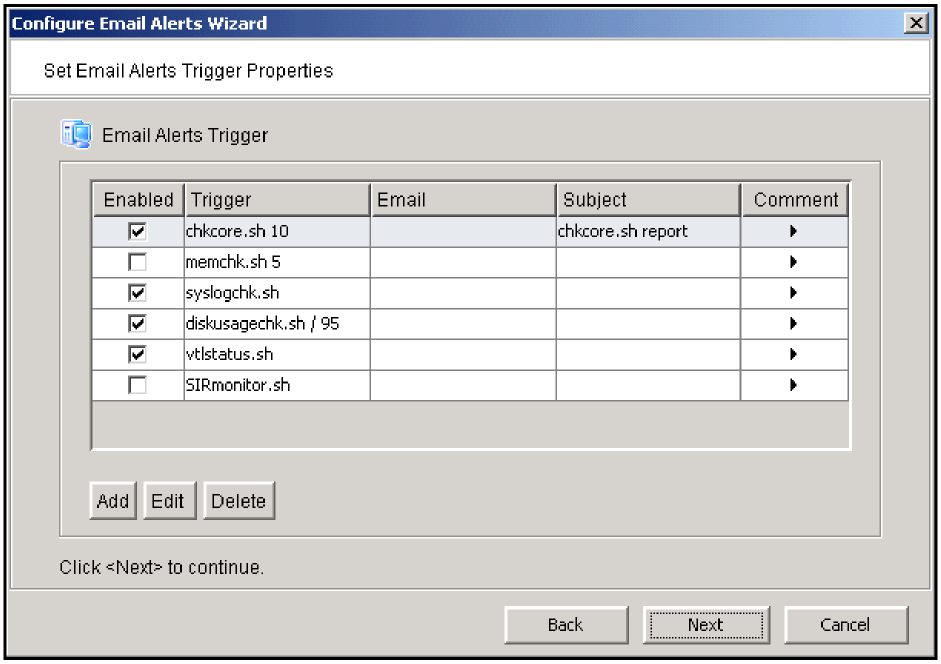
3. In the *Signature* dialog, enter the contact information that should appear in each Email Alerts email.


Configure Email Alerts Wizard
Set Email Alerts Signature Properties
Email Alerts Message Signature

Rebecca Adams
Technical Support Manager
Company ABC
(office) (123)456-7890
(cell) (321)654-0987

Click <Next> to continue.

4. In the *Trigger* dialog, set the triggers that will cause Email Alerts to send an email.


Configure Email Alerts Wizard
Set Email Alerts Trigger Properties
Email Alerts Trigger

Enabled	Trigger	Email	Subject	Comment
☑	chkcore.sh 10		chkcore.sh report	▸
□	memchk.sh 5			▸
☑	syslogchk.sh			▸
☑	diskusagechk.sh / 95			▸
☑	vtlstatus.sh			▸
□	SIRmonitor.sh			▸

Click <Next> to continue.

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).

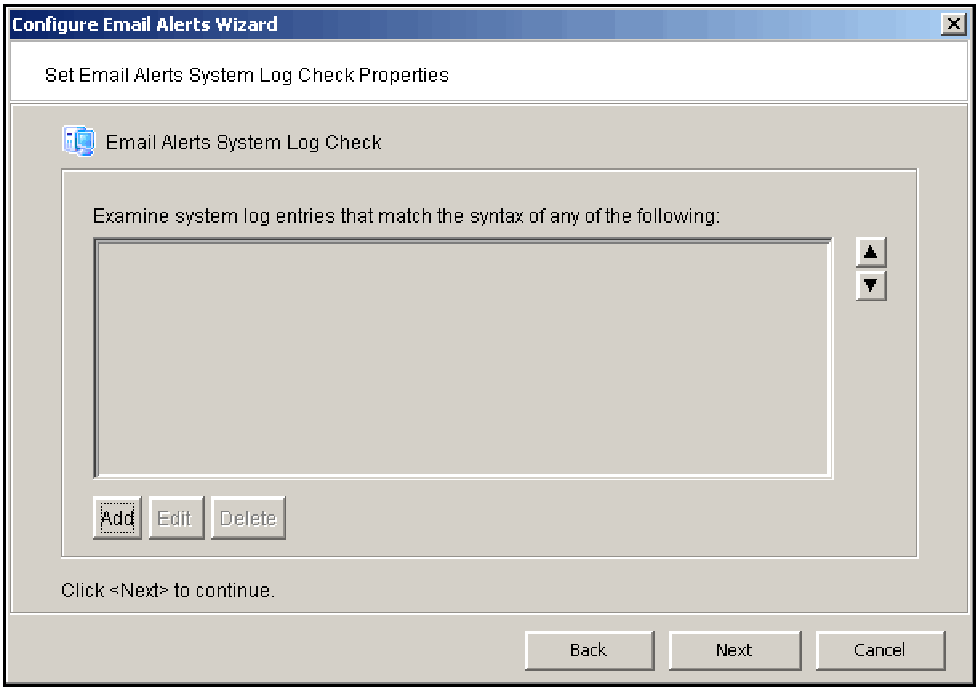
vtlstatus.sh (VTL status check) - This script calls “vtl status” and checks if any module of VTL has stopped. If so, Email Alerts sends an email report.

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.


Configure Email Alerts Wizard
Set Email Alerts System Log Check Properties
Email Alerts System Log Check

Examine system log entries that match the syntax of any of the following:

Click <Next> to continue.

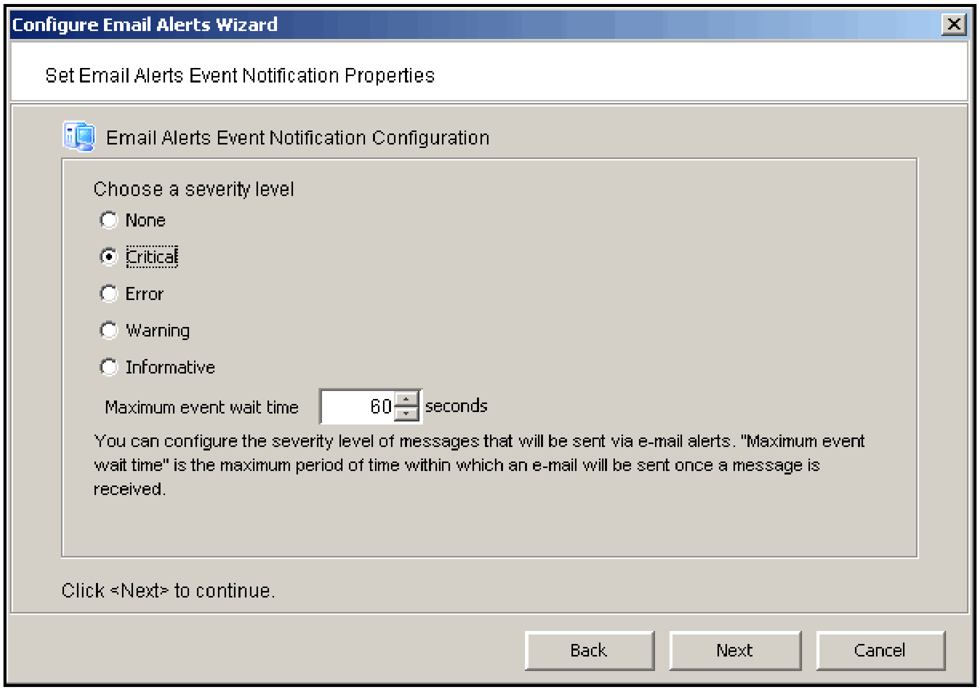
The system log records important events or errors that occur in the system, including those generated by VTL.

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.


Configure Email Alerts Wizard
Set Email Alerts Event Notification Properties
Email Alerts Event Notification Configuration
Back
Next
Cancel

Choose a severity level

○ None

● Critical

○ Error

○ Warning

○ Informative

Maximum event wait time 60 seconds

You can configure the severity level of messages that will be sent via e-mail alerts. "Maximum event wait time" is the maximum period of time within which an e-mail will be sent once a message is received.

Click <Next> to continue.

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:

- 0: No action is required and no email is sent.
- Non-zero: Email Alerts sends an email.

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.

Note: 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	--vdevid	VTL Virtual Device ID

Note: You only need to use the --server-username (-u) and --server-password (-p) arguments when you log into a server. You do not need them for subsequent commands on the same server during your current session.

Login/logout to the VTL Server

Log in to the VTL Server

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

iscon login [--server-name=<server-name> --server-username=<username>
--server-password=<password>|--environment] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to log into the specified VTL Server with a given username and password. Once successfully logged into the server, -u (--server-username) and –p (--server-password) are not necessary for the other CLI commands with optional –u and –p arguments.

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 is it is not specified.

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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 stanalone 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 then <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 maximun number of IE slots supported by the specified library type. The default is to use the maximum number of slots supported by the specified library type.

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

-I (--initial-size) and -C (--increment-size) are options to be specified with <capacity-on-demand> option. The default value for both options is 5 GB. The (--increment-size) cannot be less than 5 GB.

-m (--max-capacity) is an option to 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 createstandalonedrive -s <server-name> [-u <username> -p <password>]
-d <vdrive-type> [-r <vdrive-name-prefix>] [-R <num-of-drives>]
[-D -I <initial-size> -C <increment-size>] [-m <max-capacity>] [-X <rpc-timeout>]

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

Description:

This command creates a standalone virtual tape drive.

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

-I (--scsiaddress) is an option to specify specific physical devices to be used to create a virtual device. It can be a list of ACSLs separated by a comma or a file enclosed in <> containing an ACSL on each line.
ACSL=#:#:#:# (adapter:channel:id:lun)

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

-B (--barcode) is an option to either set the virtual tape with the provided barcode or create virtual tapes in batch mode configured with barcodes form the specified barcode range. The argument must be within the barcode range configured for the library and must not contain used barcodes. When provided as a barcode range, the option creates a virtual tape for each barcode in the range.

-t (--count) is an option to create multiple virtual tapes having the barcode automatically chosen from within the barcode range configured at library level. The library must have the required number of free slots available. If combined, "count" and "barcode" options must agree in number.

If the parent library has the auto-archive/remotecopy property enabled, use the following options to provide additional information for virtual tape creation:

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

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

-b (--physical-tape-barcode) is required to specify the list of physical tape barcode(s) when 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 <vdevid>
[-L <tape-library-vid> | -D <tape-drive-vid> | -l <slot-no>] [-X <rpc-timeout>]

iscon movevirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid> |
--slot-no=<slot-no>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command moves a virtual tape to a different location.

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

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

-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-vdevid> -S <target-name> [-U <target-username> -P <target-password>]
[-L <tape-library-vid> | -D <tape-drive-vid>] [-n <vdevname>] [-f]
[-X <rpc-timeout>]

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

Description:

This command copies a tape.

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

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

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

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

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

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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 removelicense -s <server-name> [-u <username> -p <password>] -k <license-keycode>
[-X <rpc-timeout>]

iscon removelicense --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --license=<license-keycode>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command removes a license keycode.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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-vdevid> -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-vdevid=<source-vdevid> --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-vdevid) is required to specify the ID of the virtual tape to be configured for replication.

-S (--target-name) is required to specify the target server name 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-vdevid) is the ID of the source virtual tape on the primary server to be resumed.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 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-vdevid> [-w <watermark(MB)> | [-d <YYYYMMDDHHMM> -i <#[H|M]>]] | [-r <on|off>]
[[-t <timeout>] [-I <retry-in]>] [-C <retry-for>]] [-c <on|off>] [-e <on|off>]
[-X <rpc-timeout>]

iscon setreplicationproperties --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--source-vdevid=<source-vdevid> [--watermark=<watermark(MB)>
[--watermark=<watermark(MB)> | [--date=<YYYYMMDDHHMM> --interval=<#[H|M]>]] |
[--repl-first <on|off>] [[--replication-timeout=<timeout>]
[--replication-retry-interval=<retry-in>] [--replication-retry-count=<retry-for]]
[--compression=<on|off>] [--encryption=<on|off>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to change the replication policy for the specified virtual tape.

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

Any combination of the following two options can be used to set up a replication trigger policy for a virtual with the tape caching property disabled.

-w (--watermark) is a data size based trigger in MB. The watermark is checked when the tape is unloaded from the tape drive and the replication is triggered if the amount of new data on the tape has reached the specified watermark.

-d (--date) combined with -i (--interval) is a time based trigger. The replication is triggered at the time specified by date and then repeated every interval. -d (--date) format is YYYYMMDDHHMM and -i (--interval) format is a number followed by H for hours or M for minutes (e.g. -i 2H or --interval=120M).

To delete a watermark trigger specify 0 for the watermark. To delete a time based trigger specify NA for date. At least one trigger must remain active.

The date argument is not required if you are only changing the interval.

For virtual tapes having the tape caching property enabled, 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 createvirlibinforeport -s <server-name> [-u <username> -p <password>]
[-o <filename>] [-X <rpc-timeout>]

iscon createvirlibinforeport --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 createvirtapeinforeport -s <server-name> [-u <username> -p <password>]
[-o <filename>] [-i] [-X <rpc-timeout>]

iscon createvirtapeinforeport --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 is10 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
```

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 *Physical Resources* object and select *Rescan*). Make sure that the *Discover New Devices* option is specified. Specify a *LUN Range* that you reasonably expect will include the LUN.

Check system log messages

Check the Event Log or syslog (/var/adm/messages) 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 **SCSI devices**, check the following:

- Make sure the system is powered on. Perform a power cycle to make sure.
- Physically make sure all the cable connectors are securely plugged in.
- 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.

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 *\tape<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".

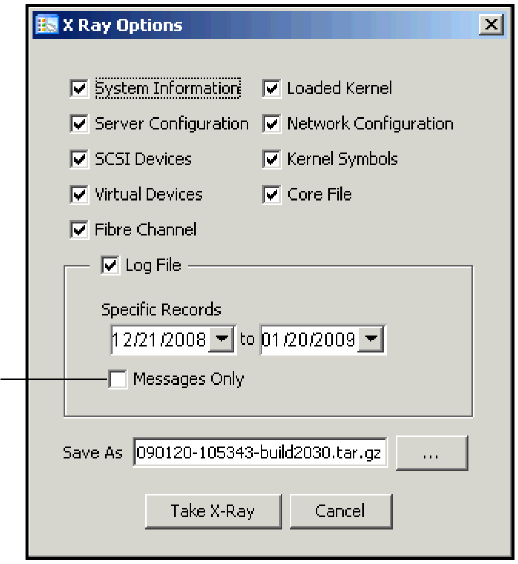
This can be caused due to corruption on the virtual tape. Replication will proceed as long as there are sectors available, even if a tape is corrupted.

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*.



☑ System Information ☑ Loaded Kernel
☑ Server Configuration ☑ Network Configuration
☑ SCSI Devices ☑ Kernel Symbols
☑ Virtual Devices ☑ Core File
☑ Fibre Channel
☑ Log File
Specific Records
12/21/2008 to 01/20/2009
☐ Messages Only
Save As 090120-105343-build2030.tar.gz

Filter out and include only VTL messages from the System Event Log.

2. Based on the discussion with your Technical Support representative, select the options you want to include and set the file name.

3. Click the *Take X-Ray* button.

Index

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com

Argentina: 5411-4317-5636 • **Australia:** 1-800-550-786 • **Austria:** 43-1-601-26-0 • **Balkans:** 301-6188-111 • **Belgium:** 32 2-704 89 83 • **Brazil:** 55-11-51872100 • **Brunei:** 65-216-8333 • **Canada:** 1-800-422-8020 **(General)**; 416-964-2001 **(Learning Management System Sales,Toronto)** • **Chile:** 562-372-4500 • **Colombia:** 571-629-2323 **Czech Republic:** 420 2 33009311 • **Denmark:** 45 4556 5040 • **Egypt:** 00 202 570 9442 • **Finland:** 358-9-525-561 • **France:** 33-1-41-33-17-17 • **Germany:** 49-89-460-08-2788 • **Greece:** 30-01-6188101 • **Hong Kong:** 852-2877-7077 • **Hungary:** 361-202-4415 • **India:** 91-80-229-8989 • **Indonesia:** 65-216-8333 • **Ireland:** 353-1-668-4377 **Israel:** 972-9-9710500 • **Italy:** 39-02-9259511 • **Japan:** 81-3-5779-1820 • **Korea:** 82-2-3453-6602 • **Malaysia:** 603-2116-1887 • **Middle East:** 00 9714 3366333 • **Mexico:** 525-261-0344 • **Netherlands:** 31-33-4515200 • **New Zealand:** 0800-786-338 • **North West Africa:** 00 9714 3366333 • **Norway: From Norway:** 47-22023950, **To Norway:** 47-23369650 • **Pakistan:** 00-9714-3366333 • **People's Republic of China:** 8610-6803-5588 • **Philippines:** 632-885-7867 • **Poland:** 48-22-8747848 • **Portugal:** 351-21-413-4000 • **Russia:** 7-095-935-8411 • **Saudi Arabia:** 00 9714 3366333 • **Singapore:** 65-216-8300 • **South Africa:** 27-11-256-6300 • **Spain:** 34-902-210-412 • **Sri Lanka:** 65-2168333 • **Sweden:** 46-8-631 22 00 • **Switzerland:** 41-1-908-90-50 **(German)** 41-22-999-0444 **(French)** • **Taiwan:** 886-2-25185735 • **Thailand:** 662-344-6855 • **Turkey:** 90 212 335 22 00 • **United Kingdom:** 44-1276-416-520 • **United States:** 1-800-422-8020 • **Venezuela:** 582-905-3800 • **Vietnam:** 65-216-8333 • **Worldwide Headquarters:** 1-650-960-1300