SGI® COPAN™ 400

USER GUIDE

007-5819-001

SGI COPAN 400 User Guide
Version 7.50

Document Number: 007-5819-001 31312.7371

Contents

Introduction

Plan your Deployment

Getting Started

Management Console

Multi-Node Groups

Tape Libraries, Tape Drives, and Tapes

Server Failover

Data Replication

Reports

Automated Tape Caching

Fibre Channel Configuration

iSCSI Clients

IBM System i Configuration

Hosted Backup

NDMP Backup Support

ACSLS and Library Station Configuration

Email Alerts

COPAN 400 Server

Command Line

SNMP Integration

Troubleshooting

Appendix

Index 377

Introduction

SGI COPAN 400 overview

SGI COPAN 400 increases the speed and reliability of backups that use standard third-party backup applications by leveraging disk to emulate industry-standard tape libraries. COPAN 400 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 COPAN 400 uses disk to back up data, it eliminates the media and mechanical errors that can occur with physical tapes and drives. And, because COPAN 400 can emulate more tape drives than your physical tape library really has, more backup streams can run simultaneously, enabling organizations to easily complete their backups within the allotted backup window.

Because you may already have physical tapes that you would like to protect, you can import data from physical tapes into your virtual tape system. If you ever need to recover files from a physical tape, you can use COPAN 400 to access those tapes for immediate recovery.

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

COPAN 400 components

There are several components to COPAN 400:

- COPAN 400 appliance - An appliance running COPAN 400 software.
- COPAN 400 Console - The graphical administration tool where you manage COPAN 400, add/configure clients, set properties, import/export tapes, and view statistics. Many of the console functions can also be performed via a command line utility. Refer to "Command Line" for more details.
- COPAN 400 Clients - The backup servers that use COPAN 400. COPAN 400 supports Fibre Channel and iSCSI backup servers on most major platforms. If the Hosted Backup feature is available, you can install a certified backup application directly on the COPAN 400 appliance, eliminating the need for a dedicated backup server.

Plan your Deployment

When planning your COPAN 400 deployment, you need to determine what type of configuration best suits your organization. In addition to disk-to-disk, the flexibility of SGI COPAN 400 supports three possible disk-to-disk-to-tape (D2D2T) configurations.

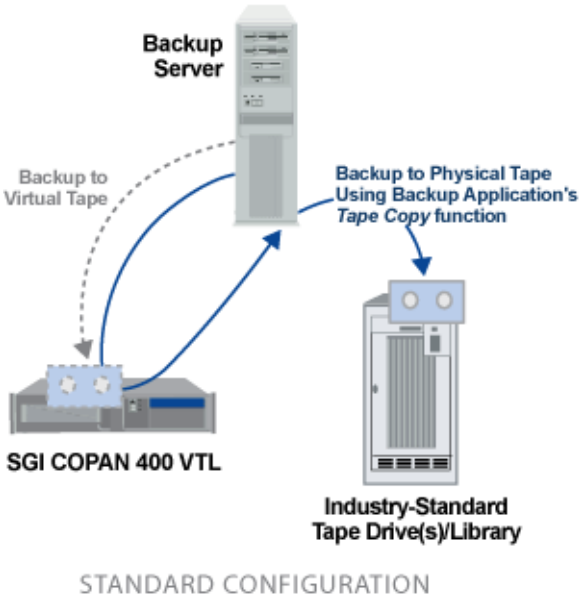
In a D2D2T scenario with SGI COPAN 400, you choose your preferred configuration of the various components— your third party backup software, the COPAN 400 appliance, the disk storage managed by COPAN 400 for use as the virtual tape library, and one or more physical tape libraries. Regardless of which configuration you choose, COPAN 400 makes it easy for you to manage both virtual tapes and physical tapes.

COPAN 400 configurations for disk-to-disk-to-tape backup

- **Standard Configuration** - Backup software runs on a backup server or on the COPAN 400 appliance and manages all tapes—virtual and physical. Data is copied to physical tape using the backup software's tape copy function.
- **Advanced Configuration** - Backup software runs on a backup server and manages the backup to virtual tape. COPAN 400 manages the disk storage and the export of data to the physical tape library.
- **Automated Tape Caching Configuration** - As in the *Advanced* Configuration, backup software runs on a backup server and transparently manages the backup to virtual tape. In addition, this configuration provides the backup application with transparent access to data regardless of whether the data is on disk or on tape. Flexible migration policies determine when data will be moved to physical tape.

Standard COPAN 400 Configuration

In the Standard COPAN 400 Configuration, the backup software manages all tapes—virtual and physical—by treating the virtual tape library as though it were just another standalone tape library attached to the backup server. To copy data from virtual to physical tapes, the backup software's *Tape Copy* function is utilized.



In this configuration, the backup software runs on an existing backup server or on the COPAN 400 appliance itself (with the Hosted Backup Option).

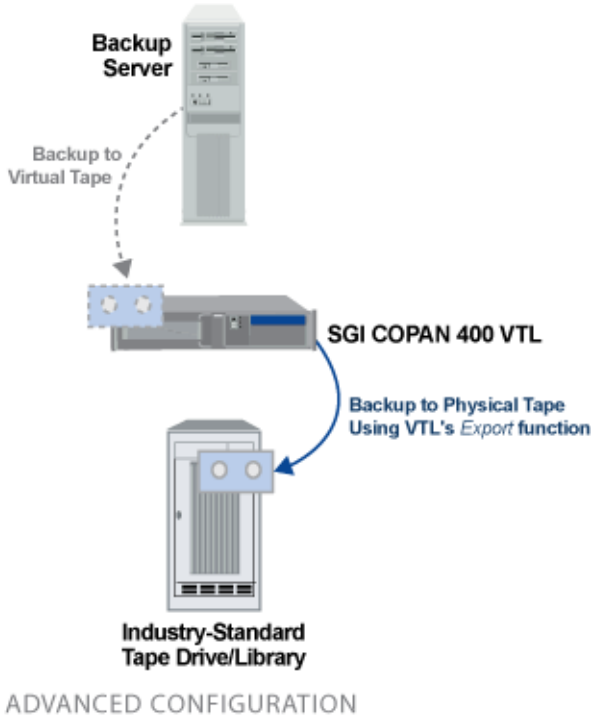
The Standard COPAN 400 Configuration is ideal for organizations that already have a backup process in place with which they are comfortable but which is not meeting all of their backup objectives. Adding a COPAN 400 appliance as another tape library allows you to easily increase your parallel backup streams and take advantage of COPAN 400's rapid data recovery without having to alter your current configuration. With the backup application managing the entire backup process, virtual tapes and physical tapes are seen in the same way: a virtual tape is *just another tape*.

With the Standard COPAN 400 Configuration, backups to virtual tapes occur quickly. Then, at a later time, the backup server can copy the data to physical tapes without impacting the production environment. Because the backup server performs the tape copying function in addition to backups additional overhead can be incurred by the backup server. Therefore, it is best to perform tape copying at off-peak hours.

While COPAN 400 natively accelerates backup from the backup server to virtual tape, data transfer between application servers and the backup application can be accelerated by hosting a backup application on the COPAN 400 appliance itself. This shortens the data path between the application server and the backup application/server and therefore enhances backup performance.

Advanced COPAN 400 Configuration

In the Advanced COPAN 400 Configuration, the backup software manages backups to the virtual tape library while the COPAN 400 appliance controls the export of data from virtual tapes to physical tapes.



COPAN 400 dramatically accelerates backups by acting as a *defacto* cache to your physical tape library and enables data to be moved to physical tapes as a background process without impacting production servers. This is an innovative approach to backup that addresses the limitations of conventional tape backup. Moreover, since COPAN 400 manages the export of data from virtual to physical tapes, there is no additional overhead for the backup server.

As in the Standard COPAN 400 Configuration, the backup software runs on an existing backup server or on the COPAN 400 appliance itself (with the Hosted Backup Option).

With the Advanced COPAN 400 Configuration, backups to virtual tapes occur very quickly. Then, at a later time, when you are done using a given tape, you can export data to physical tape for offsite vaulting or disaster recovery without impacting the production environment. COPAN 400 can also be set up in Auto Archive mode so that after each backup to virtual tape completes, data is automatically exported to physical tape.

The Advanced COPAN 400 Configuration requires you to set up the initial physical tape library emulation from within the COPAN 400 Console so that there is a 1:1 mapping, with identical barcodes, between virtual and physical tapes. This enables the backup software to keep track of backup tapes and prevents tapes from being created that would be unidentifiable by the backup software.

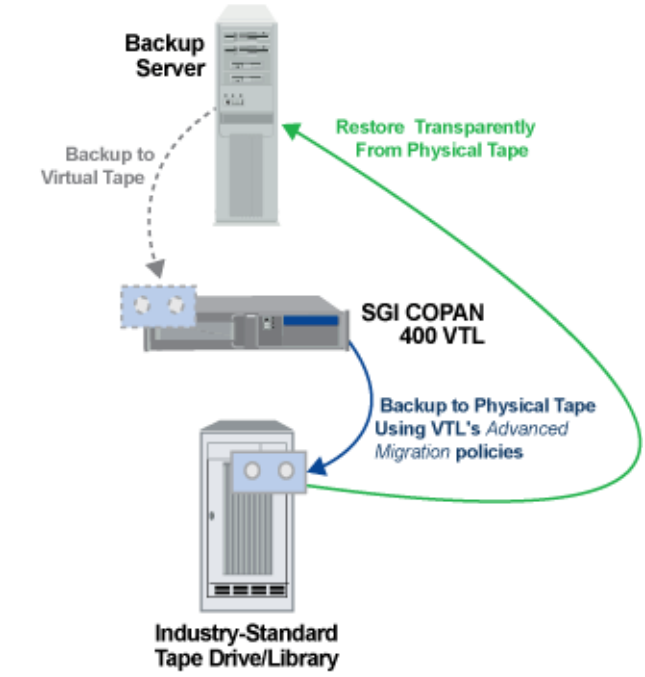
Whenever data is written to physical tape, the virtual tape can then be deleted or the copy can be left on the virtual tape for rapid recovery. The physical tape will always have the same barcode as its virtual tape counterpart. This gives you the flexibility to easily restore from either virtual or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

When it comes time to restore, the backup software identifies the barcode of the tape containing the needed data. If the data still resides on virtual tape (it was never exported or it was exported with the virtual tape left intact), it can be restored very quickly because it is being read from disk. If the data is only on physical tape, the

tape must first be re-imported into COPAN 400 with a few simple keystrokes in the COPAN 400 Console so that the backup software can access it and restore in its usual manner.

Automated Tape Caching COPAN 400 Configuration

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



AUTOMATED TAPE CACHING CONFIGURATION

As in the Advanced COPAN 400 Configuration, backup software runs on a backup server and transparently manages the backup to virtual tape.

In this configuration, COPAN 400 acts as a transparent cache to the physical tape library, dramatically accelerating backups while enabling the data to be written to physical tapes, as a background process without impacting production servers, based on extremely flexible migration policies (age of data, time of day, disk space, end of backup, etc.). The Automated Tape Caching Option also provides very flexible space reclamation policies (free space immediately upon migration, after specified retention period, when run out of space, etc.)

Getting Started

COPAN 400 has been designed for quick setup. Once you connect your COPAN 400 appliance to your storage network (as described in the *Hardware QuickStart Guide*), you should follow the instructions in the *Software QuickStart Guide* to set network information, change administrator passwords, and enter license keys. Both guides were shipped with your appliance.

The following steps guide you through configuring your COPAN 400 appliance.

Run the SGI Management Console

The SGI Management Console for COPAN 400 is the graphical administration tool that enables you to manage COPAN 400. The computer that runs the COPAN 400 console needs connectivity to the network segment where COPAN 400 is running, because it communicates directly with the server and clients (backup servers). There are two ways to run the COPAN 400 console.

Launch the web-based console

To launch a web-based version of the console, open a browser from any machine and enter the IP address of the COPAN 400 server **(**for example: http://10.0.0.2) and the console will launch. If you have *Web Setup,* select the *Go* button next to *Install Management Software and Guides* and click the *Launch Console* link.

In the future, to skip going through Web Setup, open a browser from any machine and enter the IP address of the COPAN 400 server followed by **:81,** for example: http://10.0.0.2**:81**/ to launch the console. For easier access, you may want to save the location as a Favorite or Bookmark.

Note: In order to launch the console using the IP address of the COPAN 400 server followed by **:81**, you must first download US_export_policy.jar and local_policy.jar from http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html and replace the versions in your java runtime directory:

- Unix - <java-runtime-home>/lib/security
- Win32 - <java-runtime-home>\lib\security

Install and launch the console on an administrative computer

To install the SGI Management Console software from Web Setup, open a browser from any machine and enter the IP address of the COPAN 400 server **(**for example: http://10.0.0.2). *S*elect the *Go* button next to *Install Management Software and Guides* and click the *Install Windows Console* link. You can install the SGI

Management Console onto any machine, as long as that machine has a Graphical User Interface. Note that if you are installing the console on a Windows machine, you must be a Power User or Administrator.

To launch the console after installation, select *Start* --> *Programs* --> *SGI* --> *COPAN 400 <version>.*

Connect to your server

If your server already appears in the tree, right-click it and select *Connect*. For a multi-node group, right-click the group and select *Connect* to connect to all of the servers in the group.

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 COPAN 400 servers in a range of IP addresses. You should then specify the subnet range of your COPAN 400 server and wait for the COPAN 400 server hostname to appear in the navigation tree. For COPAN 400 appliances, the hostname has the format FS*xxxxx*, where *xxxxx* is a unique number for your COPAN 400 appliance, which is displayed on a label on your appliance. When the hostname appears in the navigation tree, right-click it and select *Connect*.

2. Type the COPAN 400 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.

   If you purchased an appliance from SGI, log in with *fsadmin* as the User Name. The default password is *IPStor101* but this may have been changed in Web Setup.

   If you want to be able to add accounts or set network configuration in the console, log into your appliance with the “root” user and password (default “IPStor101”).

   The user name and password are case sensitive.

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

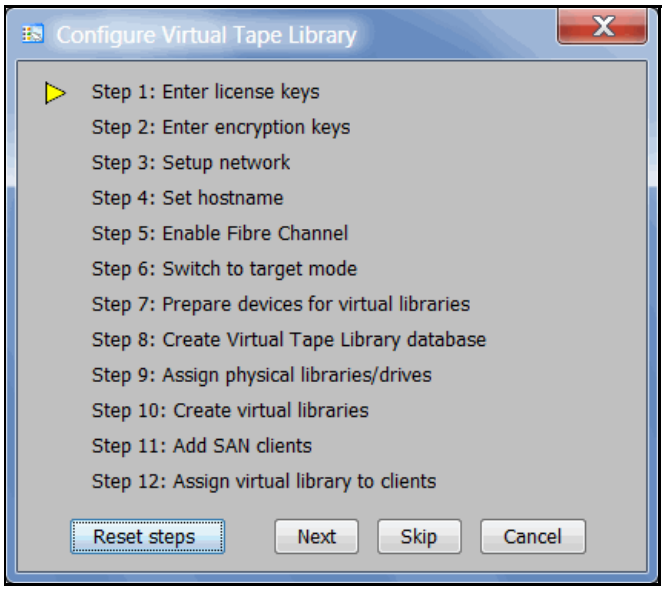
   After connecting to the server, the configuration wizard launches.

Configure your server using the configuration wizard

Notes:

- If you are using COPAN 400 in a Fibre Channel environment, refer to the "Fibre Channel Configuration" section first before beginning the wizard.
- If you are setting up a failover configuration, refer to the "Server Failover" section first before beginning the wizard.

COPAN 400 provides a convenient wizard that leads you through your COPAN 400 configuration. If your COPAN 400 server has not been configured yet, the configuration wizard will be launched when you connect to it.



Click *Next* to begin the steps in the wizard. If you already completed a step in Web Setup, select *Skip* to skip that step here.

Step 1: Enter license keys

Click the *Add* button and enter the keycodes shown on your Product Keycode certificates, one at a time.

Be sure to enter keycodes for any options you have purchased. Each COPAN 400 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 your COPAN 400 server appliance and select *License*.

Step 2: Enter encryption keys

Indicate if you want to add encryption keys. With encryption, you can create one or more keys that can be used to encrypt data when it is exported to physical tape and decrypt it when it is imported back to virtual tapes. The data on the tape cannot be read without being decrypted using the appropriate key.

1. Click *New*.
2. In the *Key Name* text box, type a unique name for the key.
3. In the *Secret Phrase* text box, type the phrase that will be used to encrypt the data.

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

4. In the *New Password* and *Confirm Password* text boxes, type a password for accessing the key.

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

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

5. In the *Password Hint* text box, type a hint that will help you remember the password.

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

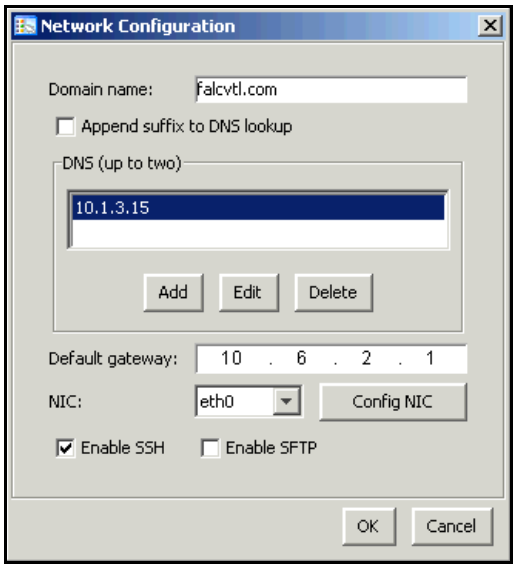
   Refer to 'Encrypt data on virtual and physical tapes' for detailed information about encryption keys.

Configuration note: After completing the configuration wizard, if you need to add encryption keys, you can right-click your COPAN 400 server appliance and select *Key Management*.

Step 3: Set up network

Note: Changing the IP address is allowed only before you configure replication. To change the IP address after you configure replication, you must remove the replication target, change the IP address, and then configure replication again.

1. Enter information about your network configuration.



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.

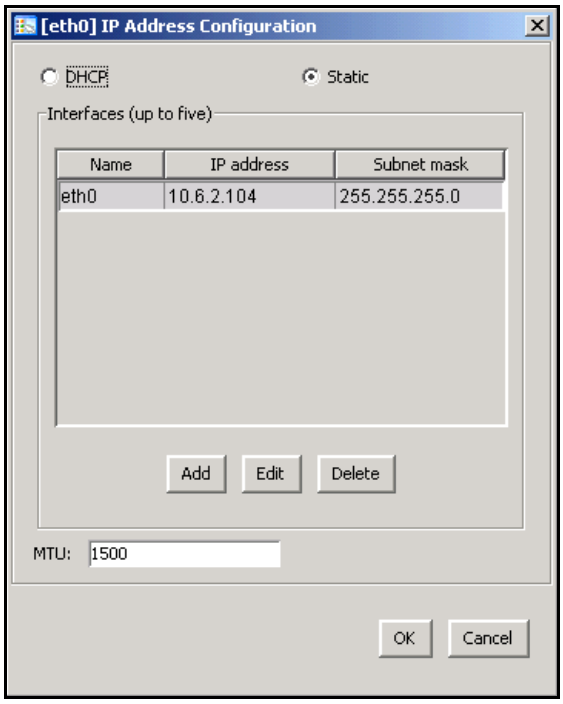
Default gateway - IP address of your default gateway.

NIC - List of Ethernet cards in the server.

Enable SSH - Enable/disable the ability to use the SSH protocol. The COPAN 400 server must have “openssh” installed in order to use SSH.

Enable SFTP - Enable/disable the ability to securely FTP into the server.

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



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

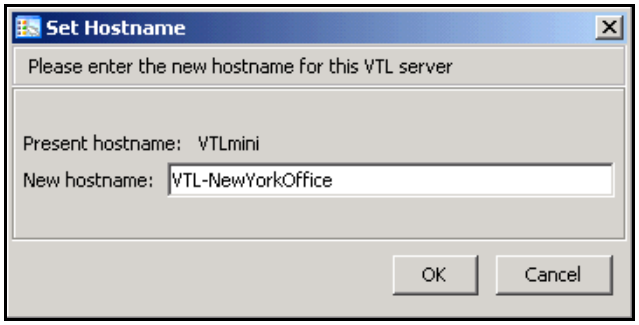
MTU - Set the maximum transfer unit of each IP packet. If your card supports it, set this value to 9000 for jumbo frames.

Configuration note: After completing the configuration wizard, if you need to change these settings, you can right-click your COPAN 400 server appliance and select *System Maintenance --> Network Configuration*.

Step 4: Set hostname

Enter a valid name for your COPAN 400 appliance.

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



Configuration note: After completing the configuration wizard, if you need to change the name again, you can right-click your COPAN 400 server appliance and select *System Maintenance --> Set Hostname*.

Step 5: 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.

If you do not have or will not be using Fibre Channel, click *Skip*. Otherwise, this step takes just a few seconds and there are no additional screens to go through.

Step 6: Switch to target mode

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

If you haven't already done so, you will need to switch any initiator zoned with a backup server to target mode so that the backup server can see the COPAN 400 server. You will then need to select the equivalent adapter on the secondary server and switch it to target mode.

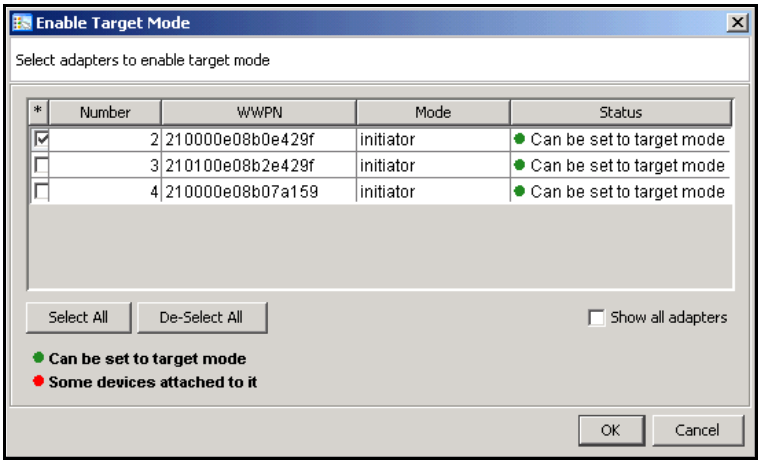
You will get a *Loop Up* message on your COPAN 400 server if a QLogic port has successfully been placed in target mode.

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.

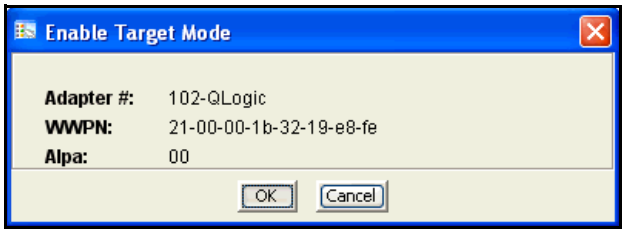
Alternatively, for QLogic HBAs, you can find the WWPN in the BIOS (press Ctrl+Q during boot up).

For Failover, if you are not using multi-ID HBAs, you minimally need two ports for client connectivity (one for normal operation, one for standby) and one initiator port to connect to storage. If you are using multi-ID HBAs, you need a minimum of one port for client connectivity and one for storage.

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



(Multi-ID HBAs) Click *Ok*.



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 7: Prepare devices for virtual libraries

This step prepares physical devices for use with COPAN 400. Depending upon your configuration, this step can take just a few seconds and there will be 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.*

Step 8: Create Virtual Tape Library database

The database contains the configuration information for the COPAN 400. If your COPAN 400 appliance has been preconfigured, this step takes just a few seconds and there are no additional screens to go through. If your COPAN 400 appliance has not been preconfigured, you must have already prepared storage resources for use with COPAN 400.

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.

   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 for you using an available device(s), but is not recommended unless your appliance has been preconfigured.

2. If desired, enable disk compression for COPAN 400.

   This can save disk space because it compresses the data that is being written to your virtual tapes. It does not affect data that is exported to physical tapes because that is controlled by the tape drive.

3. (Tape Caching only) Set the global *disk capacity* threshold.

   When this threshold value is reached, migration from virtual tape to physical tape will be triggered for all virtual libraries using the disk capacity threshold.

4. Click *Finish* to create the database.

   If you know that you have a disk available, you can create a mirror for the COPAN 400 database in order to protect your COPAN 400 configuration. Even if you lose your COPAN 400 server, the data on your tapes will be maintained. Mirroring the database is highly recommended. Refer to 'Mirror the database to protect your COPAN 400 configuration' for more information.

Configuration note: After completing the configuration wizard, if you want to enable disk compression, right-click the *Virtual Tape Library System* object and select *Properties*. To mirror the database at a later time, right-click the *Database* object (under the *Virtual Tape Library System* object) and select *Mirror --> Add*.

Step 9: Assign physical libraries/drives

If you will be importing data from physical tapes into your virtual tape library or exporting virtual tapes to physical tapes, you must assign your physical tape libraries/drives to COPAN 400.

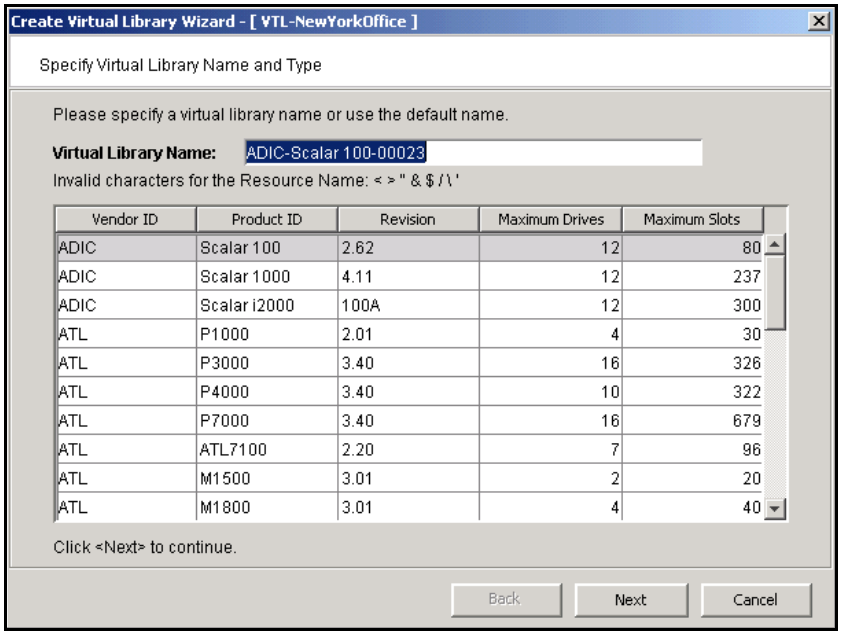
This step also inventories the physical tapes in your library/drive so that you can create virtual tapes that match your physical tapes.

Note: COPAN 400 does not support physical libraries when tape drive numbering does not start with 0 or is not sequential.

Configuration note: After completing the configuration wizard, if you need to assign new physical libraries/drives and inventory slots again, you can right-click *Virtual Tape Library System* and select *Configuration wizard*.

Step 10: Create virtual libraries

Select the tape library that you are emulating.



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

If you are using *Automated Tape Caching*, you will only see your physical tape libraries listed. Select the check box and the system will automatically match your physical library.

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.
- If you are using Automated Tape Caching, you will have to select the type of data migration triggers that you want to set and specify when the data that has been migrated to physical tape can be deleted to free up cache disk space.
- If you are not using Automated Tape Caching, you need to determine if you want to use auto archive *or* auto replication for this virtual library.

Refer to 'Create virtual tape libraries' for detailed information about creating virtual tape libraries and 'Automated Tape Caching' for detailed information about configuring Automated Tape Caching.

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

Configuration note: After completing the configuration wizard, if you need to create virtual tape libraries, you can right-click the *Virtual Tape Libraries* object and select *Add*. If you need to add drives to an existing virtual tape library, you can right-click the library and select *New Drive(s)*.

Step 11: Add SAN clients

This step allows you to select the 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 12: Assign virtual library to clients

If you added clients, do the following:

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

Refer to 'Assign virtual tape libraries and drives to backup servers' for detailed information about assigning libraries to clients.

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*.

Add SAN Clients (backup servers)

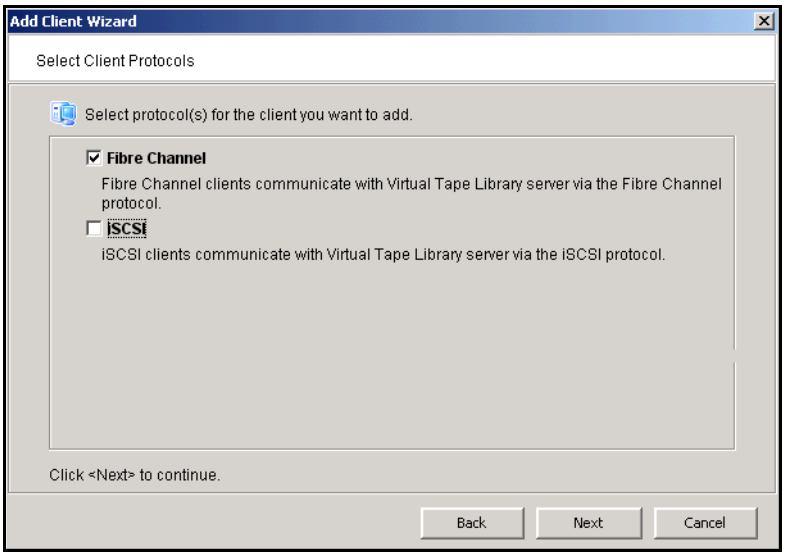
You can add SAN Clients in the following two ways:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *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 or IP address.

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



For Fibre Channel clients, click *Next* and select the *initiator* WWPN for the client. If FC initiator ports on the backup server are already zoned with COPAN 400's target port and are properly connected/powered up, they are listed automatically and you can select specific initiators from that zone. In addition, if there is only one initiator WWPN in the client, COPAN 400 will automatically select it for you and the dialog will not be displayed. If no WWPNs are listed, the backup server is not currently zoned with the COPAN 400 appliance.

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.

Select *Enable Celerra Support* if you have a licensed EMC Celerra client.

For iSCSI clients, click *Next* and select the initiator that the client uses. If the initiator does not appear, you can manually add it. For additional details on adding and managing iSCSI clients, refer to the "iSCSI Clients" chapter.

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 COPAN 400 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 user name and password. More than one user name/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.

Prepare for backups

Backup server access to the COPAN 400 server

COPAN 400 uses a “Secured Access” scheme, whereby access is dictated by creating specific clients to represent specific backup servers. A backup server can access *only* its own designated virtual tape library or drives via a dedicated port.

FC backup servers

In order for Fibre Channel backup servers to access COPAN 400 resources, you must do the following:

1. Set QLogic HBA ports to target mode.
2. Add a FC client for each backup server.
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 COPAN 400 resources, you must do the following:

1. Add an iSCSI client for each backup server.
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 COPAN 400 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 COPAN 400 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 COPAN 400 server, you can start to use the COPAN 400 as if it were a real physical 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 COPAN 400 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.
   - COPAN 400: 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 COPAN 400.

   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 COPAN 400 server, obviously there is no keypad or physical mail slot for this purpose. However, the SGI COPAN 400 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 COPAN 400 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 COPAN 400 console and right-click the virtual tape and select *Move to Vault*.

Special note for NetBackup users - To prevent a backup from going to the same tape more than once, when you are configuring backup jobs for Microsoft Exchange, DO NOT span your policies across tapes.

Confirm successful backups

While a backup job is running, you can use the COPAN 400 console to verify that data is being written to virtual tapes.

1. In the COPAN 400 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.

Management Console

The SGI Management Console for COPAN 400 allows you to manage your COPAN 400 system, users, and administrators; add/configure clients; set server properties; monitor COPAN 400 activity; manage the import/export of tapes, and run/view reports.

Launch the console

To launch an installed version of the console, select *Start* --> *Programs* --> *SGI* --> *COPAN 400* <*version*>.

To launch a web-based version of the console, open a browser from any machine and enter the IP address of the COPAN 400 server **(**for example: http://10.0.0.2) and the console will launch. If you have *Web Setup,* select the *Go* button next to *Install Management Software and Guides* and click the *Launch Console* link.

In the future, to skip going through Web Setup, open a browser from any machine and enter the IP address of the COPAN 400 server followed by **:81,** for example: http://10.0.0.2**:81**/ to launch the console. The computer running the browser must have Java Runtime Environment (JRE) version 1.6.

Note: In order to launch the console using the IP address of the COPAN 400 server followed by **:81**, you must first download US_export_policy.jar and local_policy.jar from http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html and replace the versions in your java runtime directory:

- Unix - <java-runtime-home>/lib/security
- Win32 - <java-runtime-home>\lib\security

Connect to your server

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

   If you have a multi-node group, right-click the group and select *Connect* to connect to all of the servers in the group. You must use a user name and password that exists for all servers in the groups.

   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 COPAN 400 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: 

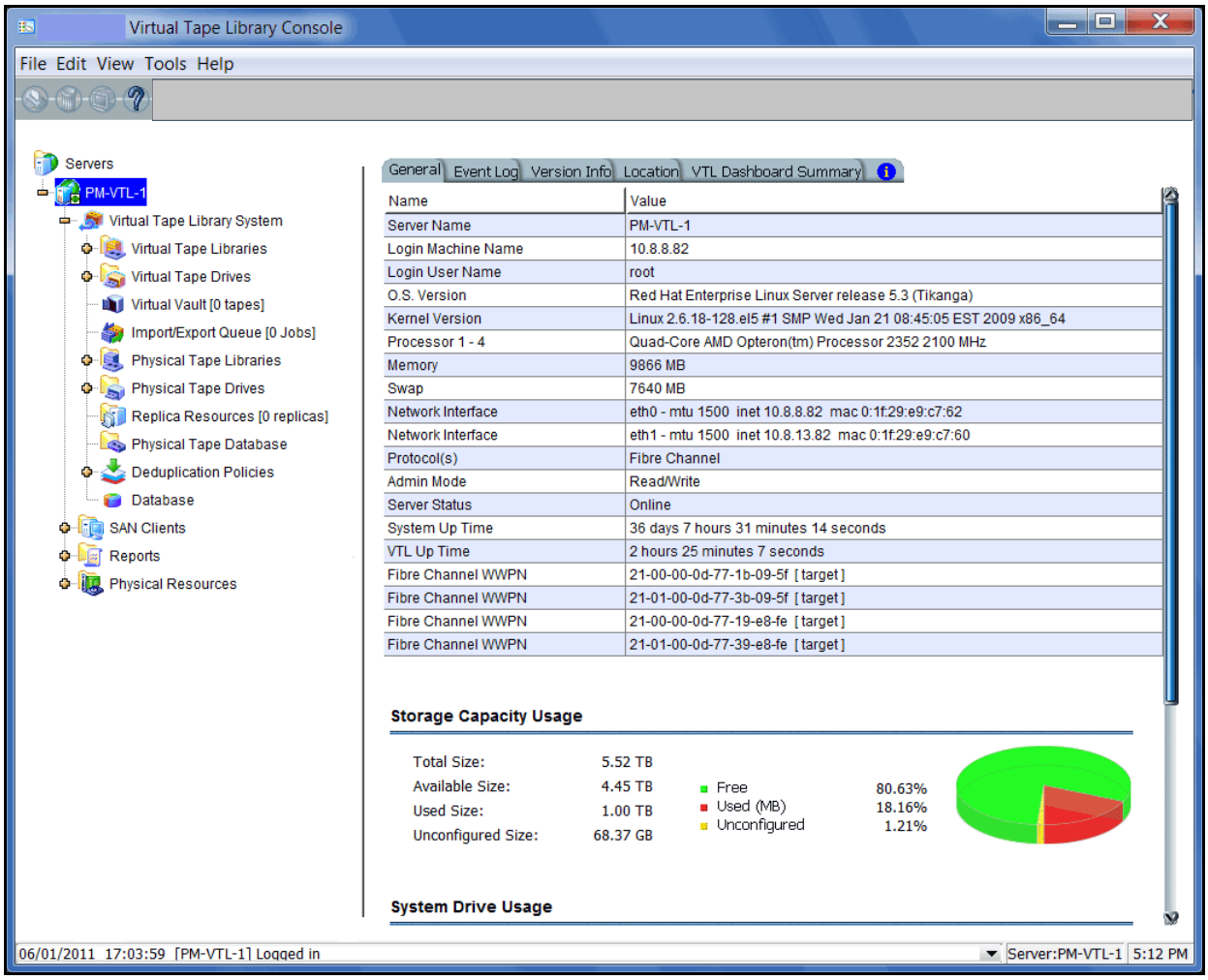
If you connect to a server that is part of a failover configuration, you will automatically be connected to both servers.

Note: Multiple 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 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.

Console user interface

The console displays the configuration for your COPAN 400 appliance. The information is organized in a familiar Explorer-like tree view.



The tree allows you to navigate the various COPAN 400 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 on the item will also toggle the expanded/collapsed view of the item.

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

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

The console log located at the bottom of the window displays information about the activities performed in this console. The log 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

Multi-Node Group object

If you have configured multi-node groups, the group object contains the servers that have been grouped together.

All of the servers in a group can be managed together. From the group level, you can manage user accounts for all servers in the group and you can set common configuration parameters, such as SNMP settings, storage monitoring trigger threshold, tape caching thresholds, compression settings, and X-rays. You can also log in to all of the servers in the group at the same time.

For more information about groups, refer to “Multi-Node Groups”.

Server object

From the server object, you can manage administrator accounts for that server, add/remove licenses, change the system password, configure server-level options such as failover and email alerts, perform system maintenance, set tape encryption keys, generate an x-ray file, join a group, 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 COPAN 400 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 COPAN 400 server and console software.
- *Location* - Displays information about the location of this server and who is responsible for maintaining it. This tab only appears if the location information was set (via *Server Properties*).
- *Attention Required* - Appears when the system has information to report.
- *Failover Information* - Displays the current status of your failover configuration, including all settings. This tab only appears if failover is configured.
- *VTL Dashboard Summary* - Displays information about the COPAN 400 server, including capacity information and capacity and performance statistics.

Virtual Tape Library System object

The *Virtual Tape Library System* object contains all of the information about your COPAN 400 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 Automated Tape Caching policies (if you are using this option)
- Set tape properties for the library (enable/modify tape capacity on demand, change maximum tape capacity)
- 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

When you select a virtual tape in the list, information about that tape is displayed in the lower portion of the information pane.

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 appear in the virtual vault after they have been moved from a virtual tape library. Virtual tapes in the vault can be replicated, exported to a physical tape, or moved to a virtual library. There is no limit to the number of tapes that can be in the virtual vault. Virtual tapes in the vault can be sorted by name, barcode, and source server. They can also be filtered to display only specific tapes.

Physical Tape Libraries

This object lists the physical tape libraries that are available to COPAN 400. For each physical tape library, you can assign physical tape drives, inventory the slots, scan tapes, import or move a tape, reset tapes in the slots, mark a library or drive disabled for maintenance purposes, or view performance statistics. For each physical tape, you can export the physical tape, copy the physical tape to a virtual tape, or link the physical tape to a virtual tape for direct access.

Physical Tape Drives

This object lists the standalone physical tape drives that are available to COPAN 400. For each physical tape drive, you can check for a physical tape, import a tape, mark a drive disabled for maintenance purposes, or view performance statistics. For the physical tape, you can eject a physical tape, copy the physical tape to a virtual tape, or link the physical tape to a virtual tape for direct access.

Replica Resources 	This object lists the Replica Resources that are on this COPAN 400 server. Replica Resources store data from local and remotely replicated virtual tapes. Clients do not have access to Replica Resources. You can sort the tapes by tape name, barcode, last replication start time, and source server.
Budget Queue 	This object lists the replication, import and export jobs, tape shredding, and Automated Tape Caching jobs that have been submitted. If necessary, you can cancel, put on hold, resume, restart a failed job, or delete a job from here.
Database 	This object contains configuration information for the COPAN 400. The database can be mirrored for high availability. Refer to 'Mirror the database to protect your COPAN 400 configuration' for more detailed information.

SAN Clients object

SAN clients are the backup servers that use the COPAN 400. COPAN 400 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

COPAN 400 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
- Physical tape usage
- Device usage and configuration

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 storage devices'.

Group Reports object

If you have a multi-node group configured, you will see a *Group Reports* object. This object provides reports that can be generated for all servers in a group. This includes standard reports that are generated on each server in the group and contain data specific to that server. You can also run a consolidated *Group Disk Space Allocation for Virtual Tapes in Libraries Report* that includes every server in the group in one single report.

Understanding the icons in the tree

Virtual tape icons

The following table describes the icons that are used to describe virtual tape drives and virtual tapes in the console:

Icon	Description
	The C icon indicates that this virtual tape drive has compression enabled.
	The A icon indicates that this is a cache for a physical tape. The O icon indicates that this cached tape has unmigrated data. Requires the Automated Tape Caching option.
	The S icon indicates that this is a direct link tape (a link to the physical tape). Requires the Automated Tape Caching option.

Physical resource icons

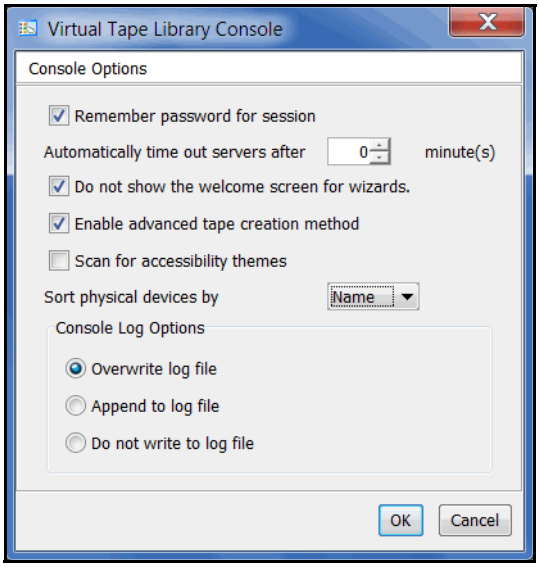
The following table describes the icons that are used to describe physical resources in the console:

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

Console options

To set options for the console:

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



2. Select the options you want to use.

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

   Automatically time out servers after nn minute(s) - The console will collapse a server that has been idle for the number of minutes you specify. If you need to access the server again, you will have to reconnect to it. The default is 10 minutes. Enter 0 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 *Advanced 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.*

   Sort physical devices by - A global setting to sort physical devices by name or SCSI address. While viewing the information in the console, you can click on a column heading to re-sort the information.

   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 console gives you a convenient way to perform system maintenance for your COPAN 400 server.

Notes:

- The system maintenance options are hardware-dependent. Refer to your hardware documentation for specific information.
- Only the root user can access the system maintenance options.

Network configuration

If you need to change COPAN 400 server IP addresses, you must make these changes using *Network Configuration*. Using any other third-party utilities will not update the information correctly.

Notes:

- If you need to change the IP address of a COPAN 400 appliance that has replication configured, you must remove the replication configuration before changing the IP address, and then you can configure replication again.
- You cannot change the network configuration of a VTL server that is in a multi-node group.

Set hostname

Right-click a server and select *System Maintenance* --> *Set Hostname* to change your hostname. The server will automatically reboot when the hostname is changed.

Notes:

- Make sure your storage is connected and accessible before you change the hostname. If it is not and the operation fails, you can change the hostname back to the original, fix your storage, and then try again.
- Do not change the hostname if you are using block devices. If you do, all block devices claimed by COPAN 400 will be marked offline and seen as foreign devices.
- You cannot change the hostname of a VTL server that is in a multi-node group or has failover configured.

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 COPAN 400 server in sync with up to five Internet NTP servers.

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

> **Note:** We recommend restarting the COPAN 400 services if you change the date and time.

Restart COPAN 400

Right-click a server and select *System Maintenance* --> *Restart COPAN 400* 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.

Rescan storage devices

To rescan a device, right-click the storage device and select *Rescan*.

Test physical device throughput

You can test the following for your physical devices:

- Sequential throughput
- Random throughput
- Sequential I/O rate
- Random I/O rate
- Latency

To check the throughput for a device:

1. Right-click the device (under *Physical Resources*).

   To test multiple devices, right-click the *Storage Devices* object.

2. Select *Test* from the menu.

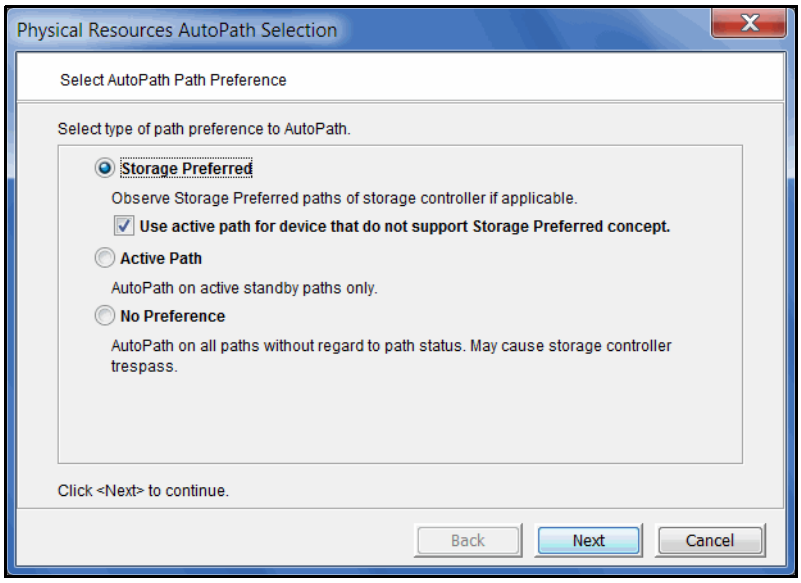
   The system will test each device and then display the throughput results on a new *Throughput* tab. If you tested multiple devices from the *Storage Devices* object, aggregate results will be shown in a dialog and the *Throughput* tab will display results for each device.

Set autopathing

Autopathing gives you the ability to balance I/O to multiple LUNs by setting the first path to use to access each LUN.

To set autopathing:

1. Right-click *Storage Devices* (under *Physical Resources*) and select *Autopath*.
2. Select the autopath method you want to use.



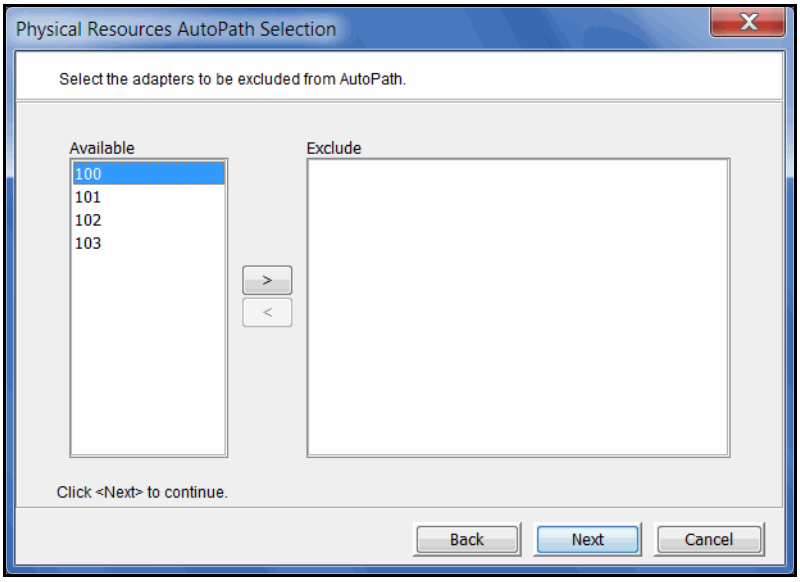
Storage Preferred - (Default) Detects and follows the preferred paths for each LUN as they are set by the storage controller on supported systems and uses them as COPAN 400's preferred paths. If there is no preferred storage path, select the sub-option and COPAN 400 will use the *Active Path*.

Use active path for devices that do not support the Storage Preferred concept - Select this sub-option in case storage controllers do not have storage preferred paths. If you select this sub-option, COPAN 400 will not trigger paths to trespass (switch).

Active Path - COPAN 400 determines the currently active paths and uses them.

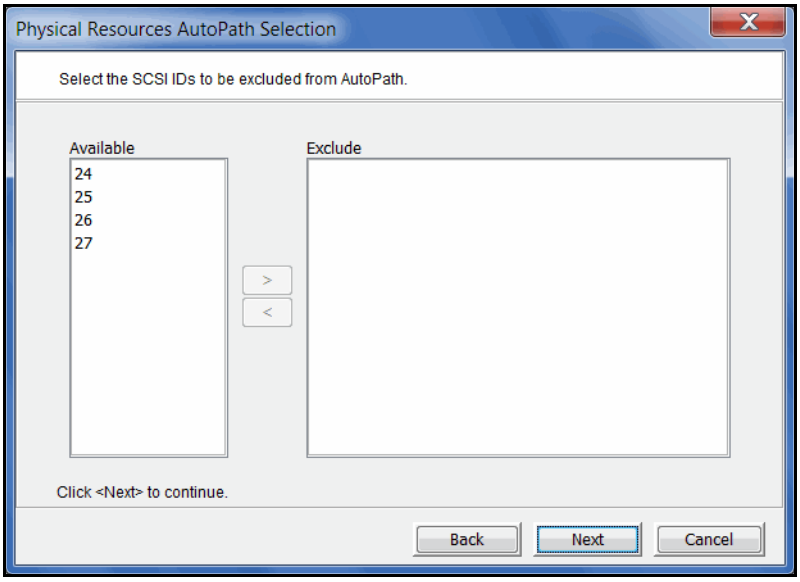
No Preference - Do not use the other methods. COPAN 400 uses all available independent paths. This can cause paths to trespass.

3. Select any adapters that should be excluded.

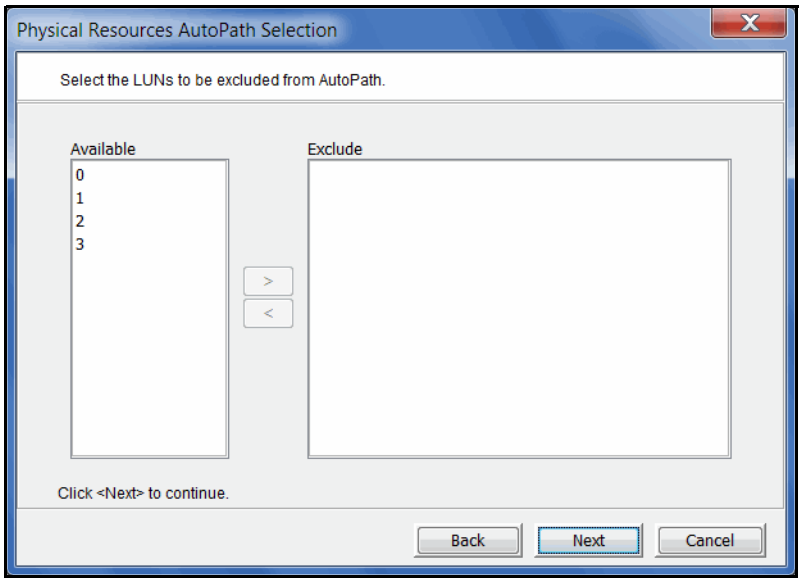


You may need to do this if you have a specific path that you want to maintain. In that case, you would exclude the adapter, SCSI ID, and LUN for that path.

4. Select any SCSI IDs that should be excluded.



5. Select any LUNs that should be excluded.



6. Confirm all information and click *Finish*.

   The path configuration becomes effective immediately, but is not saved permanently. If you are satisfied with the results, you should save them so that they can be reused during startup and rescan and can be restored. To do this, right-click *Storage Devices* (under *Physical Resources*) and select *System Preferred Path --> Save.*

   If you ever need to restore your settings back to the last version that was saved, right-click *Storage Devices* (under *Physical Resources*) and select *System Preferred Path --> Restore*. This is useful if someone manually changes the settings and you want to revert to the saved version.

   Note: Setting autopathing and saving/restoring the system preferred path will impact the I/O path that may be set for devices with multiple paths. Refer to 'Load balance the path for each downstream storage LUN' if you need to reset your settings.

Exclude LUNs from being allocated

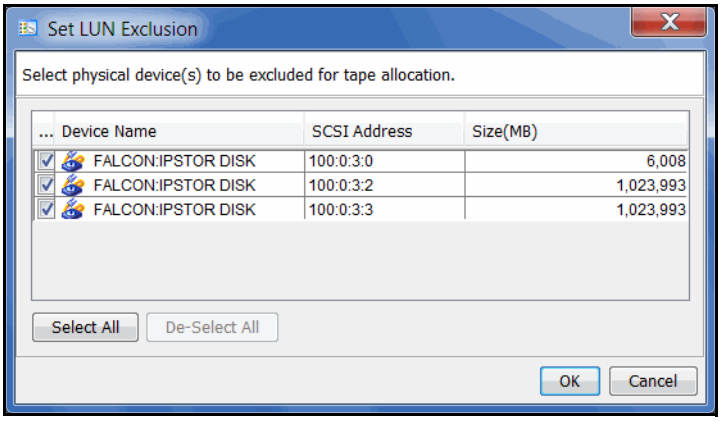
The LUN Exclusion feature allows you to exclude specific physical devices from being used to allocate disk space for virtual tapes. LUN Exclusion is useful if you need to retire an old storage array. LUN Exclusion can be used in conjunction with LUN migration to prevent COPAN 400 from using old LUNs for new backups while moving the existing data from the old LUNs to new LUNs.

LUNs do not need to be virtualized in order to be excluded; unassigned disks can also be excluded.

To exclude LUNs:

1. Right-click *Storage Devices* (under *Physical Resources*) and select *Set LUN Exclusion*.

2. Select one or more physical devices to exclude.

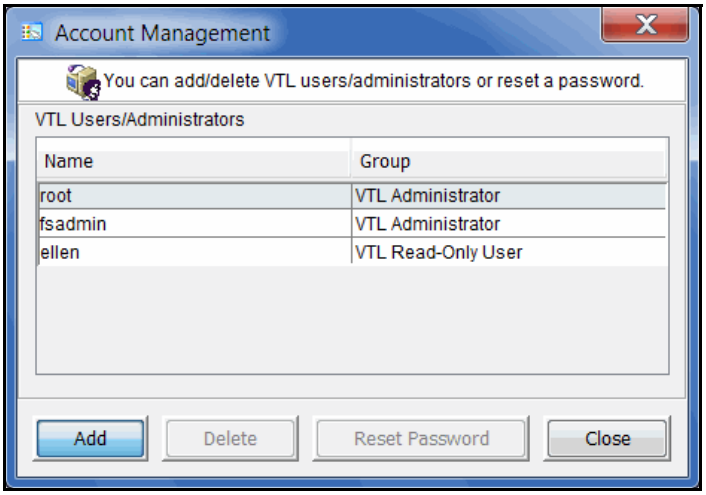


3. Click *OK* when done.

Administrators

Only the root user can add or delete a COPAN 400 administrator or change an administrator's password.

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



There are three types of administrators:

- *COPAN 400 Administrators* are authorized for full console access (except that only the root user can add or delete a COPAN 400 administrator, change an administrator's password, or access the system maintenance options).

- *COPAN 400 Read-Only Users* are only permitted to view information in the console and take x-rays. They are not authorized to make changes and they are not authorized for client authentication.

- *COPAN 400 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.

   When you add an administrator, the name must adhere to the naming convention of the operating system running on your COPAN 400 server. Refer to your operating system's documentation for naming restrictions.

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

Change password

After initial setup, it is recommended that you change the default password.

1. Right-click the COPAN 400 server name and select *Change Password*.
2. Enter the original password (*IPStor101*, on SGI appliances), new password, confirm the new password, then click *OK*.

Event Log

The Event Log details significant occurrences during the operation of the COPAN 400 server. You can view the Event Log in the console when you highlight a server or group in the tree and select the *Event Log* tab in the right pane.

Information displayed in the Event Log comes from the */var/log/messages* file on the COPAN 400 server. A maximum of 10,000 records will be displayed in the Event Log.

The columns displayed in the Event Log 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 COPAN 400 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.
Server	The COPAN 400 server that this message is about. You will only see this column if you are viewing the Event Log at the group level.
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 on a column heading to re-sort the information. For example, if you click on 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.

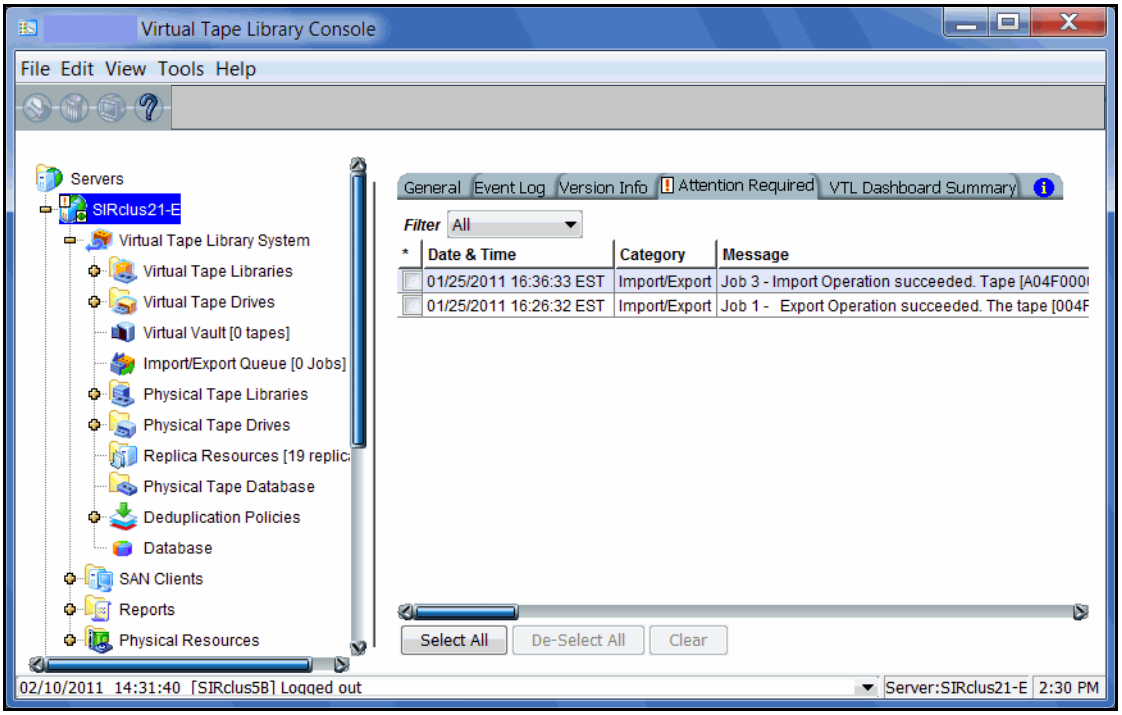
Export data from the Event Log	You can save the data from the Event Log in one of the following formats: comma delimited (.csv) or tab delimited (.txt) text. Click the *Export* button to export information.
Print the Event Log	Click the *Print* button to print the Event Log to a printer.
Clear the Event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

Attention Required tab

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

- Physical library failures
- Hardware appliance errors
- Replication errors
- Import/export job status

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



The *Attention Required* tab only appears for a COPAN 400 server (or at the group level) when an error/notification occurs; it will not appear at other times. When the tab does appear, you will see an exclamation icon on the server. 

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

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

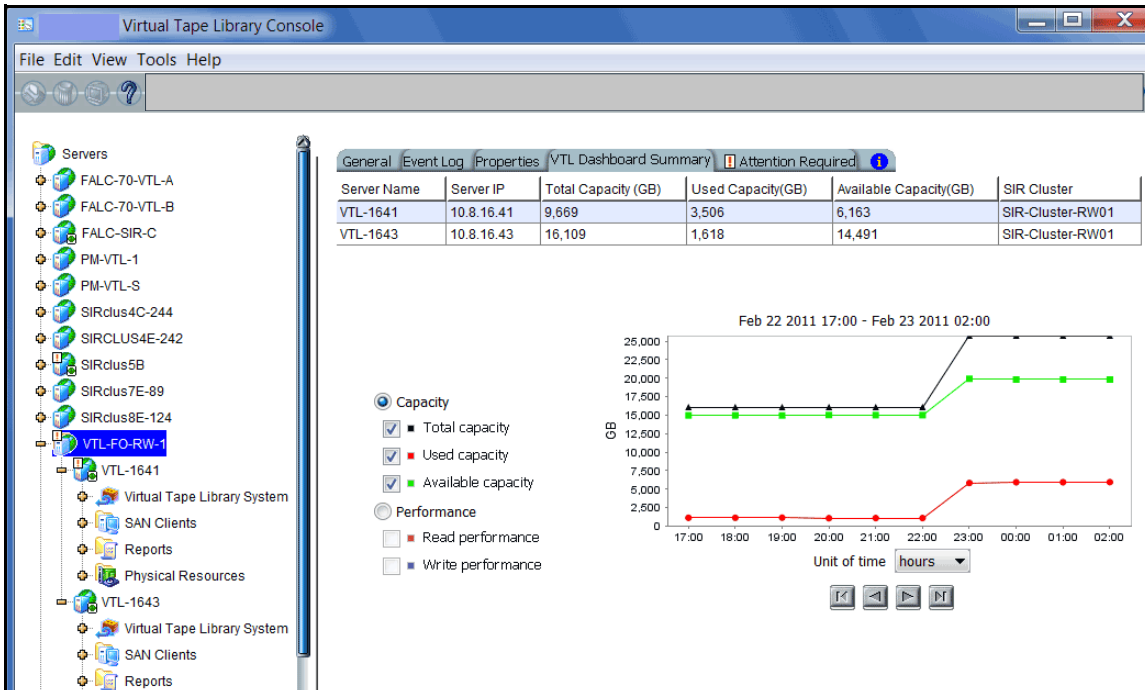
To view only a specific category of events, select the category from the *Filter* drop-down box.

Clear issues from the list

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

COPAN 400 Dashboard Summary

To view statistics for a COPAN 400 server or failover group, highlight the server (or failover group) icon and select the *COPAN 400 Dashboard Summary* tab in the right panel.



The top section displays information about the COPAN 400 server, including capacity information.

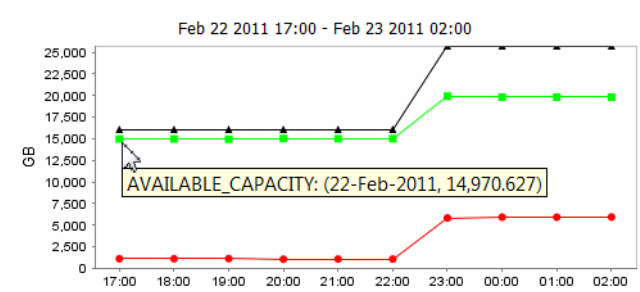
The bottom section allows you to display your choice of capacity and performance statistics for your Fibre Channel clients.

Data on the dashboard is recorded every minute.

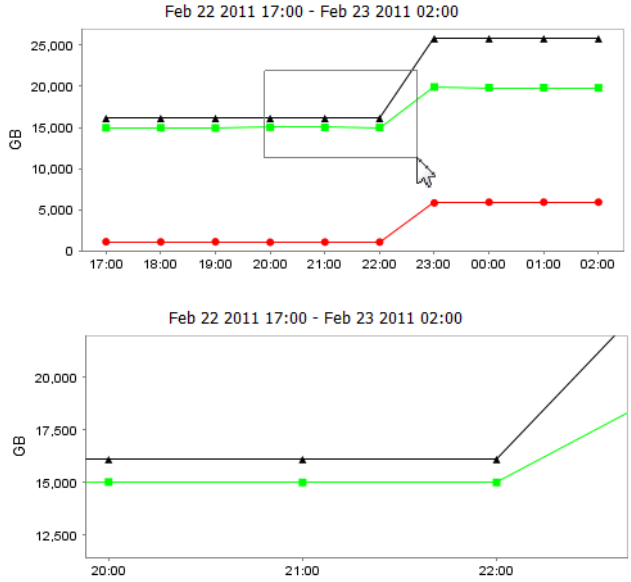
Read and write performance statistics are acquired from all adapters (configured in initiator mode and dual mode) and from local storage. If compression is enabled, the write values will be the compressed values. The statistics include all of the I/O data that is transferred regardless of the activity type.

Select a *Unit of time* (hours, days, weeks, or months) from the drop-down list to adjust the granularity of the graph. The data points in the graph will match the starting point for that unit. For example, if you select *Months*, the data point for March will show statistics for just after midnight on March 1. If you select hours, all data read/written between 7:00-8:00 will be displayed at the 7:00 data point. Use the arrow buttons to scan through accumulated data.

You can put your cursor on a data point to see detailed information.



If you want to zoom into the chart to enlarge it, drag your cursor from left to right over the area you want to expand.



When you are finished, drag your cursor from right to left anywhere in the chart and the display will zoom out, back to a normal view.

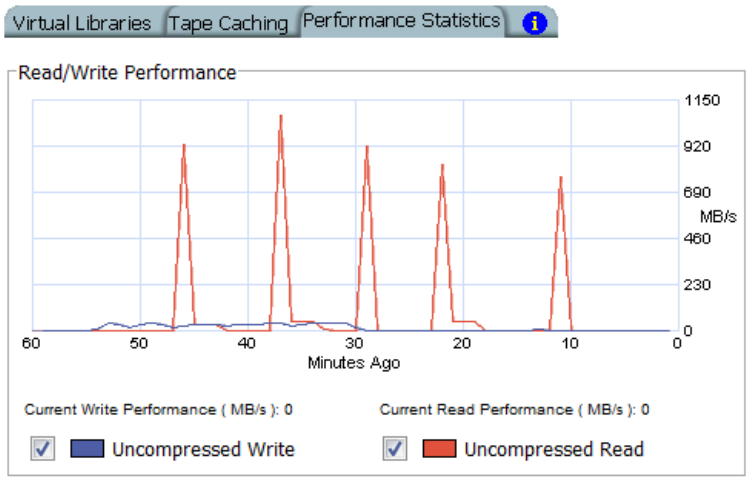
Note: If the server has failed over, you will not see any information in the dashboard summary. Once failback occurs, dashboard summary information will be displayed.

Performance statistics

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

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

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



To hide a read or write performance chart, click the appropriate checkbox.

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 COPAN 400 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 COPAN 400 reports.

3. On the *SNMP Maintenance* tab, indicate the system information that should be available in your SNMP manager and the types of event log messages should be sent as traps to your SNMP manager.

   SysLocation - Enter the location of your system.

   SysContact - Enter contact information. This could be a name or an email address.

   Trap Level - By default, event log messages are *not* sent, but you may want to configure COPAN 400 to send certain types of messages. Five levels of messages are available:

   - None – (Default) 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.

   Once you have selected a trap level, the bottom of the dialog will display a table where you can click *Add* to enter your SNMP server, community name, and the SNMP trap version used by your SNMP manager.

4. On the *Performance* tab, indicate if you want to enable replication throttling and then enter the maximum number of KBs per second that should be used for replication.

   You can limit the amount of available network bandwidth that is used for replication on the source server side. Transmission will not exceed the set value. This is a global server parameter and affects all resources.

   Once enabled, the default is 10 KBs per second. If throttling is not used, replication will use the maximum bandwidth that is available. Besides 0, valid input is 10-1,000,000 KB/s (1G).

5. On the *Storage Monitoring* tab, enter the maximum percentage of storage that can be used by COPAN 400 before you should be alerted.

   When the utilization percentage is reached, a warning message will be sent to the Event Log. If you have an SNMP manager, the current status can be monitored from there.

6. 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 COPAN 400 server and console.

With this information, you can apply maintenance patches to your COPAN 400 server through the console.

Note: Server upgrade patches must be applied directly on the server and cannot be applied or rolled back via the console.

Apply patch

To apply a patch:

1. Download the patch onto the computer where the console is installed or a location accessible from that machine.

   Patches can be downloaded from the SGI customer support portal.

2. Highlight a server in the tree.
3. Select *Tools* menu --> *Add Patch.*
4. Confirm that you want to continue.

   If this server is part of a failover configuration, you must suspend failover before continuing.

5. Locate the patch file and click *Open*.

   The patch will be copied to the server and installed.

6. Check the Event Log to confirm that the patch installed successfully.

Roll back patch

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

1. Highlight a server in the tree.
2. Select *Tools* menu --> *Rollback Patch.*
3. Confirm that you want to continue.

   If this server is part of a failover configuration, you must suspend failover before continuing.

4. Select the patch and click *OK*.
5. Check the Event Log to confirm that the patch uninstalled successfully.

Mirror the database to protect your COPAN 400 configuration

You can mirror the database in order to protect your COPAN 400 configuration. Even if you lose your COPAN 400 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 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, COPAN 400 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 COPAN 400 database. The mirror can be defined with disks that are not necessarily identical to each other in terms of vendor, type, or even interface (SCSI, FC, iSCSI).

To set mirroring:

1. Prepare a physical device to use for the mirror.

   Note: If you are adding a mirror in an active production environment, you should add this LUN to the LUN exclusion list before continuing, in order to prevent it from being allocated for other purposes during the mirror configuration process. Refer to 'Exclude LUNs from being allocated' for details.

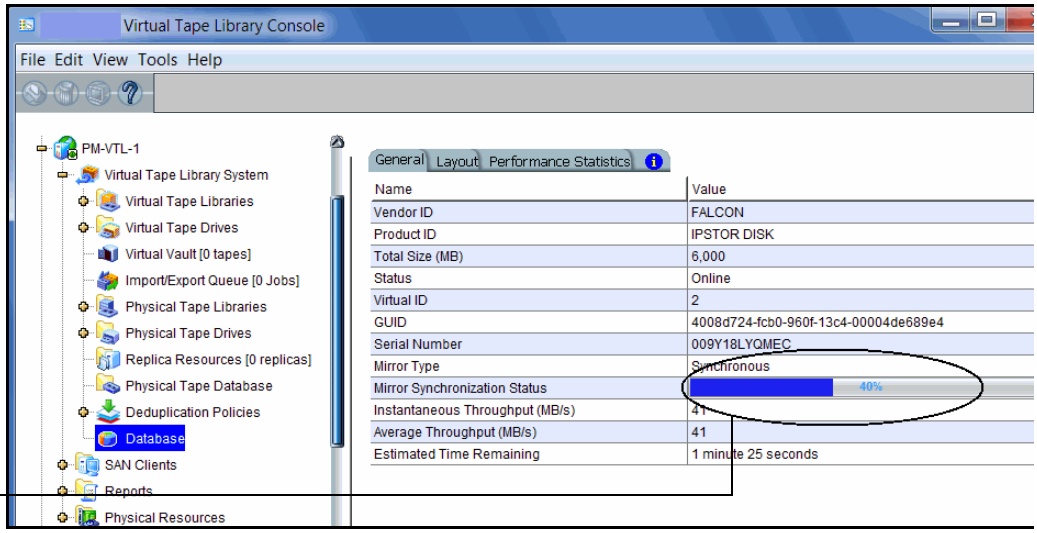
2. Right-click the *Database* object (under the *Virtual Tape Library System* object) and select *Mirror --> Add*.

3. Select which physical device to use for the mirror.

4. 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.



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, COPAN 400 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, COPAN 400 swaps the primary with the mirrored copy.

   Important: To replace the disk without having to reboot your COPAN 400 server, refer to ‘Replace a failed physical disk without rebooting your COPAN 400 server’.

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.

   Important: To replace the disk without having to reboot your COPAN 400 server, refer to 'Replace a failed physical disk without rebooting your COPAN 400 server'.
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.

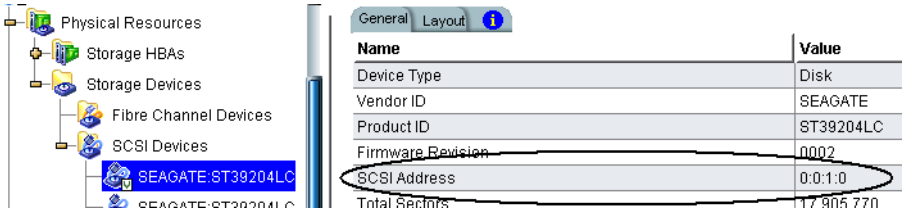
Replace a failed physical disk without rebooting your COPAN 400 server

Do the following if you need to replace a failed physical disk without rebooting your COPAN 400 server.

1. If you are not sure which physical disk to remove, execute the following to access the drive and cause the disk's light to blink:

   ```
   ipstorhdparm x x x x
   ```

where x x x x stands for A C S L numbers: Adapter, Channel, SCSI, and LUN number, which you can find in the console.



2. You MUST remove the SCSI device from the Linux operating system by executing:

   ```
   echo "scsi remove-single-device x x x x">/proc/scsi/scsi
   ```

   where x x x x stands for A C S L numbers: Adapter, Channel, SCSI, and LUN number.

3. Execute the following to re-add the device so that Linux can recognize the drive:

   ```
   echo "scsi add-single-device x x x x">/proc/scsi/scsi
   ```

   where x x x x stands for A C S L numbers: Adapter, Channel, SCSI, and LUN number.

4. Rescan the adapter to which the device has been added.

   In the console, right-click *AdaptecSCSI Adapter.x* and select *Rescan*, where *x* is the adapter number the device is on.

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.

Mirroring and Failover

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

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

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

Manually save/restore a COPAN 400 configuration

COPAN 400 includes a utility (*vtlrecover*) that enables you to protect your COPAN 400 configuration and recover your COPAN 400 system in case of the following:

- The Linux boot disk of the appliance is lost or corrupted.
- The file system where the COPAN 400 software is installed is lost.

Information and requirements

- In order to use this utility, all appliance hardware, including FC HBAs and network adapters, storage, physical libraries/drives, and connectivity must be intact and functioning properly.
- The utility does not back up or restore COPAN 400 patches. Patches need to be saved and restored prior to running the restore process.
- The utility does not restore your database mirroring configuration. If you had database mirroring configured before recovery, you will need to reconfigure it after recovery.
- The budget queue and scheduled reporting will not be saved and cannot be restored.

After restoring your configuration

- If you deleted any tapes after saving your configuration, those tapes will show up with a red dot (incomplete) after restoring the configuration.
- If you created any tapes after saving your configuration, those tapes will go to the vault.
- If you reclaimed any direct link tapes after saving your configuration, those tapes will show up with red dots.
- After the restore is completed, any expansions or shrinking done after saving your configuration will be adjusted after the restore is completed as part of the normal tape consistency checking done at COPAN 400 startup.

Save your configuration

Note: You should run this utility after you make any major configuration changes.

Use the following procedure to save configuration information:

1. Run the following command: $ISHOME/bin/vtlrecover save archive.tar

   This generates an output file which includes all configuration information needed for recovery.

2. If the system is a failover configuration, repeat the first step on each node.

   This must be done when the failover system is in a normal mode of operation (i.e., both nodes are functioning correctly).

3. Copy the output file(s) to a safe remote location outside the COPAN 400 appliance.

   The file(s) will be needed to restore the configuration.

Restore a configuration - standalone system

Use the following procedure to restore the configuration on a standalone (non-failover) system.

1. If the Linux operating system is lost, reinstall Linux using an approved procedure.

   For an SGI appliance, use the SGI installation procedure to install the operating system.

2. Configure the hostname, network IP addresses, and other network settings as before.

   Note: The hostname MUST match that of the server that was previously saved.

3. Install COPAN 400 software using the recommended installation procedure.

   Be sure to apply the same level of patches as the previous system had.

4. Copy the saved configuration file from the remote location to $ISHOME/bin.

5. Run the following command: $ISHOME/bin/vtlrecover restore archive.tar.bz2

   NOTE: Depending on how many tapes are present in the COPAN 400 system, it may take up to 10 minutes to restore the system.

6. Connect from the console and verify that all configuration information has been restored.

   All virtual tapes, including direct link tapes, will be automatically moved to the appropriate libraries.

Restore a configuration - failover environment

There are two scenarios for restoring a configuration in a failover environment:

- Takeover was successful - Follow the instructions below to restore your configuration.
- Takeover was not successful because the failed server's configuration and database were corrupted - Contact Technical Support for help restoring the configuration.

Takeover was successful

Use the following procedure to restore the COPAN 400 configuration on a failed server when the surviving server has taken over successfully.

1. If the Linux operating system is lost, reinstall Linux using an approved procedure.

   For an SGI appliance, use the SGI installation procedure to install the operating system.

2. Configure the hostname, network IP addresses, and other network settings as before.

   Note: The hostname MUST match that of the server that was previously saved.

3. Install COPAN 400 software using the recommended installation procedure.

   Be sure to apply the same level of patches as the previous system had.

4. Copy the saved configuration file from the remote location to $ISHOME/bin.

5. Run the following command: $ISHOME/bin/vtlrecover restore archive.tar.bz2

   NOTE: Depending on how many tapes are present in the COPAN 400 system, it may take up to 10 minutes to restore the system.

6. In the console, right-click the secondary server, select *Failover --> Stop takeover* to perform a failback.

7. Connect from the console and verify that all configuration information has been restored.

   All virtual tapes, including direct link tapes, will be automatically moved to the appropriate libraries.

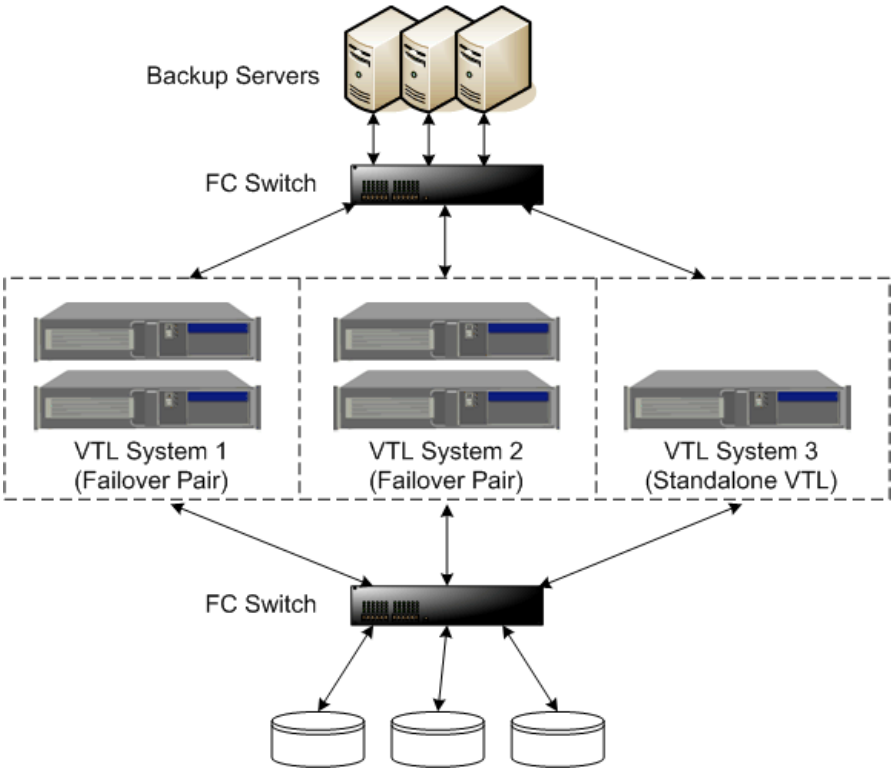
Multi-Node Groups

If you have multiple COPAN 400 servers, you can create multi-node groups in the console, allowing all COPAN 400 servers in the group to be managed together.

Each multi-node group can contain up to eight servers and can include a combination of single servers and/or failover pairs (but failover must be configured before adding them to a group).

A multi-node group can be built by simply connecting all nodes through switches.

The following diagram shows how a multi-node group can be built containing failover pairs and standalone servers.



All of the servers in a group can be managed together. The following management functions are available at the group level:

- Single sign-on - Log in to all of the servers in the group at the same time with a single user name and password that exists for all servers in the groups.
- Create/delete groups
- Add/remove members

- Consolidated reporting - Reports can be generated for all servers in a group. This includes standard reports that are generated on each server in the group and contain data specific to that server. You can also run a consolidated *Group Disk Space Allocation for Virtual Tapes in Libraries Report* that includes every server in the group in one single report.
- Consolidated Event log/Attention required monitoring - The Event log displays events from all servers in chronological order.
- Common configuration settings - Including hardware/software compression, SNMP, storage monitoring triggers, tape caching thresholds, and X-ray creation.
- Consolidated user management - Users can be added/deleted at the group level

Note that if any server in a group is offline, you will not be able to change global properties. In such cases, you will need to remove the offline server from the group before any global properties can be changed.

Create a group

To create a group:

1. Right-click the *Servers* object and select *Create Group*.

   You can also right-click a server and select *Join Multi-Node Group*. If the group name you enter does not already exist, a new group will be created for that server.

2. Enter a name for the group.

   You can enter letters, numbers, a dash, or underscore. Spaces and other characters are not allowed.

Add servers to a group

Notes:

- Each server can only be part of one multi-node group.
- You do not need to connect to a server before adding it to a group.
- If you want to add failover servers to a group, failover must be configured first.
- In order to join a group, the new server should have the same user name and password as the servers that are already in group because this is not changed when the server is added to a group.
- Common configuration settings, including hardware/software compression, reporting configuration, SNMP, storage monitoring triggers, and tape caching thresholds, are not automatically applied to servers that are added to the group. If the servers are not all configured the same way, you must manually update each one after adding it to the group.

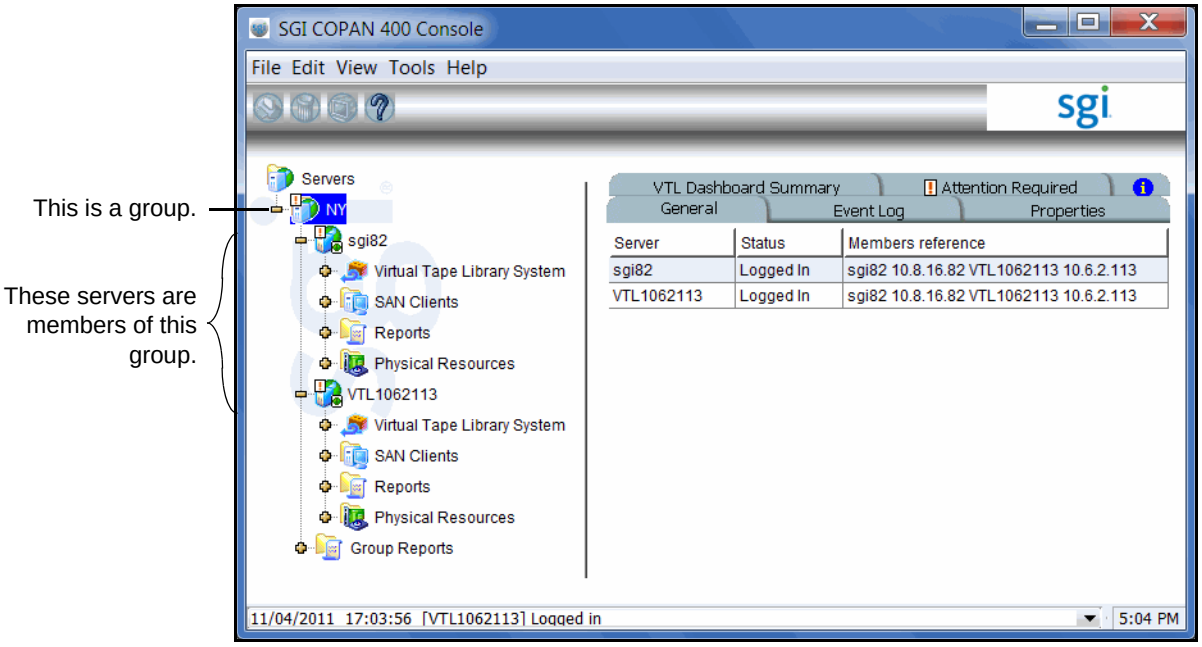
To add a server, you can do either of the following:

- If you are already connected to a server, right-click the server and select *Join Multi-Node Group*. You will then need to type the group name *exactly* as it appears (names are case sensitive).

- If you are not connected to a server, right-click a group and select *Add Member.* You will then need to enter an IP address and a valid user name and password. When you add subsequent servers, you will only have to enter the IP address. The system will use the user name and password from the first server that you added.

When you are done, all of the servers in a group will be listed in alphabetical order beneath the group in the console. Failover pairs will be displayed together, one below the other.

Your console will now look similar to the following:



Remove a server from a group

Both online and offline servers can be removed.

Notes:

- If you delete the only server in a group, the group itself will be deleted.
- When a server leaves a group, all administrator accounts that were added at the group level remain with the server.

To remove a server from a group:

1. Right-click the server you want to remove and select *Leave Multi-Node Group*.
2. Answer *Yes* to confirm.

Tape Libraries, Tape Drives, and Tapes

Create virtual tape libraries

You can create virtual tape libraries that emulate your physical tape libraries.

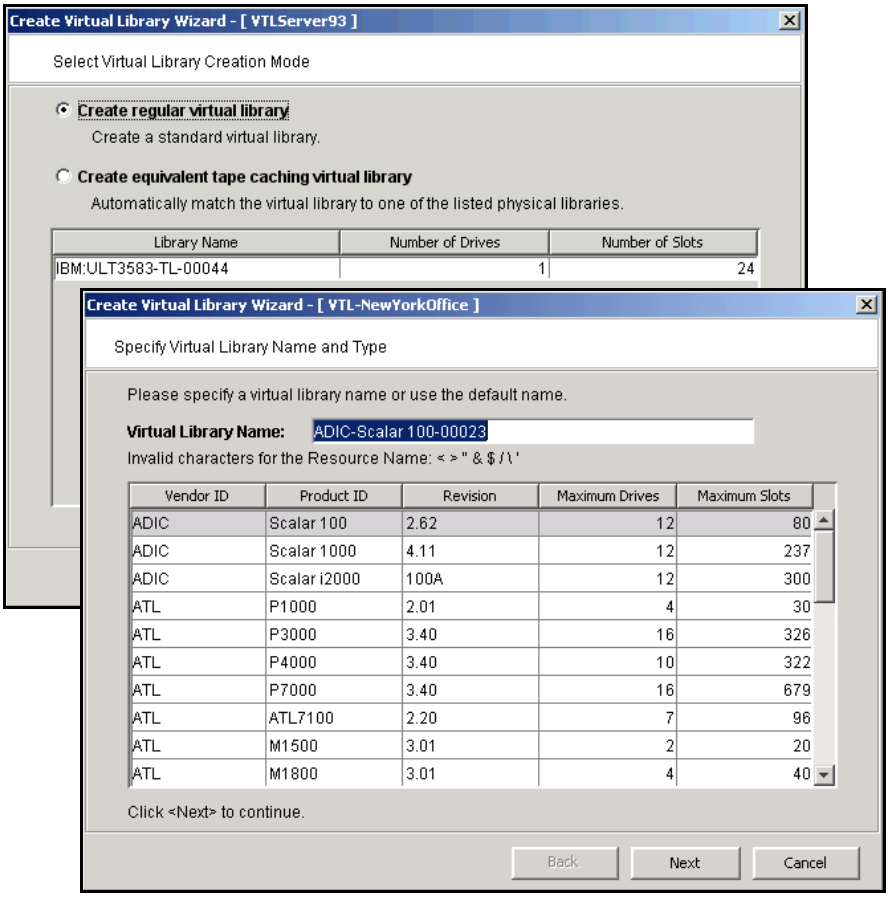
There are two ways to create a virtual tape library:

- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on 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 COPAN 400 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*.

1. Select the physical tape library that you are emulating.

This is the dialog you will see if you have already assigned a physical tape library to your COPAN 400.



This is the dialog you will see if you are not using a physical tape library (or have not yet assigned it to your COPAN 400).

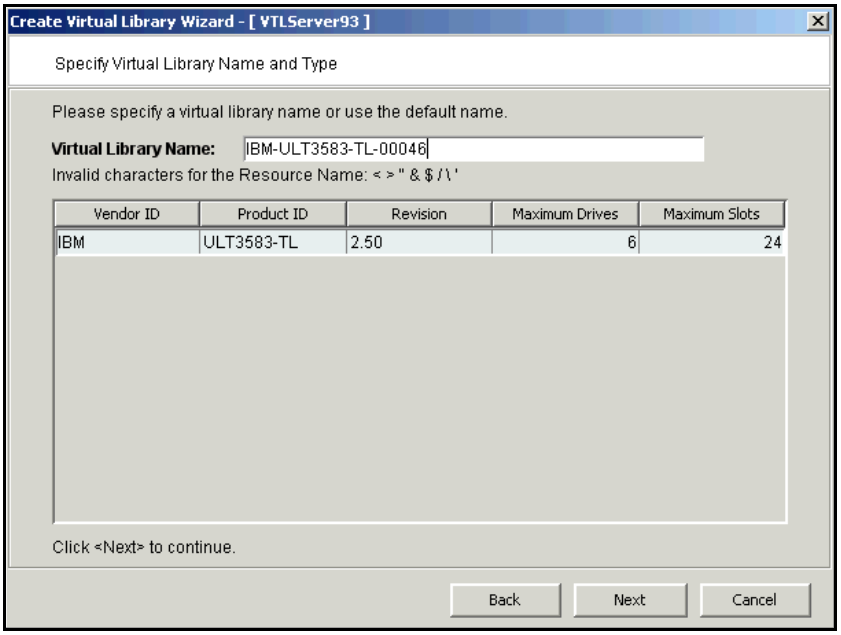
If you have a physical tape library, you need to create a virtual tape library that resembles it in order for the virtual tapes to use the same format as the physical tapes. This is important for importing and exporting functions and guarantees that your backup application will accept the tapes.

Note: For IBM iSeries clients, you must select the IBM 3590E11, IBM 3583, or the IBM 3584 tape library.

Creating an equivalent tape caching library will use *Automated Tape Caching*, which enhances functionality by acting as a cache to your physical tape library, providing transparent access to data regardless of its location. If you choose this option, you will only see your available (not already configured) physical tape libraries listed. Select the check box and the system will automatically match your virtual library to the physical library.

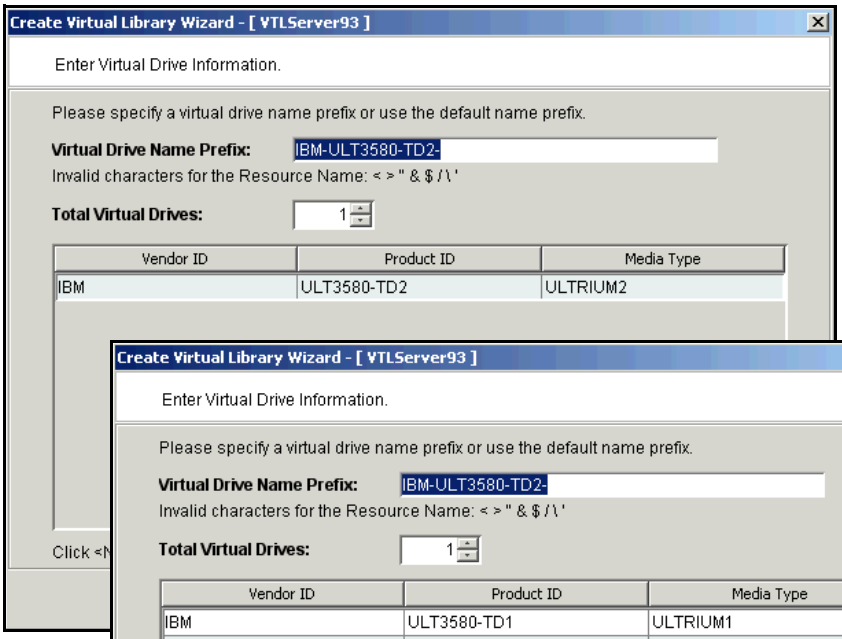
Note: The automatic matching of virtual libraries to physical libraries is not available for ACSLS-managed libraries.

2. (Equivalent tape caching library only) Specify a name for the virtual library.

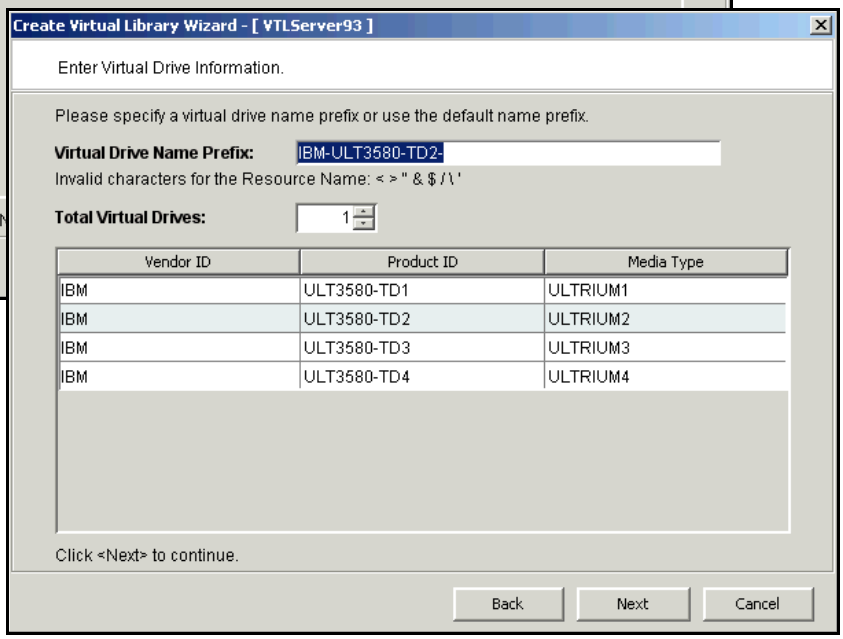


3. Enter information about the tape drives in your library.

This is an example of what you will see if you are creating an equivalent tape caching library.



This is an example of what you will see see if you are creating a standard tape library.



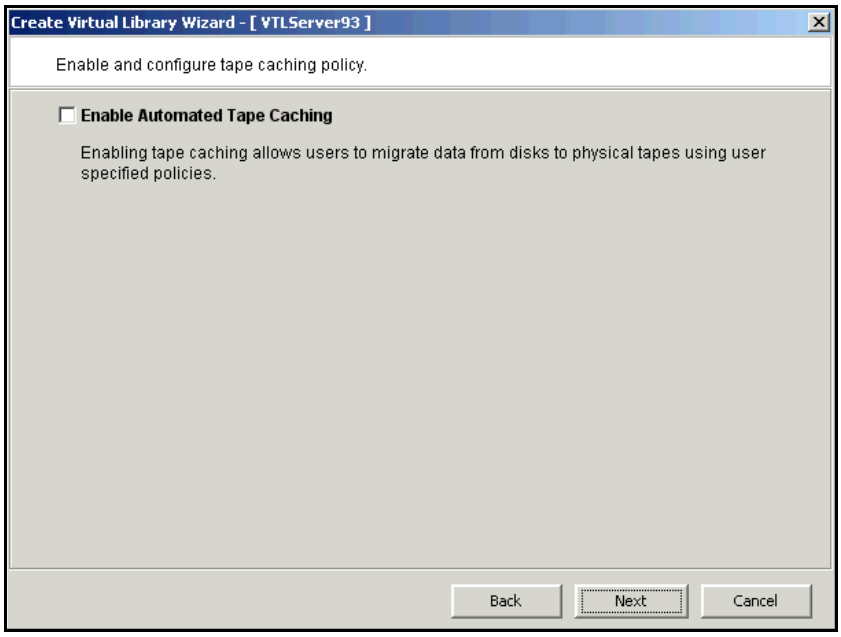
If you are creating an equivalent tape caching library, the appropriate drives are selected for you.

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.

Note: After creating this virtual tape library, if you need to add drives to it, right-click your library and select *New Drive(s)*.

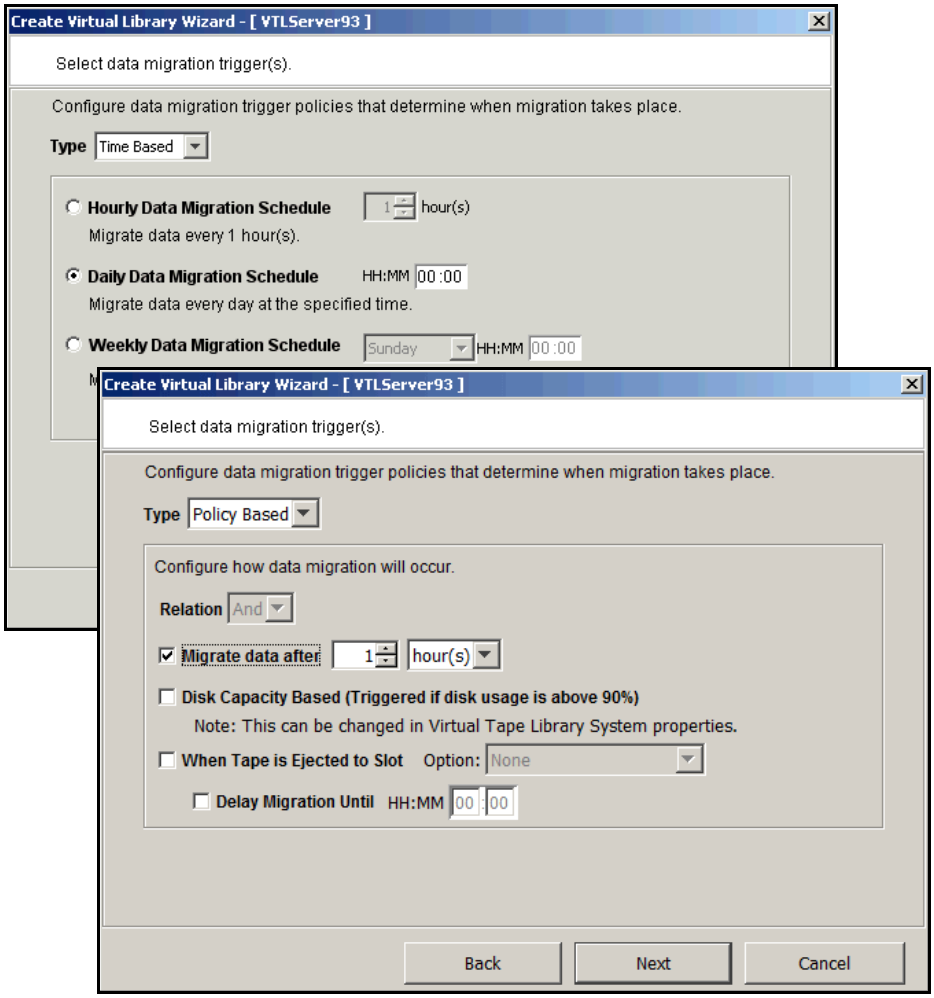
4. If this virtual library was not automatically matched to a physical library, indicate if you want to use Automated Tape Caching for this library.



Selecting this option here means that the virtual library will act as a cache to your physical tape library, providing transparent access to data regardless of its location.

However, selecting this option here will *not* automatically match this virtual library to a physical library. This means that you do not have to maintain a 1:1 mapping between virtual and physical tape drives.

5. (Automated Tape Caching only) Specify your migration triggers.

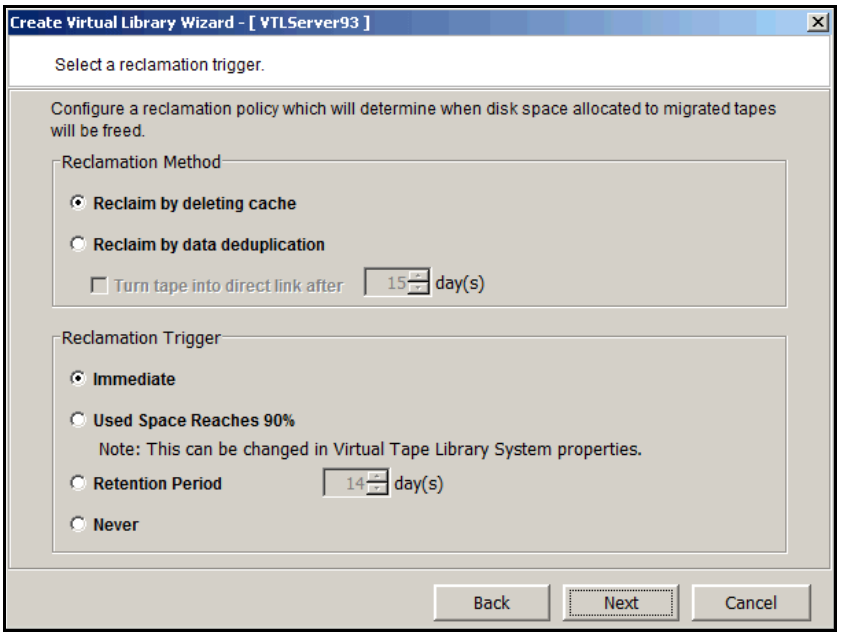


Select *Time Based* or *Policy Based* to toggle between the two types of triggers.

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

For detailed information about these settings, refer to 'Automated Tape Caching'.

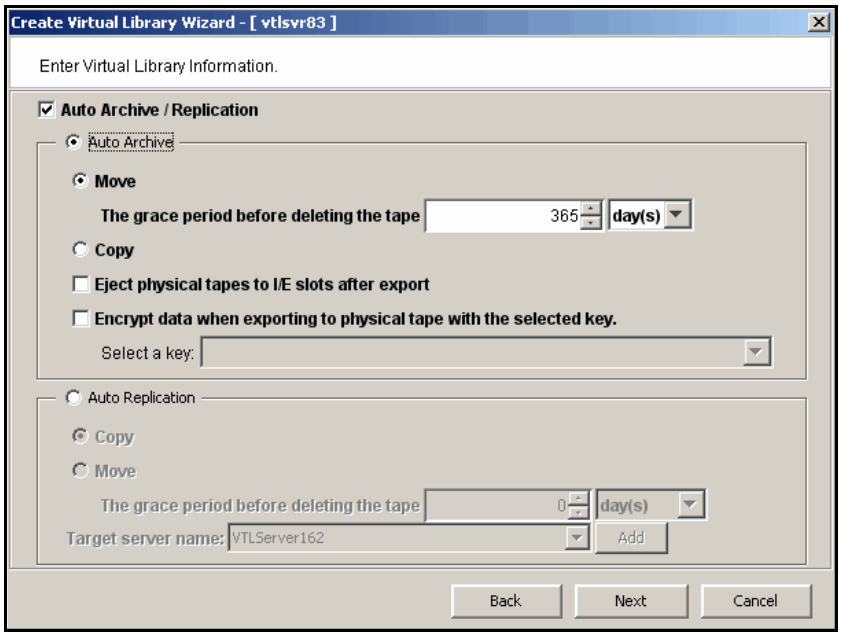
6. (Automated Tape Caching only) Specify reclamation triggers.



Reclamation triggers control when the data that has been migrated to physical tape can be deleted to free up cache disk space.

For detailed information about these settings, refer to 'Automated Tape Caching'.

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



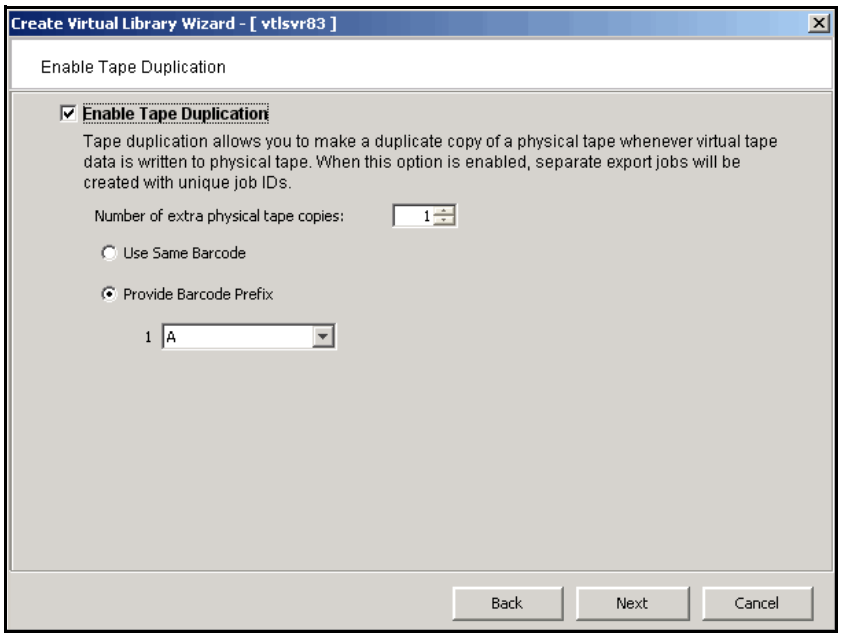
You can select either *Auto Archive* or *Auto Replication* for a virtual library, but not both.

Auto Archive writes data to physical tape whenever a virtual tape is moved to an Import/Export (IE) slot from a virtual library by a backup application or other utility after a backup. (You will see the tape in the virtual vault.) In order for the *Auto Archive* function to work, the physical tape library must support barcodes because when COPAN 400 attempts to export to a physical tape, it must find a matching barcode in a physical library (you do not need to specify which physical library).

- Determine if you want the virtual tape copied (retained) or moved (removed) after the data is transferred. If you select *Move*, indicate how long to wait before deleting it.
- Indicate if you want to eject your *physical* tapes to the library's import/export slots after exporting.
- You can encrypt the data while exporting as long as you have created at least one key.

Auto Replication replicates data to another COPAN 400 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 COPAN 400 server.

8. If you have at least two physical tape libraries (same model, same number of drives, same tapes with the same barcodes) connected to your system, indicate if you want to enable Tape Duplication for this library.



Tape duplication allows you to make up to five duplicate copies of a physical tape whenever virtual tape data is exported to physical tape. The number of physical libraries controls the number of duplicate copies; you need six physical libraries to make five duplicates.

You can select whether the physical tape will have the same barcode as the virtual tape or will use a specific prefix that replaces the first character of the barcode. For example, if your virtual tape barcode is “123456” and you specify that the prefix is “A”, the system will look for a physical tape with the barcode “A23456”.

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

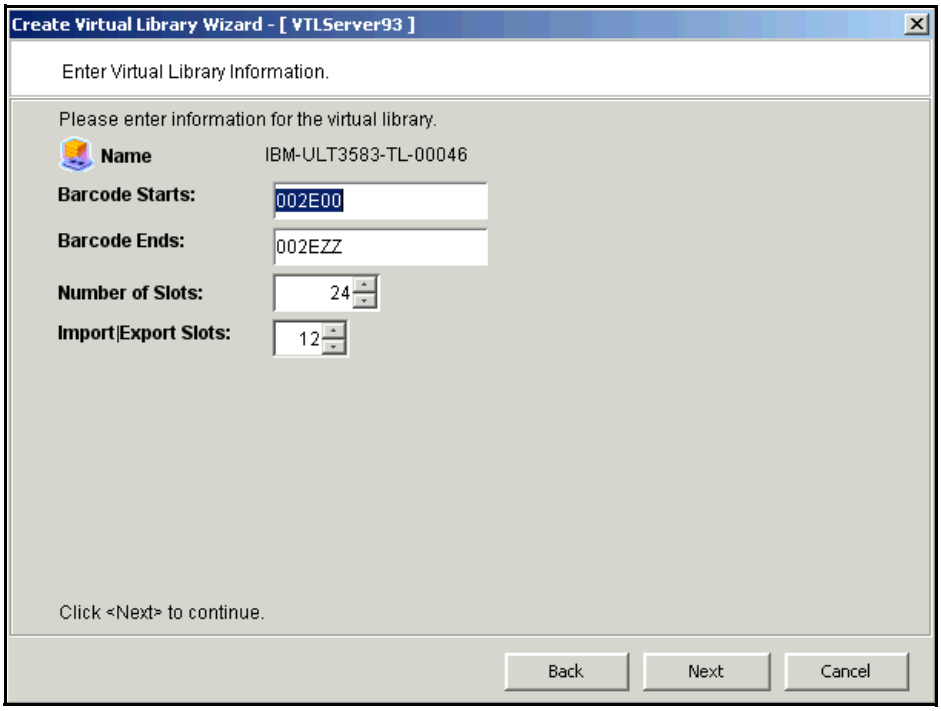
When data is exported, separate export jobs will be created for each physical library and each job will have a unique job ID. Multiple duplication jobs will run concurrently.

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

Notes:

- You should not have duplicate physical tape barcodes in your system *unless* you are using tape duplication.
- Once you configure Tape Duplication, you should not unassign any of the physical libraries from COPAN 400.

9. Enter barcode information for the virtual library.



Barcode Starts/Ends - Indicate a range of barcodes that will be used when creating virtual tapes. By default, barcodes increment in an alphanumeric sequence; for example, **XXX0009** to **XXX000A**. In order to set the barcode to

increment in a numeric sequence (**XXX0009** to **XXX0010**), you have to set the last three digits of the *Barcode Ends* field to **999**; for example, **XXX0999**

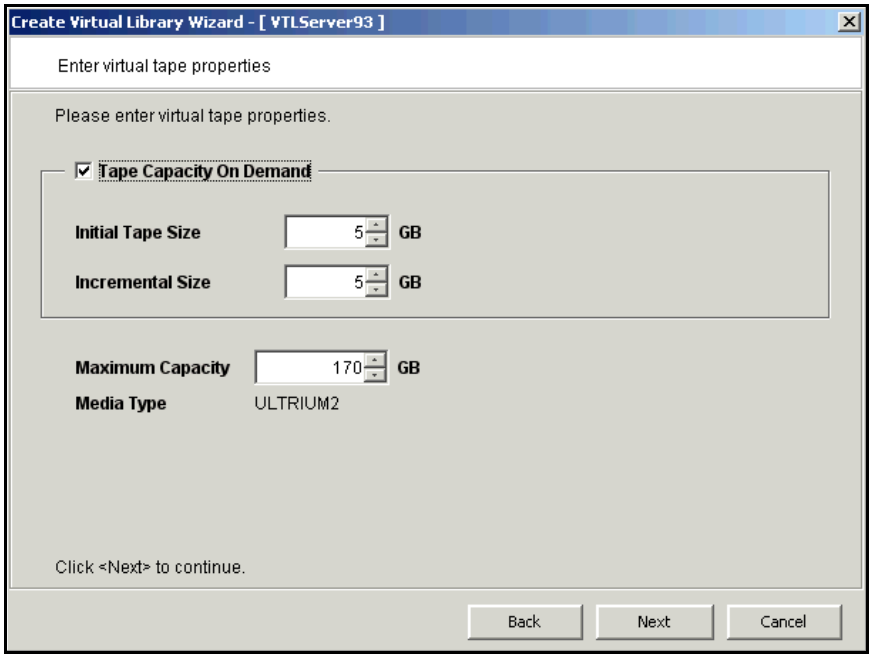
Note that for IBM libraries, the default barcode range is set to six characters.

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

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

Note: If you are using an HP EML E-Series library with LTO drives with IBM® Tivoli® Storage Manager, you need to change the default library barcode to six digits.

10. Enter the guidelines for expanding virtual tape capacity.



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, COPAN 400 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 and the tape is reset to its initial size. 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.

- If you will *not* be exporting data to physical tape, you can enter any maximum capacity.
- If you *will* be exporting data to physical tape but you will not be using COPAN 400's hardware or software compression, you can enter any maximum capacity, but if you enter a capacity that exceeds the native uncompressed capacity for the media, you may not be able to export to physical tape.
- If this virtual library will use tape caching, you should not resize the virtual tapes because migration will fail when the amount of data exceeds the size of the physical tape.
- If you *will* be exporting data to physical tape *and you will* be using COPAN 400's hardware or software compression, you should set the maximum capacity to 15% less than the uncompressed capacity of the selected media. (A 15% reduction is the default value). This is because COPAN 400's compression algorithm can vary depending upon the dataset; certain file types (ZIP, PDF, GIF, RAR, etc.) are already compressed and cannot be compressed further.

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

    If you are not using Automated Tape Caching, you will be prompted to create virtual tapes. Answer *Yes* to continue. Refer to the following section for more information about creating virtual tapes.

    If you are using Automated Tape Caching, you will be prompted to synchronize your virtual library to your physical library. Refer to 'Create a cache for your physical tapes' for more information.

Create virtual tapes

You can create virtual tapes in the following ways:

- After you create a virtual tape library, you will be prompted to create tapes for it.
- Use the configuration wizard - If you have already configured your system, you can launch the wizard by right-clicking on the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard.* Skip to Step 2, which lets you create a virtual library and tapes for that library.
- Right-click a virtual tape library or the *Tapes* object and select *New Tape(s)*.

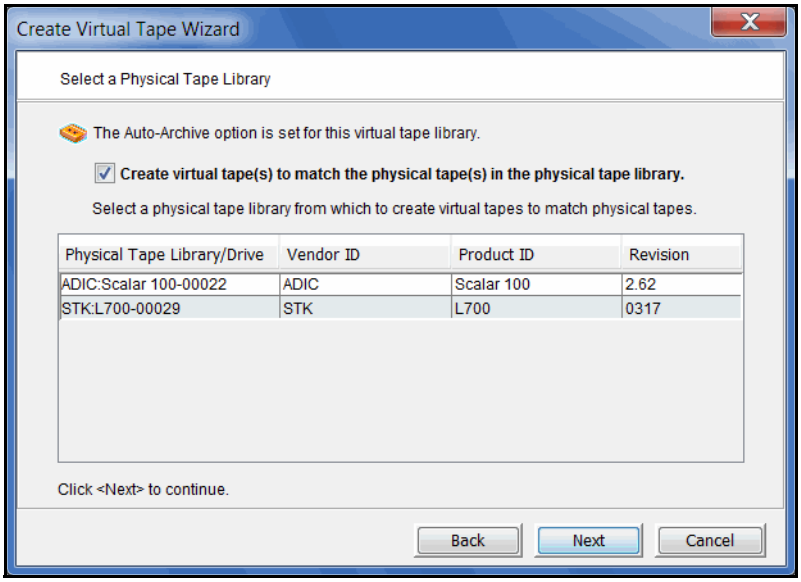
The *Create Virtual Tape wizard* will vary depending on whether or not you have enabled the *Advanced Tape Creation* method (set in *Tools --> Console Options).*

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.

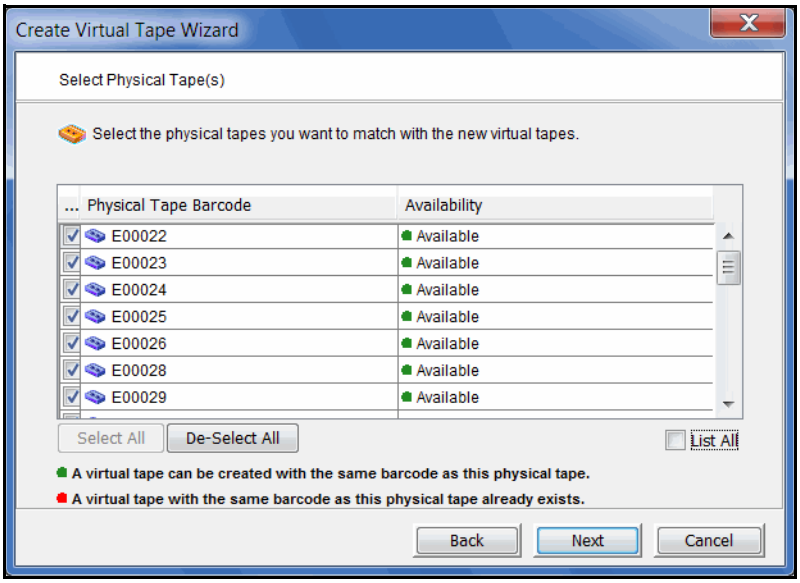
2. If *Auto Archive* is enabled for the virtual library, select the physical tape library you want to match with virtual tapes.



   This enables you to have a physical tape with a barcode that matches your virtual tape. This is important for exporting functions.

   If you selected the *Auto Archive* option but have not yet connected a physical tape library to the COPAN 400 appliance, you can either create virtual tapes without setting a matching barcode or discontinue creating virtual tapes at this time and exit the dialog.

3. If *Auto Archive* is enabled for the virtual library and you are matching physical tapes, select the physical tapes for which you want to create matching virtual tapes.

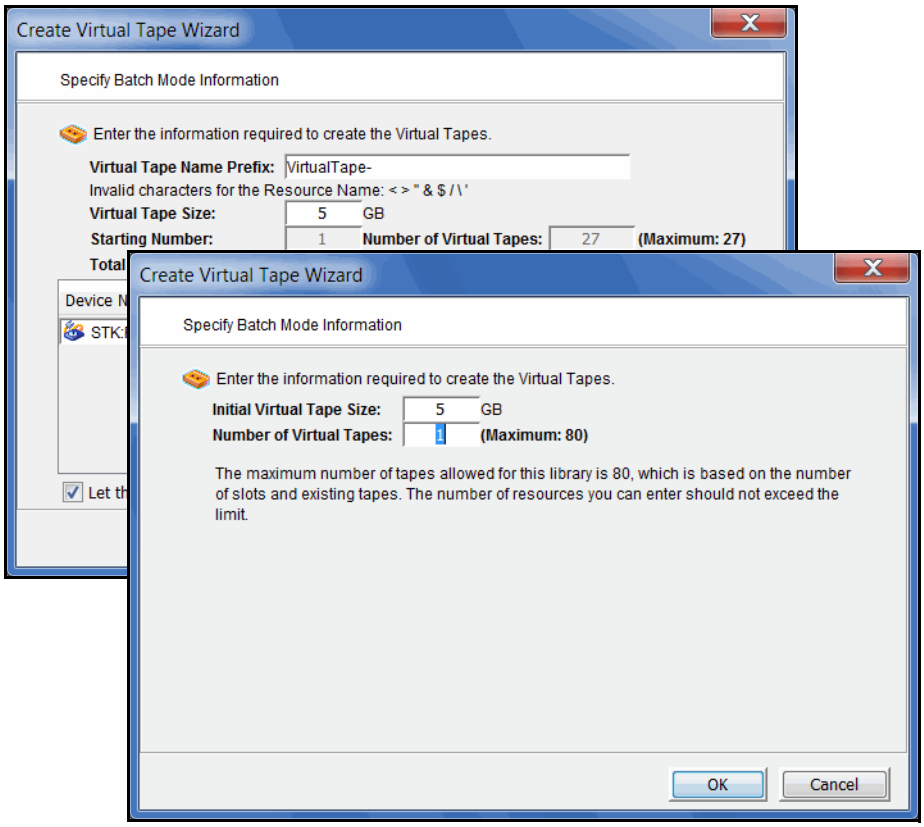


4. (*Advanced Tape Creation* only) If you selected the *Custom* creation method, specify which physical device should be used to create the virtual tapes.

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

5. Depending upon which method you selected, specify the tape prefix, tape size, and, if applicable, the number of tapes to create.

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



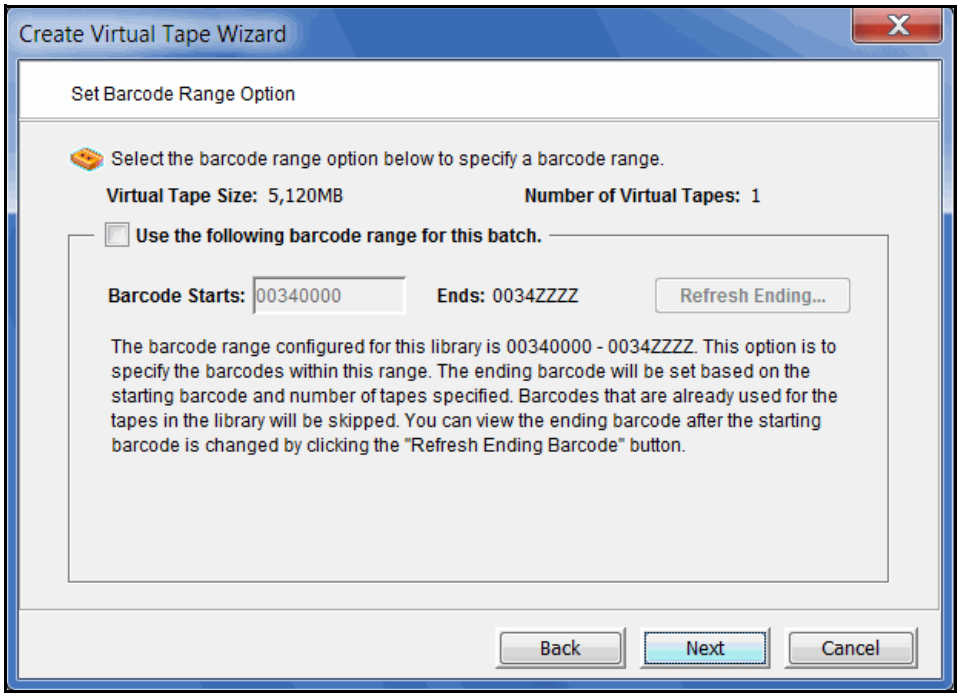
You will see this dialog if the *Advanced Tape Creation* method is not enabled.

6. 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.

7. (*Advanced Tape Creation* only) If you are not matching physical tapes, you can set a barcode range for the virtual tapes you are creating.



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

How virtual tapes are allocated

COPAN 400 uses a sophisticated methodology to determine which LUN to use when allocating space for virtual tapes.

Using two algorithms, *Dynamic LUN Allocation* and *Round Robin*, virtual tapes being expanded or created in *Express* mode are allocated from the LUN that is currently experiencing the least amount of I/O. (Virtual tapes created in *Custom* mode use the LUN that is specified.)

When virtual space is needed, the system looks at the available LUNs. A scoring method is used to determine how *busy* each LUN is. If the scores for all LUNs are equal (i.e. all LUNs are *free* or all are equally busy), Round Robin logic is used to select the next available LUN in the rotation queue.

Once a LUN is selected, COPAN 400 looks to see if there is enough continuous space available on the LUN to match what is needed. If there is enough, that space is allocated. Afterward, the LUN is pushed to the “back” of the queue, ensuring that tapes are evenly distributed across all LUNs.

If there is not enough continuous space on a single LUN, COPAN 400 allocates the biggest chunk of continuous space available. Smaller chunks on the same LUN are then allocated (but never chunks less than 1 GB) to reach the total amount needed. If there is not enough space available, COPAN 400 continues allocating from another LUN.

When Tape Capacity on Demand is used and tape expansion is needed, COPAN 400 will attempt to expand the tape on the current LUN, provided there is enough space available. Once that LUN is filled, Round Robin logic will select the next LUN to allocate space from.

By default, a single allocation pool is used for all available storage. All available LUNs are assigned to this pool. For enhanced performance, multiple allocation pools can be defined to further distribute I/O between multiple controllers and RAID units. Because configuration is different for every environment, contact SGI Professional Services if you would like to configure multiple allocation pools for LUN allocation.

Locate and display virtual tapes in the Console

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

Search by barcode

To search by barcode for a specific virtual tape:

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

3. Enter the full barcode.

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

Display virtual tapes

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

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

For single tapes, the right-click menu allows you to create a remote copy; rename the tape; delete the tape; move the tape to the virtual vault, slot, or drive; configure replication, and display/set tape properties (barcode, tape capacity on demand, write protection, auto archive, auto replication, and tape duplication).

For multiple selected tapes, the right-click menu allows you to delete the tapes, move them to the virtual vault, and configure replication.

To load tapes into all empty virtual tape drives or to dismount tapes from all virtual tape drives, right-click the virtual tape library object in the tree and select *Auto Load Tapes* or *Auto Unload Tapes*.

Sort all tapes

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

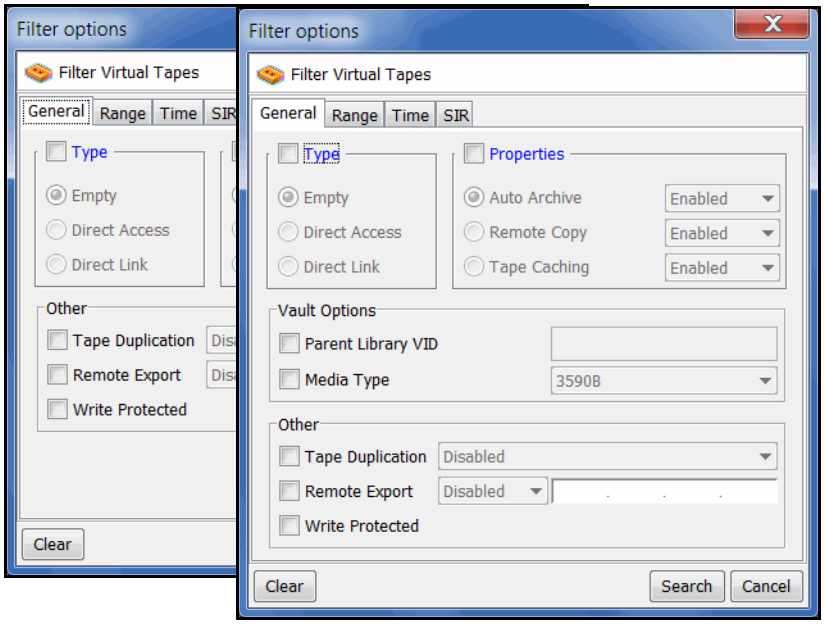
1. Select the appropriate heading in the drop-down box next to *Sort*.
2. Indicate whether they should be sorted in *Ascending* or *Descending* order.

Filter the display of tapes

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

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

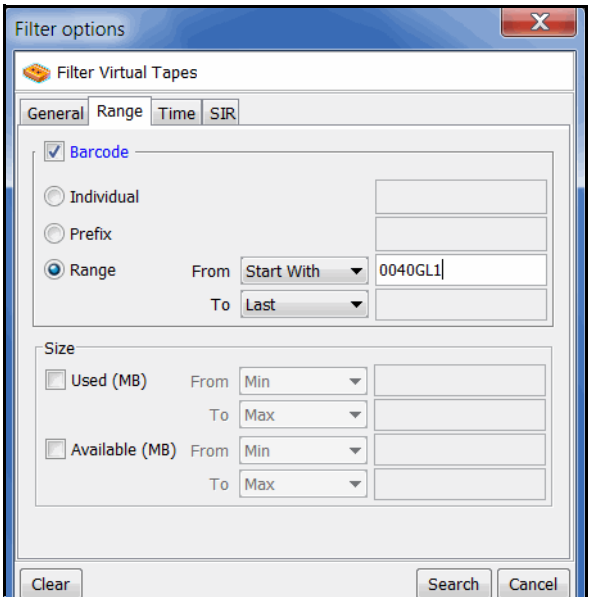
You will see this dialog if you started from the *Tapes* object.



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

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

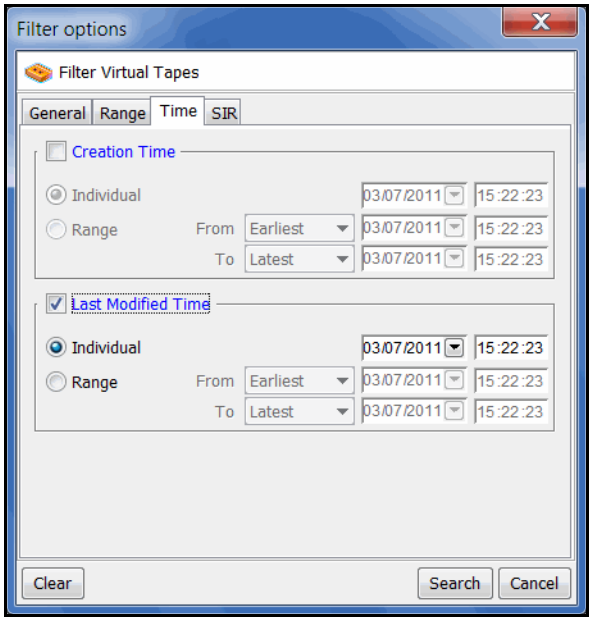
3. On the *Range* tab, you can enter a range of barcodes and/or sizes.



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

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

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



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

5. 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.

Assign virtual tape libraries and drives to backup servers

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

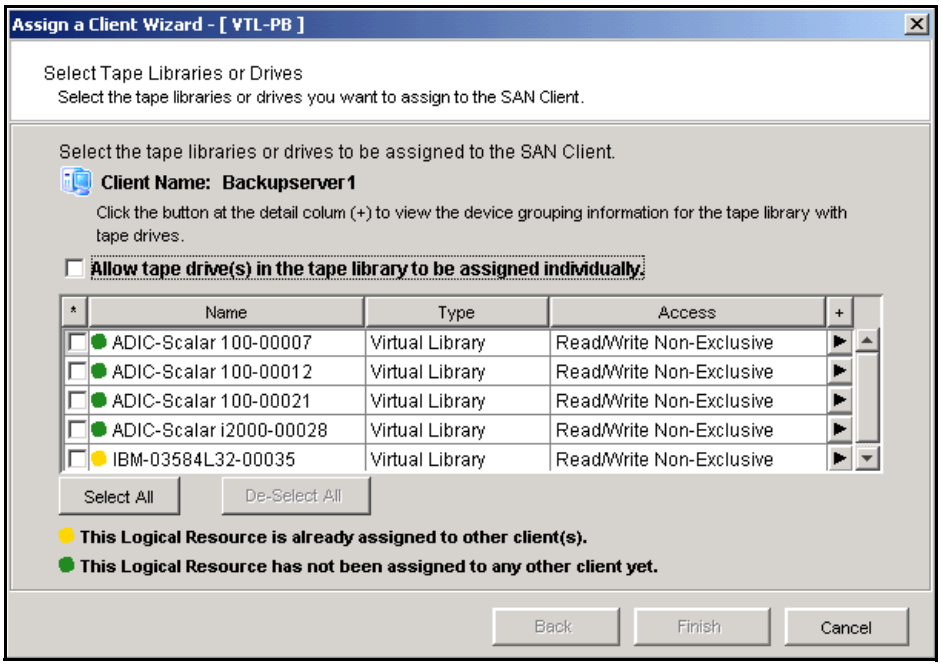
There are three ways to assign a library or drive to a client (backup server):

- Use the configuration wizard - If your system is already configured, you can launch the wizard by right-clicking on 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.
- Begin with a client object and select a virtual tape library.
- Begin with a virtual tape library and select the backup server to assign it to.

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 or drive.



   All tape drives in a 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 COPAN 400 server and backup server will treat each individually assigned drive as if it were a standalone tape drive.

2. Click *Finish* when you are done.

3. Use the backup server's operating system to discover the COPAN 400 server.

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

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

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

4. Use your backup software to discover the library.

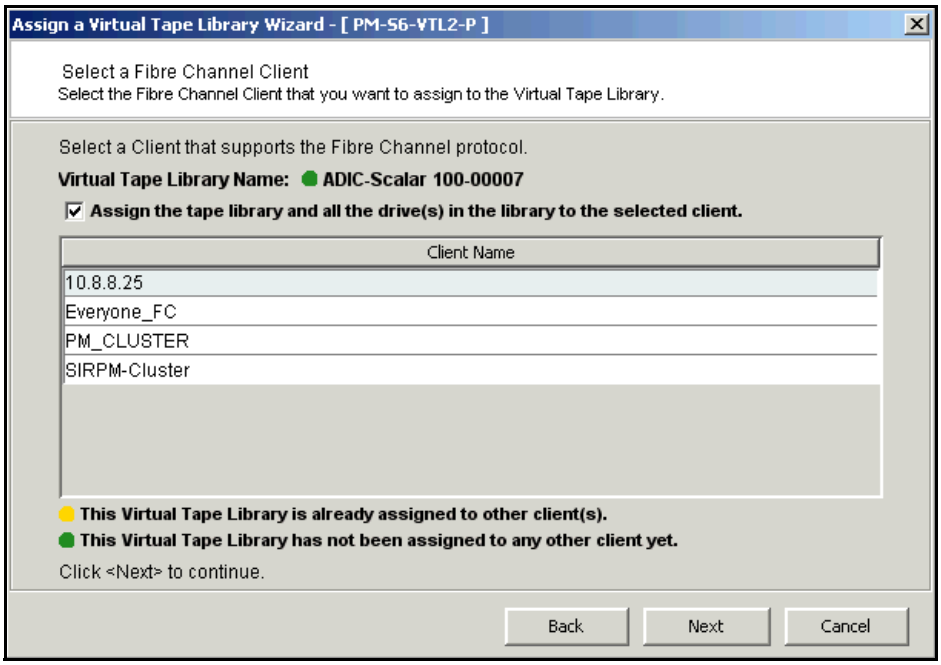
   The steps to do this vary according to your backup software.

Virtual tape library

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

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

2. Select a backup server.



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

Physical tape libraries

You can import data from physical tapes into your virtual tape library or export data from virtual tapes to physical tapes. Before you can perform these operations, do the following:

1. Connect the physical tape library to the COPAN 400 system.

   This can be done using Fibre Channel zoning or, if the appliance has a SCSI card, using a direct SCSI connection.

2. Restart Revolution services in order to discover the newly-assigned physical tape library.

   You can now identify these new devices in the navigation tree. Expand the *Physical Resources* object and then the *Fibre Channel Devices* or *SCSI Devices* object (depending on the connection).

   On the *General* tab of the console information pane, a physical library has a Device Type of *Medium Changer* and a physical drive has a Device Type of *Tape Device*. New devices have a Category value of *Unassigned*.

3. Assign the physical library/drives to the virtual tape library (refer to 'Assign physical libraries/drives to COPAN 400').

4. For export purposes, create virtual tapes that correspond to barcoded physical tapes (refer to 'Create virtual tapes').

Assign physical libraries/drives to COPAN 400

If you will be importing data from physical tapes into your virtual tape library or exporting virtual tapes to physical tapes, you must assign your physical tape libraries/drives to COPAN 400. This process also inventories the physical tapes in your library/drive so that you can create virtual tapes that match your physical tapes.

Notes:

- A physical tape library can only be assigned to one COPAN 400 server at a time, unless the ACSLS option is being used.
- COPAN 400 does not support physical libraries when tape drive numbering does not start with 0 or is not sequential.

1. Assign physical libraries/drives to COPAN 400 in one of the following two ways:
   - Use the configuration wizard - You can launch the wizard by right-clicking on the *Virtual Tape Library System* object in the console and selecting *Configuration Wizard.* If you haven't already prepared your physical library/drive, you can do that as well.
   - Right-click the *Physical Tape Libraries* object or the *Physical Tape Drives* object and select *Assign*.
2. Select the physical libraries/drives to be assigned to COPAN 400.

3. Click *Finish/Assign* to assign.

Inventory physical tapes

You can perform an inventory of the physical tapes in a physical tape library. This allows you to create virtual tapes that match your physical tapes. To do this, right-click a physical tape library and select *Inventory*.

Designate a physical library or drive as disabled

For maintenance purposes, a physical library or drive can be marked as disabled. While it is designated as disabled, the library/drive cannot be used for any import/export functions. To do this, right-click a physical tape library or drive and select *Disable*. Afterwards, when the library/drive is available, you can enable it.

Reset physical tapes in a library

Resetting a physical library reinitializes the library and puts tapes back in the appropriate slots. This function is useful after a problem (such as a physical tape stuck in a slot) is resolved. To reset a library, right-click a physical tape library and select *Reset.*

Import data from tapes

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

You can also import data from virtual tapes being used by another SGI virtual tape library.

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

Import data from a physical tape

The import function allows you to:

- Copy the contents of a physical tape to a virtual tape
- Directly access a physical tape without copying the entire tape
- Recycle a physical tape
- Import data from virtual tapes used by another SGI virtual tape library

Before you import a tape

You must verify the following before you can import tapes:

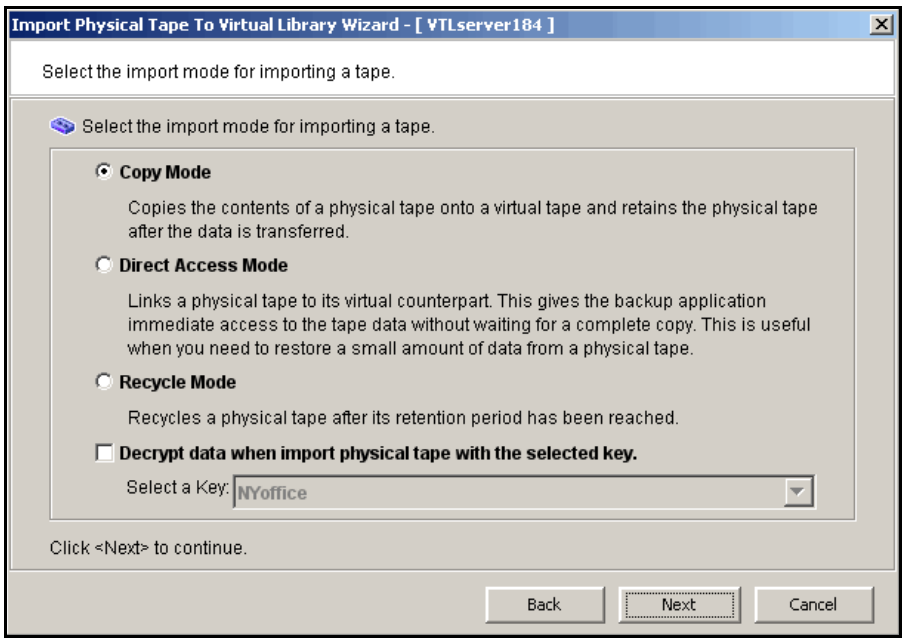
- The drive type (i.e. IBM:ULTRIUM-TD3) and the media type (i.e. Ultrium3) of the library you are importing from must match the library to which you are importing.
- If you are connecting through a switch, the COPAN 400 server must be in the same zone as the physical tape library or other COPAN 400 server from which you are importing.

Import a tape

1. Right-click your physical tape library/drive and select *Import Tape*.
2. Select which virtual library to import into.

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

3. Select how you want the data copied.



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

Direct Access Mode - Links a physical tape to its virtual counterpart. This gives the backup application immediate access to the tape data without waiting for a complete copy. This is useful when you need to restore a small amount of data from a physical tape. Direct access tapes are write protected. Therefore, you can only read from the tape and not write to it.

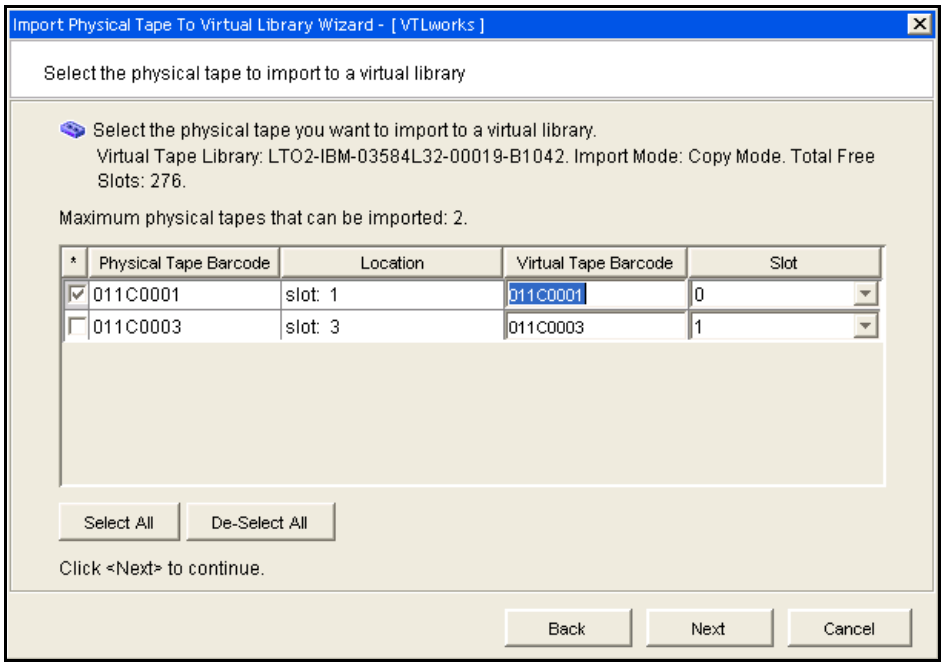
Recycle Mode - Recycles a physical tape after its retention period has been reached. If you import a tape in recycle mode and the virtual tape is subsequently initialized, the physical tape is now considered recycled and can be used for future export operations.

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

   You can select this option only if at least one key exists. (For more information, refer to 'Encrypt data on virtual and physical tapes'.) If you select this option, you must select the key to use.

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

5. Select the physical tape you want to import.



You can select a tape based on its barcode or slot location. You can then use the same barcode for the virtual tape or you can enter a new barcode. You can also select a slot for the virtual tape.

You can import whichever tapes you need; you are not required to import all tapes in a library.

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

   You can check the Budget queue to watch the progress of the job.

   When import is completed, the virtual tape is automatically moved to the virtual vault.

Import data from a tape in another virtual tape library

In order to import data from a virtual tape in another SGI virtual tape library, the two COPAN 400 servers must be connected or zoned together so that they can communicate with each other. To import data:

1. On the source COPAN 400 server (where your original tape is located), create a SAN client to represent the target COPAN 400 server (the server to which the tape will be imported).

2. On the COPAN 400 server to which you are importing tapes, highlight *Physical Resources --> Storage HBAs* and select *Rescan*.

   Select the *Discover New Devices* option.

3. After re-scanning, verify that the tape library and drives you are importing from appear under *Storage Devices*.

4. Right-click the *Physical Tape Libraries* object under *Virtual Tape Library System* and select *Assign*.

5. Select the physical tape library and click *Assign*.

6. Select all tape drives that belong to the physical tape library created previously and click *Assign*.

7. Right-click the physical tape library and select *Import Tape*.

8. Select the virtual library to which you want to import the tape.

9. Select *Copy Mode* to copy the data.

10. Select the tape(s) you want to import.

    You can select a tape based on its barcode or slot location. You can use the same barcode for the virtual tape or you can enter a new barcode. A free destination slot in the virtual library has been automatically assigned to store the virtual tape. You can choose another empty destination slot manually by clicking on the down arrow button.

11. Verify the information and then click *Finish* to import the tape(s).

    You can view status by highlighting the job in the *Budget Queue*. You will see a *Percent Complete* progress bar in the right-hand frame.

    When completed, the virtual tape will be automatically moved to the virtual tape library.

Export data to physical tape

You can export data from a virtual tape to a physical tape in a physical tape library. This process is useful for offsite data archiving.

With COPAN 400's built-in incremental export functionality for automatic export, only the modified data is exported and appended to physical tape, if the same tape was exported previously.

On the other hand, if a tape has been reformatted or rewritten, the export job will overwrite the physical tape with all of the information on the virtual tape. If a different tape is exported to that same physical tape, the data will be overwritten on the physical tape.

Notes:

- You cannot use the COPAN 400 export function if you are using the Automated Tape Caching option.
- Because some third-party backup applications alter what they write to the tape depending on the type of cartridge used, COPAN 400 only exports tapes to *like* media. You cannot export to a dissimilar physical tape. This guarantees that the backup application will accept the tape as valid; from the backup application's point of view, there is no difference between the virtual and physical tape.

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

- From your backup software using the software's own *Tape Copy* function
- Using COPAN 400's *Export* function, either manually or automatically after each backup using the *Auto Archive* function

As an alternative to exporting data to a physical tape, the COPAN 400 Automated Tape Caching option provides a cache to your physical tape library, providing transparent access to data regardless of its location. The Automated Tape Caching option provides advanced flexibility that allows you to set up policies that automatically trigger data migration to physical tapes.

The COPAN 400 export methods are explained below. Refer to 'Automated Tape Caching' for more information about Automated Tape Caching.

Export manually

Manual exporting data from a virtual tape builds a full physical tape. Incremental export functionality does not apply to manual export.

To manually export data:

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

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

General | Layout | Statistics | Physical Drives | Physical Tapes

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

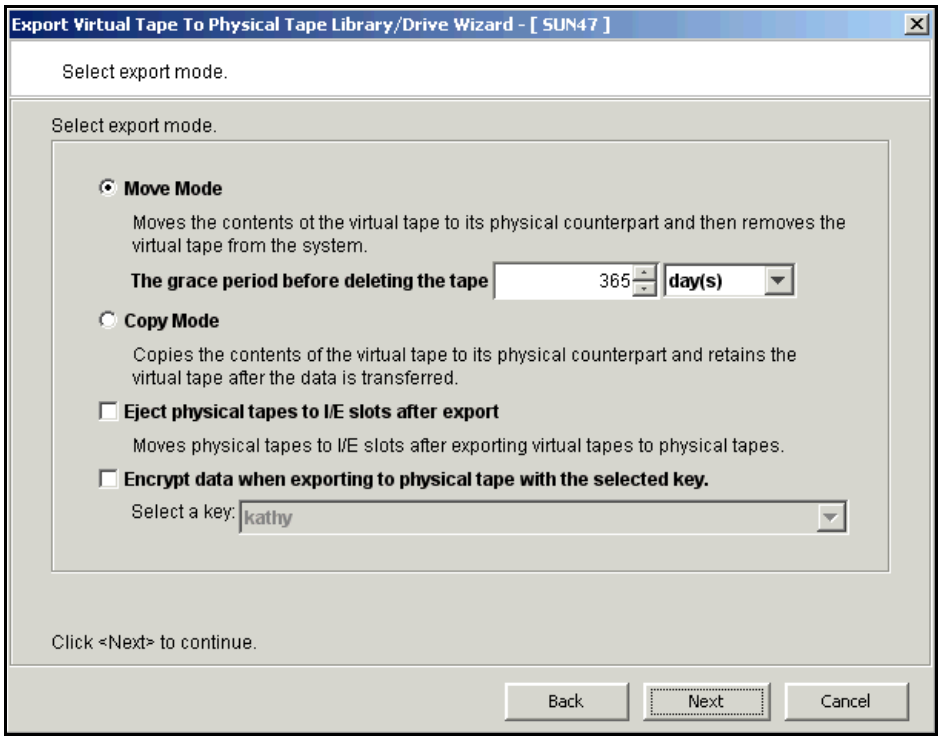
This is what you will see if the tape library supports barcodes.

General | Layout | Statistics | Physical Drives | Physical Tapes

Barcode	In Slot
	0
	1
	2
	4
	6

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

4. Right-click the virtual tape under *Virtual Vault* and select *Export Tape*.
5. Select the physical tape library/drive to which you want to export.
6. Select how you want the data exported and if you want the physical tape exported to the import/export slots.



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

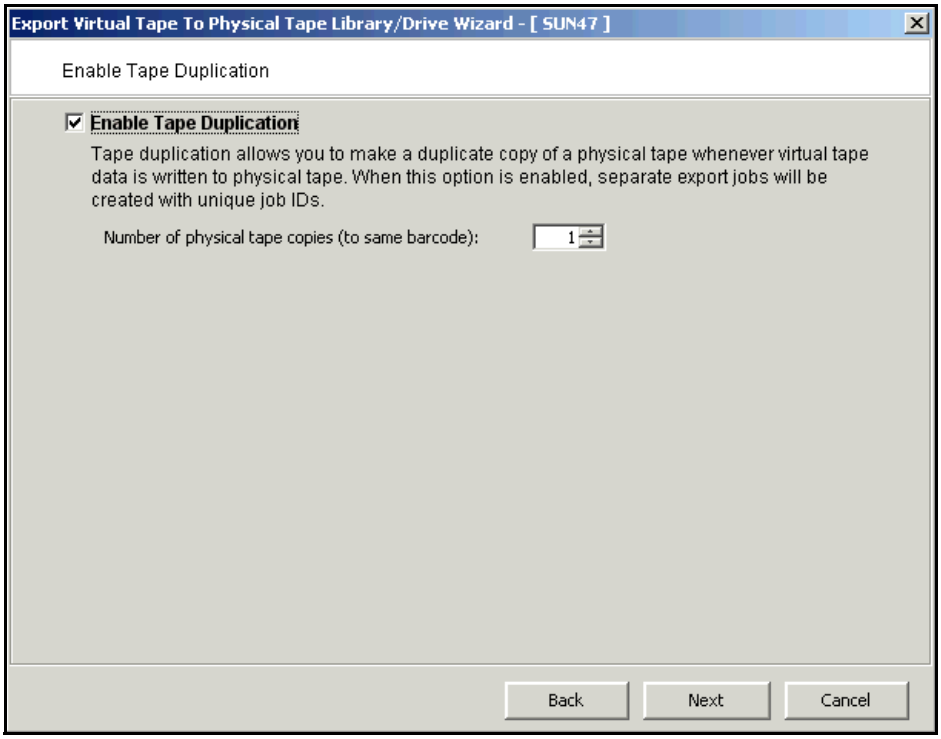
Tape Duplication below, the virtual tape data will not be deleted until the duplication job finishes successfully.

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

Eject physical tapes to I/E slots after export - Move physical tapes to I/E slots after exporting.

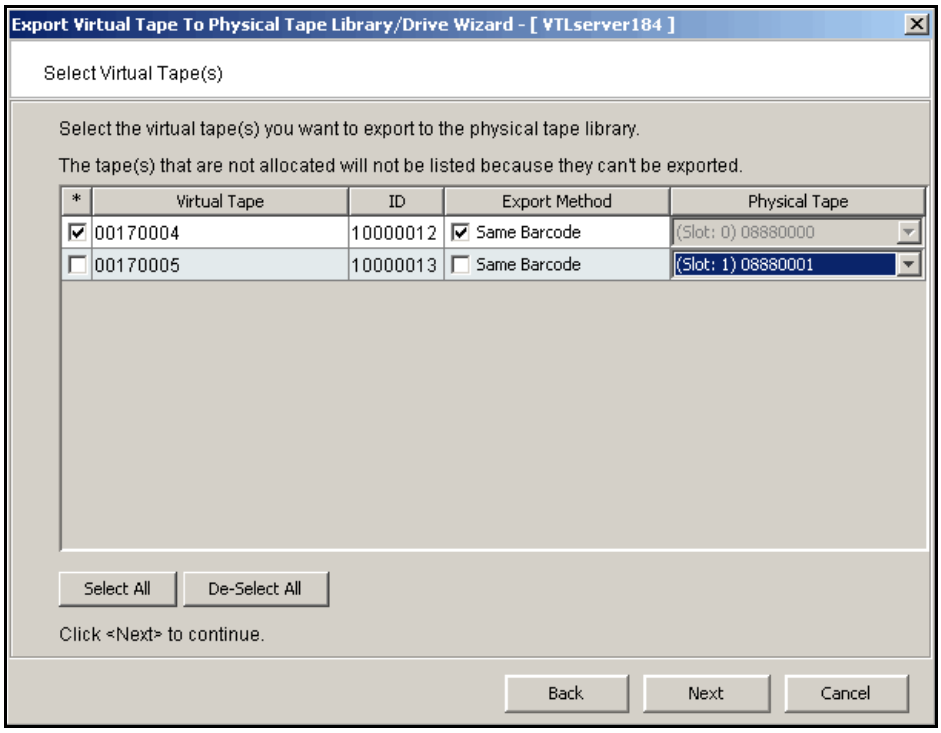
Encrypt data when exporting to physical tape with the selected key - Select if you want to encrypt the data on the tape. You can select this option only if at least one key has been created. If you select this option, you must select the key to use. All the data on the tape will be indecipherable until is imported back to a virtual tape library and decrypted using the same key. For more information about encryption, refer to 'Encrypt data on virtual and physical tapes'.

7. Determine if you want to use Tape Duplication.



Tape Duplication makes a duplicate copy of the physical tape when data is exported. You must have at least two identical physical libraries (same model, same number of drives, same tapes with the same barcodes). When data is exported, separate export jobs will be created for each physical library and each job will have a unique job ID. Refer to 'Tape Duplication' for more information about Tape Duplication.

8. Select the virtual tape(s) you want to export.



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

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

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

   You can check the Budget queue to watch the progress of the job.

Auto Archive

Auto Archive writes data to physical tape whenever a virtual tape is moved to an Import/Export slot by a backup application or other utility after a backup (you will see the tape in the virtual vault). In order to use *Auto Archive*, the physical tape library must support barcodes because when COPAN 400 attempts to export to physical tape it must find a matching barcode in a physical library (you do not need to specify which physical library).

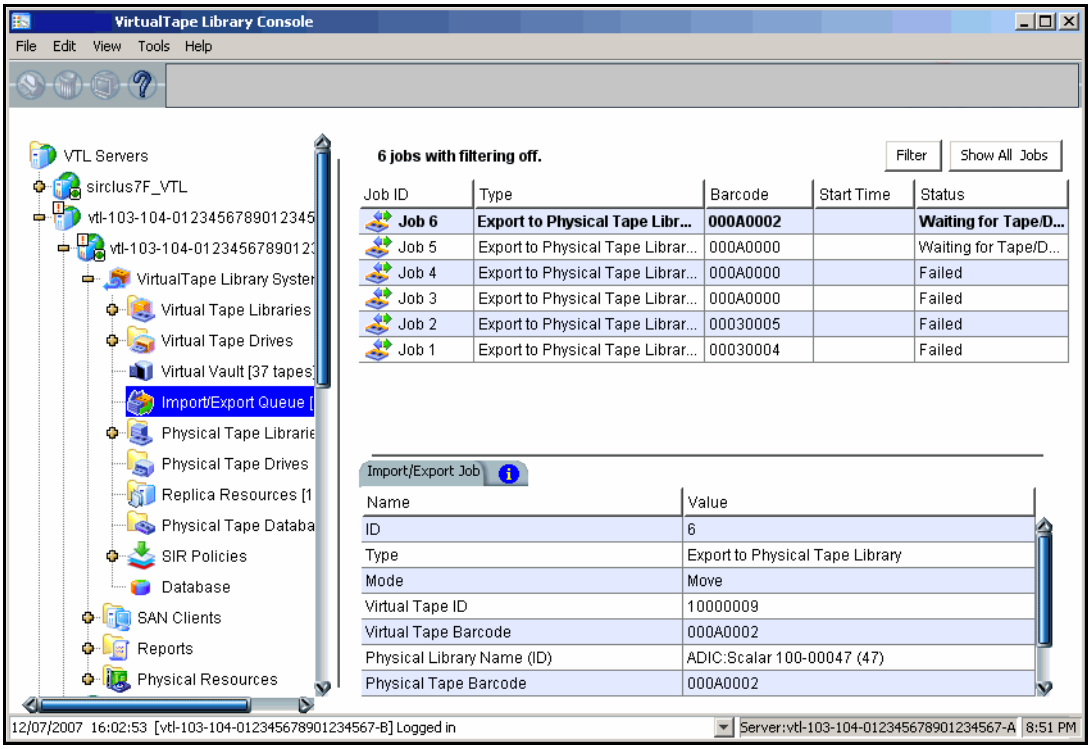
Note: You can only use Auto Archive if you are not currently using the Automated Tape Caching option or the Auto Replication feature on this virtual tape library.

You can configure Auto Archive when you create the library or afterward, as described below:

1. Right-click a virtual tape library and select *Properties*.
2. Select the *Auto Archive* checkbox.
3. Select export options as described for manual export (refer to 'Export manually').

Manage jobs in the budget queue

When you highlight the *Budget Queue* in the tree, a list of all replication jobs, import and export jobs, tape shredding jobs, and Automated Tape Caching jobs that have been submitted is displayed in the right-hand pane.



While the right pane is usually just for informational purposes, you can cancel, put on hold, resume, restart a failed job, or delete a job directly from the right pane by highlighting one or more jobs and using the right-click context menu. You can also highlight any job to see detailed job information.

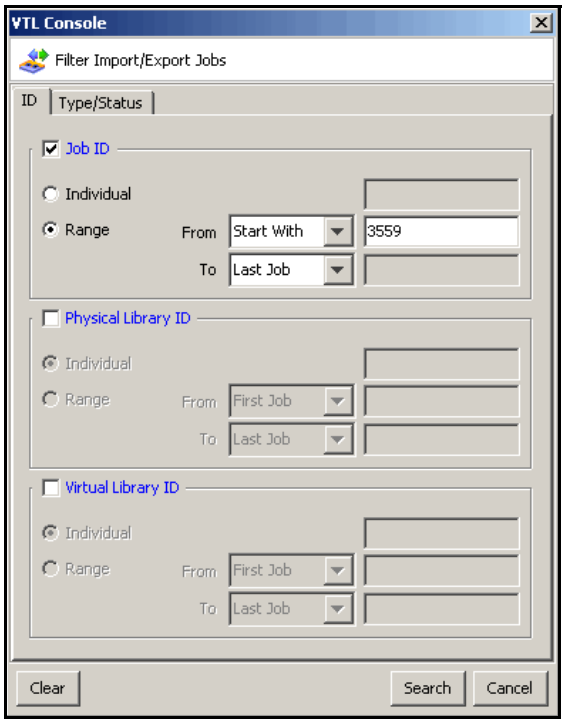
Completed jobs will be purged after 30 days. You can also delete jobs manually. To delete jobs, highlight one or more jobs, right-click, and select *Delete*.

Filter the display of jobs

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

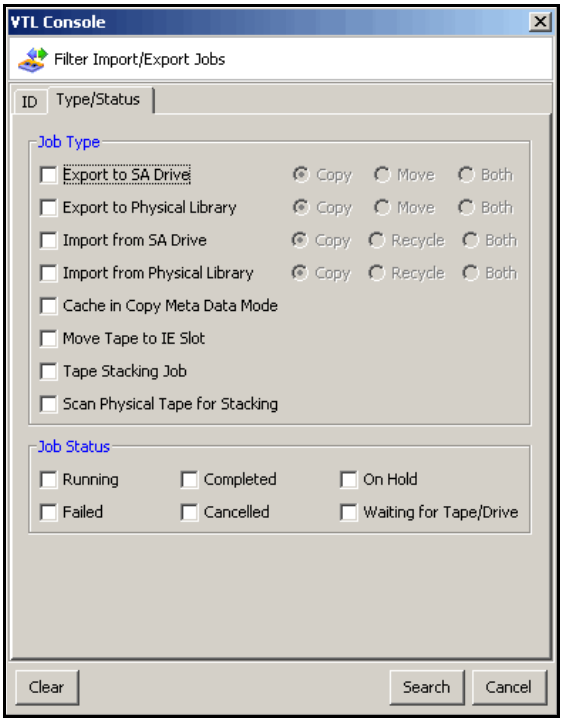
1. Click the *Filter* button.

2. On the *ID* tab, you can specify an individual job or a range of jobs.



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.

3. On the *Type/Status* tab, you can specify a job type.



4. Click *Search*.

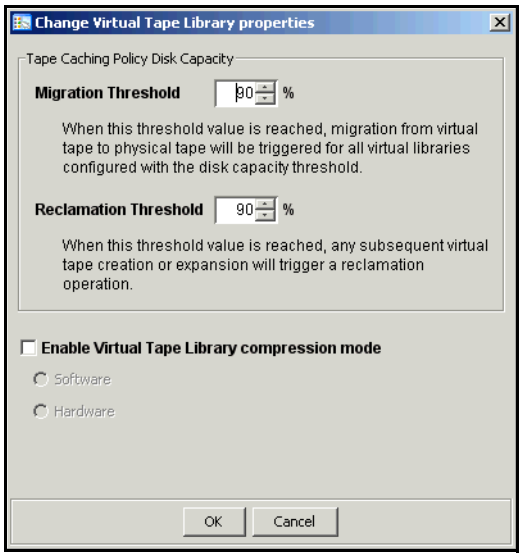
   Afterwards, *just* the jobs that match the selected criteria will be displayed in the right pane. You can click the *Show All Jobs* button when you are done.

Set virtual tape library system properties

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

1. In the console, right-click *Virtual Tape Library System* and select *Properties*.

   If the server is a member of a group, right-click the group and select *VTL Properties*.



2. Select the options you want to use.

   Tape Caching Policy Disk Capacity Migration Threshold - Migration will occur when the used disk space exceeds the specified disk capacity.

   Tape Caching Policy Disk Capacity Reclamation Threshold - Cache disk space is freed up when the used space reaches this threshold.

   Enable Virtual Tape Library compression mode - COPAN 400's compression saves disk space by compressing files so that more data can be stored by a virtual tape drive. Refer to 'Use virtual tape drive compression' for more information.

Use virtual tape drive compression

COPAN 400's compression saves disk space by compressing files so that more data can be stored by a virtual tape drive. The increase in capacity is directly related to the compressibility of the data being backed up. If you can compress the data being backed up by a factor of up to 2:1, you can store up to twice as much information on the virtual tape. Disk compression can vary depending upon the dataset; certain file types (ZIP, PDF, GIF, RAR, etc.) are already compressed and cannot be compressed further.

COPAN 400 supports two types of compression:

- Hardware compression - uses a Hifn Express DR 1000/1050 (1 GB/sec compression), 1620 (1,800 MB/sec), or DR 600/650 (600 MB/sec) compression card. A license keycode is required for hardware compression.
- Software compression - uses an LZO algorithm that runs on the COPAN 400 server.

In order to use either type of compression, you must enable tape drive compression from your backup server.

Note: If you are already using software compression that is performed by your backup application, you should not use COPAN 400's compression. Using both types of compression will cause COPAN 400 to try to compress already-compressed data and this can slow down your backups.

Enable/disable compression

To enable or disable compression:

1. Enable tape drive compression in your backup application.
2. If you are using hardware compression, install a certified compression card in your COPAN 400 server.

   The compression card must be installed before compression begins. If you try to use hardware compression and the compression card is not available, COPAN 400 will send an error message to the Console event log and uncompressed data will be written to the virtual tape drive.

   Note: When it comes time to restore data, if the compression card is not available, you will still be able to restore your data because a software version of the decompression will be used. However, this will slow down the performance of the decompression.

3. In the console, right-click *Virtual Tape Library System* and select *Properties*.

   If the server is a member of a group, right-click the group and select *VTL Properties*.

4. Select the *Enable Virtual Tape Library compression mode* checkbox and specify whether you are using *Software* or *Hardware* compression.

If you are upgrading a COPAN 400 system that previously used software compression to now use hardware compression, the compression mode will be switched to *hardware* when the tape is overwritten.

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

If compression is enabled on the COPAN 400 server, you can still disable or enable compression on each individual virtual tape drive in the same manner as real tape drives -- via your backup application or via SCSI commands which are sent by the operating system. Depending on your operating system, do one of the following:

- UNIX — On backup servers that run Solaris or other UNIX operating systems, specify a compressed tape device file such as /dev/rmt/0cbn to enable compression or /dev/rmt/0ubn to disable compression.
- Windows — On Windows servers select the option in your backup software to enable or disable hardware tape drive compression. If global COPAN 400 compression is disabled, it is possible to enable individual drive compression, but it will have no effect.

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


IBM-ULT3580-TD1-00841

Note: CRC checking can be enabled for hardware compression cards to help detect data corruption and identify the source of the corruption. This feature is disabled by default. Contact SGI Technical Support if you need to use this feature.

Change firmware of a virtual library or drive

You can change the firmware of a virtual library or drive to match that of the physical library/drive. To do this:

1. Right-click a virtual tape library or drive and select *Change Firmware*.
2. Enter the new firmware and click *OK*.

Encrypt data on virtual and physical tapes

To ensure that the data you export to tape is confidential and secure, COPAN 400 enables you to create encryption keys that use the Advanced Encryption Standard (AES) 256-bit key algorithm (Secure Tape) published by the National Institute of Standards and Technology, an agency of the U.S. government. When you export data to physical tape, you can choose an encryption key to encrypt the data. When you import the same data back to virtual tapes, you must choose the same key to decrypt the data and enable it to be read.

Each key consists of a secret phrase. For additional security, each key is password-protected. You must provide this password in order to change the key name, password, or password hint, or to delete or export the key.

You can apply a single key to all virtual tapes when you export them to physical tape, or you can create a unique key for each one. Creating multiple keys provides more security; in the unlikely event that a key is compromised, only the tapes that use that key would be affected. However, if you use multiple keys, you must keep track of which key applies to each tape so that you use the correct key to decrypt the data when you import the physical tape back to virtual tape.

Once you have created one or more keys, you can export them to a separate file called a key package. If you send encrypted tapes to other locations that run COPAN 400, you can also send them the key package. By importing the key package, administrators at the other sites can then decrypt the tapes when they are imported back into virtual tape libraries managed by COPAN 400.

You can enable encryption and specify which key to use when you:

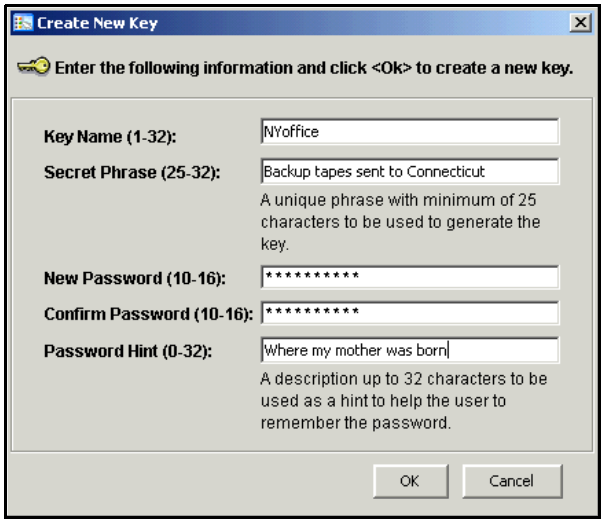
- Manually import or export a tape
- Configure to use the auto archive feature
- Create a cache for physical tapes, if you are using Automated Tape Caching

Note: If you apply an incorrect key when importing a tape, the data imported from that tape will be indecipherable.

Create a key

To create a key to use for data encryption:

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



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

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

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

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

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

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

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

7. Click *OK*.

Change a key name or password

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

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

To change a key name or password:

1. In the navigation tree, right-click the server name and click *Key Management*.
2. From the *Key Name* list, click the key you want to change.
3. Click *Edit*.
4. If you closed the *Key Management* dialog box after creating the key, type the current password for accessing this key in the *Password* text box.

   If you just created the key, did not close the *Key Management* dialog box, and subsequently decided to change the key, you are not prompted for the password.
5. Make the desired changes.
6. Click *OK*.

Delete a key

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

To delete a key:

1. In the navigation tree, right-click the server name and click *Key Management*.
2. From the *Key Name* list, click the key that you want to delete.
3. Click *Delete*.
4. In the *Password* text box, type the password for accessing this key.
5. Type YES to confirm.
6. Click *OK*.

Export a key

When you export a key, you create a separate file called a *key package* that contains one or more keys. You can then send this file to another site that uses COPAN 400, and administrators at that site can import the key package and use the associated keys to encrypt or decrypt data.

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

To export a key:

1. In the navigation tree, right-click the server name and click *Key Management*.
2. Click *Export*.
3. In the *Package Name* text box, type the file name to use for this key package (1–32 characters).
4. In the *Decryption Hint* text box, type a three-character hint.

   When you subsequently attempt to import a key from this key package, you are prompted for a password. If you provide the correct password, the decryption hint specified here appears correctly on the *Import Keys* dialog box. If you provide an incorrect password, a different decryption hint appears. You can import keys using an incorrect password, but you will not be able to decrypt any files using those keys.
5. From the *Select Keys to Export* list, select the key(s) that you want to include in the key package.

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

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

   If you selected a key and subsequently decide not to include it in the key package, you can clear the key. You can also clear all selected keys by clicking *De-Select All*.
6. Select *Prompt for new password for all keys in package* if you want to create a new password for the key package.

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

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

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

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

8. Click *OK*.

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

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

Import a key

Once you have created a key package, you can open that package and specify which keys to import into COPAN 400. Once you import a key, you can use that key to encrypt or decrypt data.

To import a key:

1. In the navigation tree, right-click the server name and click *Key Management*.
2. Click *Import*.
3. In the *Find Package* text box, type the full path to the key package.

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

4. Click *View.*
5. Type the password for accessing the key package in the *Password* text box.

   Note: After you provide the password, make sure that the displayed *Decryption Hint* matches the decryption hint specified when the key package was created. If the hint is not correct, click *Password* and provide the correct password for accessing the key package. If you provide an incorrect password, you will still be able to import the keys in the package, but you will not be able to use them to decrypt any data that was previously encrypted using those keys.

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

   You can select only those keys that have a green dot and the phrase *Ready for Import* in the *Status* column. A red dot and the phrase *Duplicate Key Name* indicates that a key of the same name already exists in this instance of COPAN 400 and cannot be imported.

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

Note: A key of the same name might not necessarily have the same secret phrase. For example, you might have a key named Key1 with a secret phrase of ThisIsTheSecretPhraseForKey1. If the key package was created by another instance of COPAN 400, it might also have a key named Key1, but its secret phrase might be ThisIsADifferentSecretPhrase. Since the key names are the same, you will not be able to import the key in the key package unless you rename the existing Key1. After you rename the key, you can continue to use it to decrypt tapes that were encrypted using that key, and you can also import the key named Key1 from the key package and use it to decrypt tapes that were encrypted using that key.

7. Click *OK*.

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

Shred a virtual tape

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

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

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

To shred tapes:

1. Move the tape(s) you want to shred to the virtual vault.
2. Select the tape(s) you want to shred.

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

   For multiple tapes, highlight all of the tapes you want, right-click, and select *Tape Shredding --> Shred Tapes.*
3. If desired, select the option to delete the tape after shredding it.
4. Type *YES* to confirm and click *OK*.

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

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

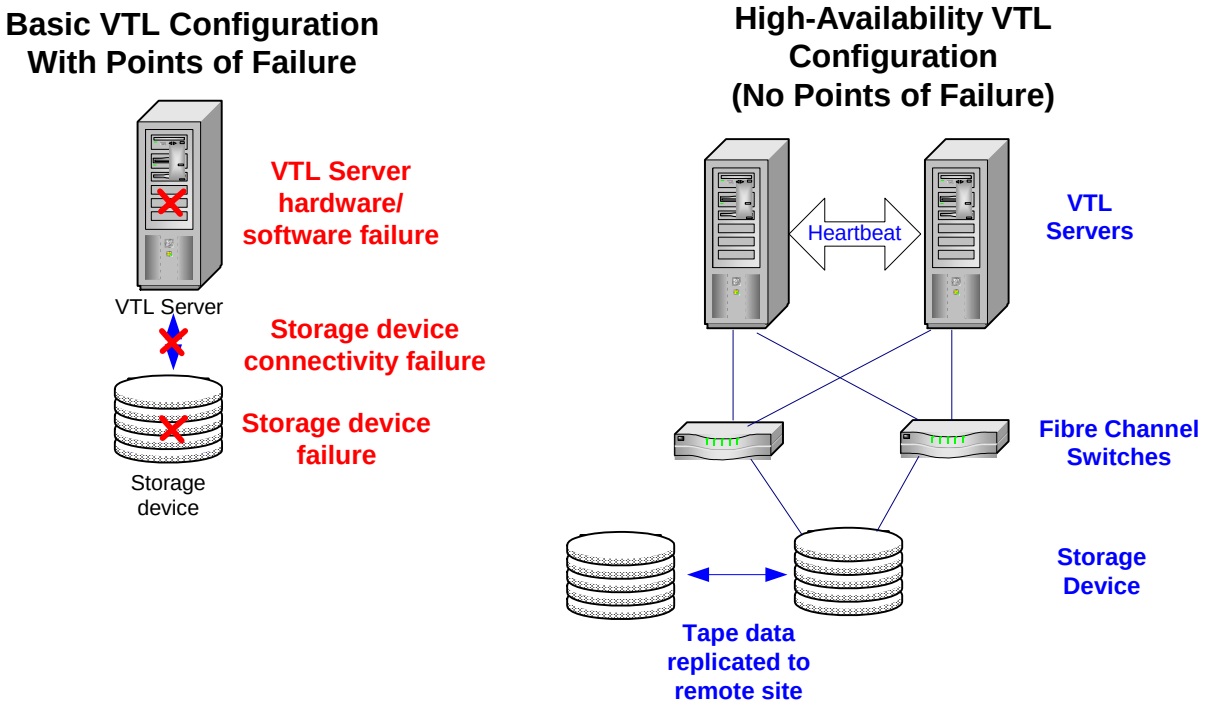
Server Failover

Overview

To support mission-critical computing, Failover provides high availability for your COPAN 400 system, protecting you from a wide variety of problems, including:

- Storage device path failure
- COPAN 400 server failure (including storage device failure)

The following illustrates a basic COPAN 400 configuration with potential points of failure and a high availability configuration, where COPAN 400's high availability options work with redundant hardware to eliminate the points of failure:



Storage device path failure

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

You can eliminate this potential point of failure by providing a multiple path configuration, using multiple Fibre Channel switches, and/or multiple adapters, and/or storage devices with multiple controllers. In a multiple path configuration, COPAN 400 automatically detects all paths to the storage devices. If one path fails, COPAN 400 automatically switches to another.

Note that Fibre Channel switches can demonstrate different behavior in a multiple path configuration. Before using this configuration with COPAN 400, you must verify that the configuration can work on your server *without* the COPAN 400 software. To verify:

1. Use the hardware vendor's utility to see the devices after the driver is loaded.

   You can also use Linux's *cat /proc/scsi/scsi* command.

2. Use the hardware vendor's utility to access the devices.

   You can also use Linux's *hdparm* command.

3. Unplug the cable from one device and use the utilities listed above to verify that everything is working.

4. Repeat the test by reversing which device is unplugged and verify that everything is still working.

COPAN 400 server failure (including storage device failure)

COPAN 400's Failover option provides high availability for COPAN 400 operations by eliminating the down time that can occur should a COPAN 400 server (software or hardware) fail.

In the COPAN 400 failover design, a COPAN 400 server is configured to monitor another COPAN 400 server. In the event that the server being monitored fails to fulfill its responsibilities to the SAN clients it is serving, the monitoring server will seamlessly take over its identity.

COPAN 400 uses a unique monitoring system to ensure the health of the COPAN 400 servers. This system includes a self-monitor and an intelligent heartbeat monitor.

The *self-monitor* is part of all COPAN 400 servers, not just the servers configured for failover and provides continuous health status of the server. It is part of the process that provides operational status to any interested and authorized parties, including the console and supported network management applications through SNMP. The self-monitor checks the COPAN 400 processes and connectivity to the server's storage devices.

In a failover configuration, COPAN 400's intelligent *heartbeat monitor* continuously monitors the primary server through the same network path that the server uses to serve its clients.

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

- All is well and no failover is necessary.
- The self-monitor detects a *critical error in the COPAN 400 server processes* that is determined to be fatal but does not affect the network interface. In this case, the secondary will inform the primary to release its COPAN 400 identity and will take over serving the failed server's clients.

- The self-monitor detects a *storage device connectivity failure* but cannot determine if the failure is local or applies to the secondary also. In that case the device error condition will be reported through the heartbeat. The secondary will check to see if it can successfully access the device. If it can, it attempts to access all devices. If it can successfully access all devices, the secondary initiates a failover. If it cannot successfully access all devices, no failover occurs.

Because the heartbeat shares the same network path as the server's clients, it is determined that clients cannot access their resources whenever the heartbeat cannot be retrieved. This is considered a *Catastrophic failure* because the server or the network connectivity is incapacitated. In this case the secondary will immediately attempt to initiate a failover. The primary server’s power control management interface must be able to respond to the secondary server in order for failover to occur.

Failover terminology

Primary/ Secondary servers

COPAN 400 *primary* and *secondary* servers are separate, independent COPAN 400 servers that each have their own assigned clients. In *Active-Passive Failover*, the primary COPAN 400 server is monitored by the secondary COPAN 400 server. In the event the primary server fails, the secondary takes over.

In *Active-Active Failover (*or *Mutual Failover)*, both servers are configured to monitor each other. The terms *Primary* and *Secondary* are purely from the client's perspective. Each server is *primary* to its own clients and *secondary* to the other's clients. Each server normally services its own clients. In the event one server fails, the other will take over and serve the failed server's clients.

Failover/ Takeover

Failover/takeover is the process that occurs when the secondary server takes over the identity of the primary. Failover will occur under the following conditions:

- One or more of the COPAN 400 processes goes down.
- There is a network connectivity problem, such as a defective HBA or a loose network cable.
- There is a storage path failure or power failure.

There is a three minute delay after failover occurs. During this time, no I/O is permitted.

Recovery

The process when the secondary server releases the identity of the primary to allow the primary to restore its operation.

There is a three minute delay during recovery. During this time, no I/O is permitted.

Auto Recovery

Auto Recovery occurs after a failover, when control is returned to the primary server once the secondary server determines that the primary server has recovered. It determines this by continually monitoring the primary server, even after the failover.

If failover is caused by loss of network connectivity, auto recovery will occur when all heart monitoring connections are restored. If you are using multiple IP addresses for health monitoring, all network connections must be restored to initiate auto recovery.

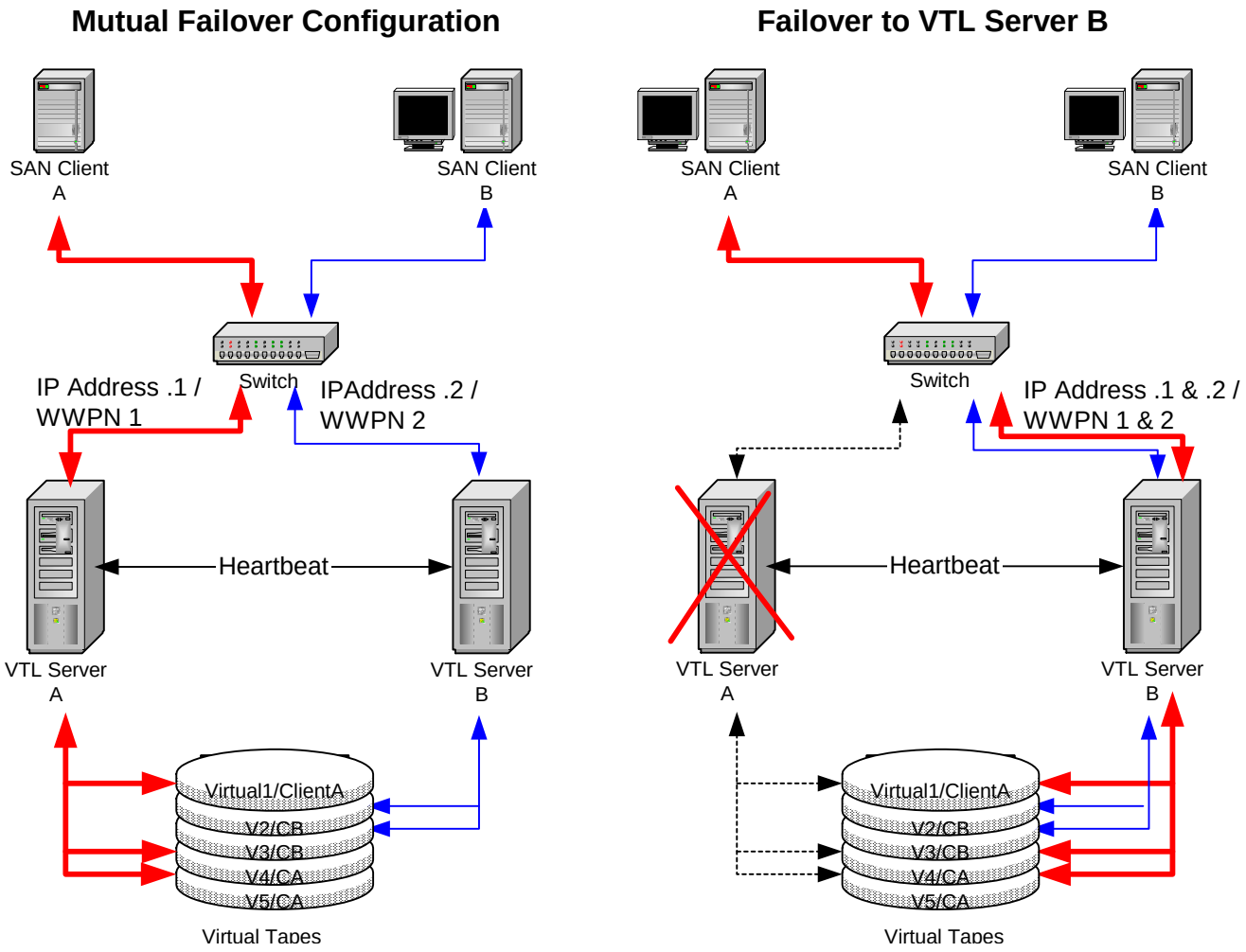
Once control has returned to the primary server, the secondary server returns to its normal monitoring mode.

Failover Group

For ease of identification, the primary and secondary failover servers in a set are grouped together in the console beneath the failover group object.

Power control management interface

A hardware-level interface that monitors various hardware functions on a server. IPMI and HP iLO are supported interfaces.



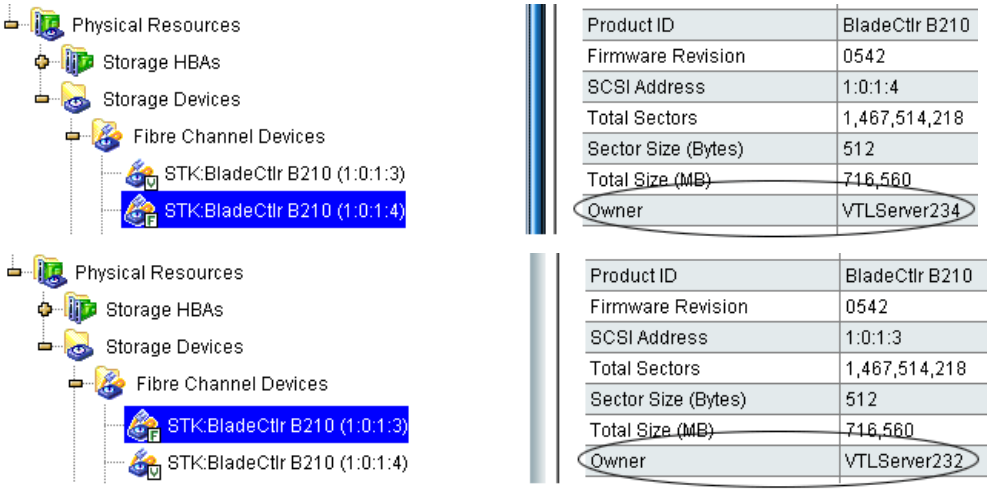
This diagram illustrates a COPAN 400 failover configuration. When server A fails, server B takes over and serves the clients of server A in addition to its own clients.

Failover requirements

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

- You must have two COPAN 400 servers.
- The failover pair should be installed with identical operating system versions and must have identical storage configurations.
- The servers need access to all common virtual devices but devices cannot be owned by both servers. This means that storage devices must be attached in a multi-host SCSI configuration or attached on a Fibre loop or switched fabric. In this configuration, both servers can access the same devices at the same time (both read and write). You will see something similar to the following when you look at the physical storage in the console.

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



- Both servers must have Fibre Channel Target Mode enabled.
- Both servers must have exactly the same COPAN 400 options licensed.
- Physical drives cannot be shared among COPAN 400 servers. Physical drives should be visible to the other server but not assigned to COPAN 400.
- Both servers must be able to access the COPAN 400 database resource.
- (SCSI only) Termination should be enabled on each adapter, but not on the device, in a shared bus arrangement.
- Failover servers must be configured with a power control management interface on the motherboard. IPMI (Intelligent Platform Management Interface) and HP iLO are supported interfaces. Refer to 'Power control management' for more information.
- Both servers must reside on the same network segment, because in the event of a failover, the secondary server must be reachable by the clients of the primary server. This network segment must have at least one other device that generates a network ping (such as a router, switch, or server). This allows the secondary server to detect the network in the event of a failure.
- If you are protecting multiple IP addresses, each protected IP address must be in its own subnet.

- You need to reserve an IP address for each network adapter in your failover servers. The IP address must be on the same subnet as the server. These IP addresses are used by the servers to monitor each other's health. The health monitoring IP address remains with the server in the event of failure so that the server’s health can be continually monitored. After failover, the health monitoring IP address still exists until the network services are restarted. Note that COPAN 400 clients and the console should not use the health monitoring IP address to connect to a server.
- In addition to standard IP addresses, each server must have a power control IP address (used by power control software).
- A standby initiator port needs to be available. This port needs to be connected to the same FC switch as the target port and should not be zoned to anything else. In a multi-ID configuration, you can configure the target port to act as a standby initiator.
- The primary and secondary servers should use the exact same Target Port ID scheme on the matching WWPNs. We recommend using the same initiator adapter numbers on both sides to connect to the same storage, so the ACSL of all the devices will look identical on both sides.
- You must use static IP addresses for your failover configuration. We also recommend that the IP addresses of your servers be defined in a DNS server so they can be resolved.
- The first time you set up a failover configuration, the secondary server must not have any logical resources (including virtual tapes, drives, or libraries) or clients.
- Because the primary and secondary servers will become part of a failover group, the servers cannot belong to a multi-node group.

Power control management

Power control management is a hardware-level interface that monitors various hardware functions on a server. Power control management is required in order for failover to occur. IPMI and HP iLO are supported interfaces.

At times, a server may become unresponsive, but, because of network or internal reasons, it may not release its resources or its IP address, thereby preventing failover from occurring. To allow for graceful failover, IPMI or HP iLO will reset the power of the primary server, forcing the release of the server's resources and IP address.

IPMI is included and configured on all SGI appliances.

If you are using a third-party appliance, you must determine if power control management is provided by your hardware vendor. To check for IPMI, use the dmidecode command and look for the *IPMI Device Information* section. You must also make sure that the *Interface Type* is defined.

If you determine that power control management is provided, you must follow the vendor's instructions to configure it and you must create an administrative user via your configuration tool. The IP address cannot be the virtual IP address that is set for failover.

Backup server failover configuration

While failover and failback are transparent for the COPAN 400 server, some configuration may be necessary for your backup server in order for physical devices to be accessed after failover. The configuration varies by backup application and operating system. To ensure that physical devices can be accessed after failover, we recommend you follow the instructions below.

Windows 2000

Veritas NetBackup	In order for NetBackup to access COPAN 400 devices after failover, set the backup server's Fibre Channel HBA timeout value to a higher value (such as 250 seconds).

HP-UX

All backup software	HP-UX uses the FC port ID as its target ID. Failover will change the FC switch port ID. Cisco switches automatically support switch port swapping. If you are using a Brocade switch model 3900 and up (3900, 12000, 24000, 4100, etc.) with a Tachyon adapter, you have to manually set up a port swapping script. Refer to 'Port swapping for Brocade switches' for more information.

AIX

All backup software	AIX uses the FC port ID to generate its local ID. Failover will change the FC switch port ID. If you are using AIX 4.3, 5.1, or 5.2 with a Brocade switch model 3900 and up with a Tachyon adapter, you have to manually set up a port swapping script. Cisco switches automatically support switch port swapping. Refer to 'Port swapping for Brocade switches' for more information. If you are using AIX 5.3 or above with a Brocade switch model 3900 or above, you only need to enable the dynamic tracking option; it is not needed to use the port swapping scripts. Note that TSM 5.4 supports failover without a port swapping script.

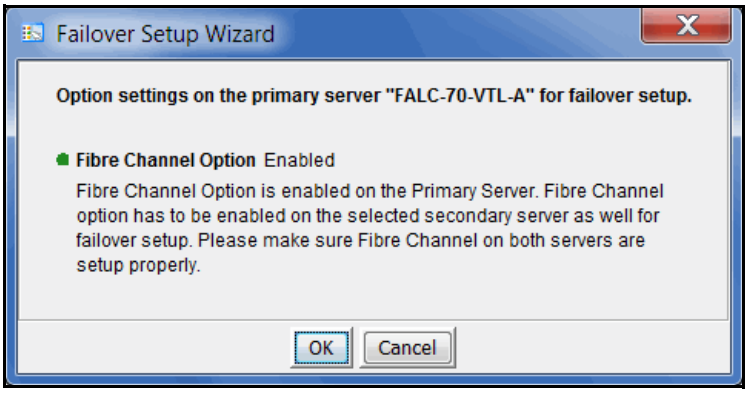
Configure Failover

Notes:

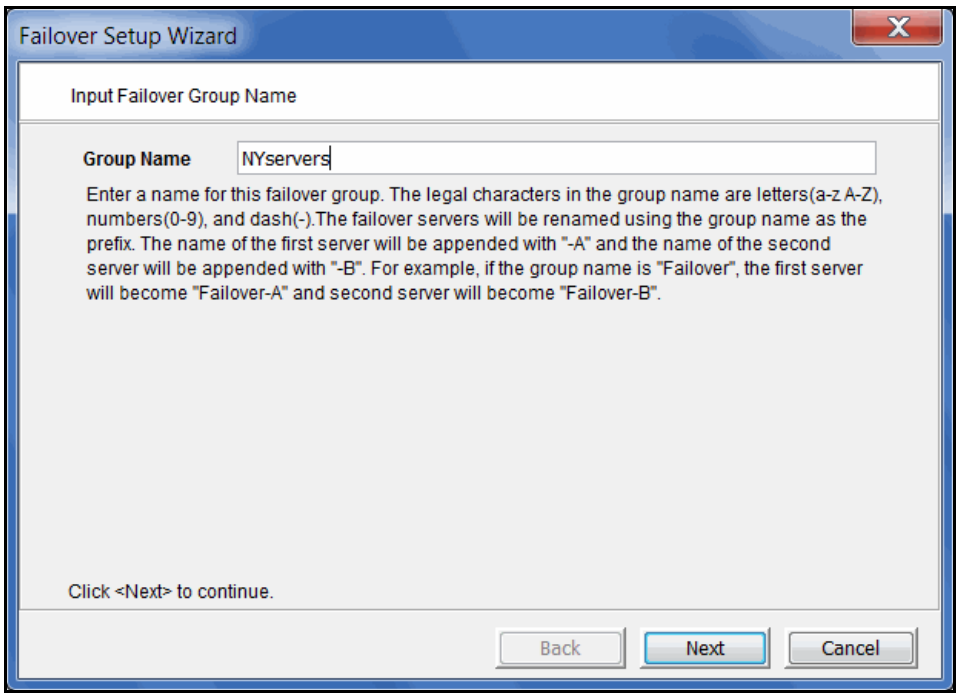
- You will need to know the IP addresses and WWPNs of the failover servers and the health monitoring process. It is a good idea to gather this information and find available IP addresses before you begin the setup.
- If you have not already done so, enable Fibre Channel on both the primary and secondary servers.
- If you have not already done so, on both the primary and secondary servers, enable target mode for any initiator that is zoned with your backup server. Refer to "Switch to target mode" for more information.
- You cannot enable or disable iSCSI once you configure failover. If you want to change the state of iSCSI, you should do it before configuring failover.

1. Right-click the server that will become the primary server in your failover configuration and select *Failover --> Failover Setup Wizard*.

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



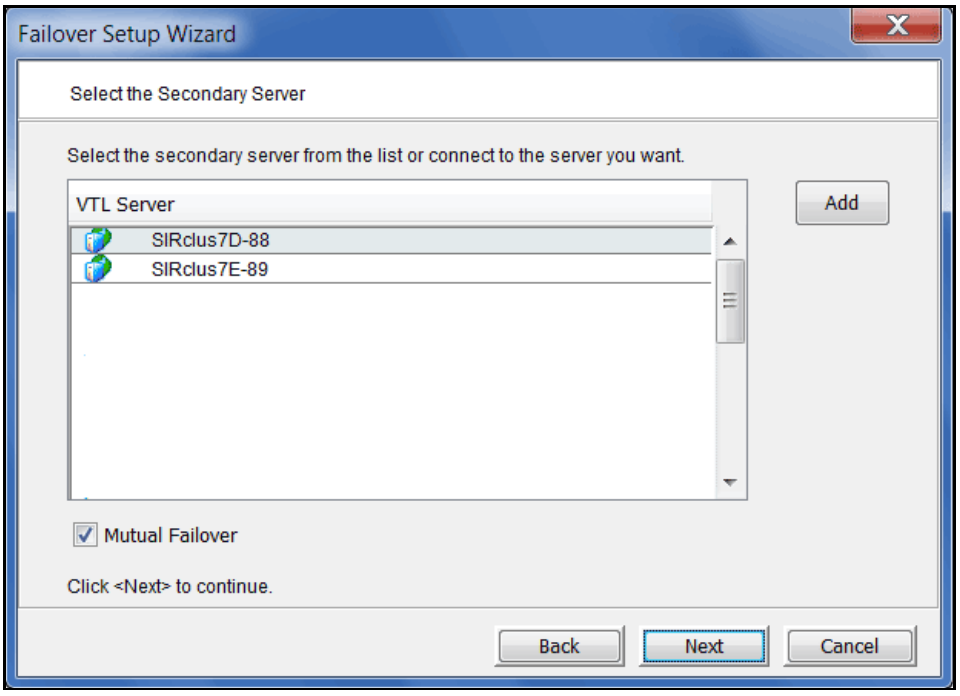
2. Enter a name for the failover pair.



For ease of identification, the primary and secondary failover servers in a set are grouped together in the console. If the servers are already part of a group, that group name will continue to be used and you will not see this dialog.

The failover group name can contain letters, numbers, a dash, or underscore. Spaces and other characters are not allowed.

3. Select the secondary server.

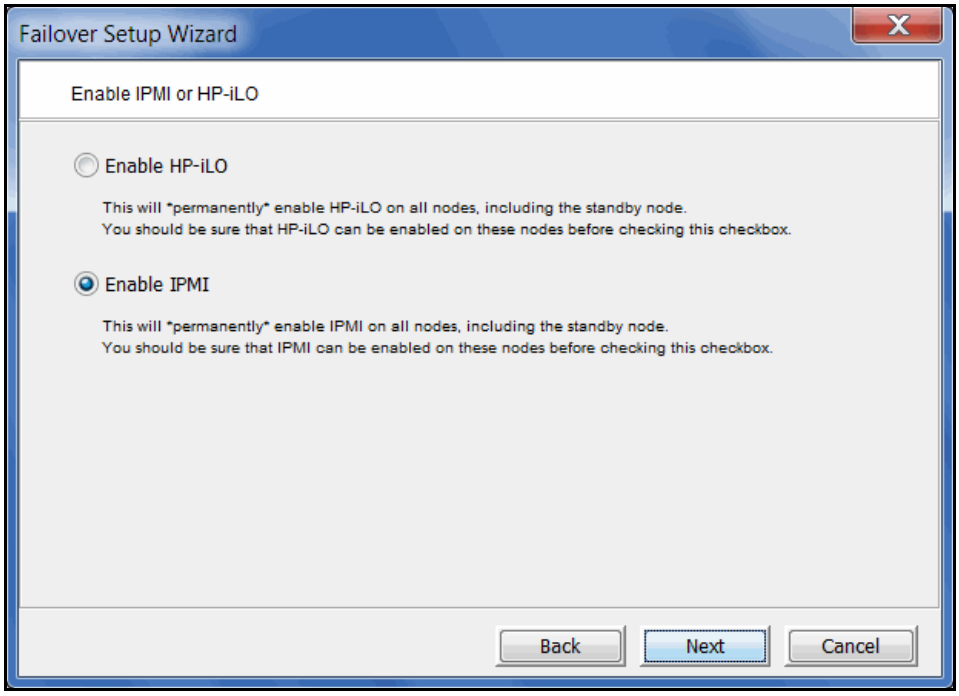


Select *Mutual Failover* if you want both servers to monitor each other.

4. If prompted, determine if you want to change the host name of each failover server.

   If you choose to change the host name, the failover group name will be used as the prefix for the server name. The name of the first server is appended with "-A" and the name of the second server with "-B". For example, if the group name is "NewYork", the first server will be "NewYork-A" and the second server will be "NewYork-B". In order to rename a server, the server will have to be restarted.

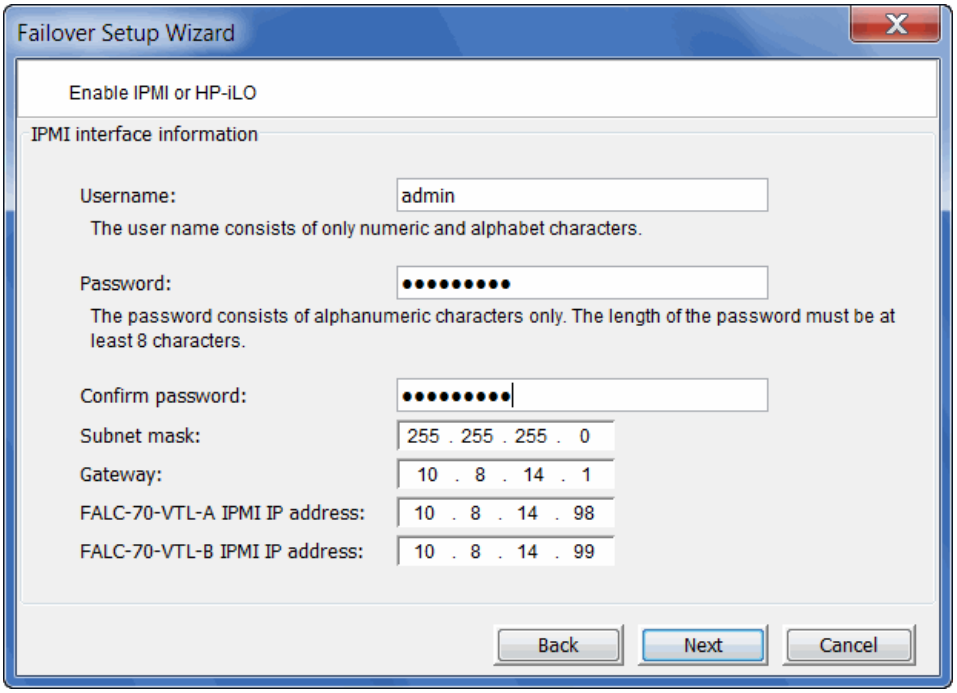
5. Confirm or select the type of power control management interface your hardware is using.



   The system automatically selects the correct one for you.

   When you click *Next*, the driver will be loaded on each node.

6. Enter power control information.

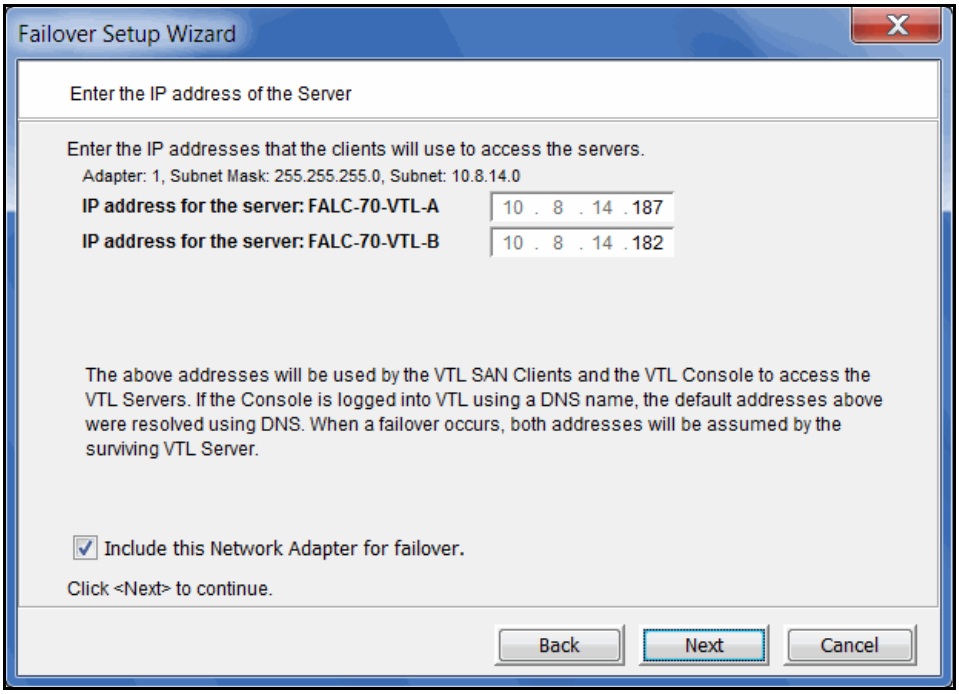


The subnet, gateway, and IP address information is automatically pre-filled.

On SGI appliances, the IPMI user name and password are preset as *admin* and *falcon101*.

The user name and password you specify here will overwrite the existing information.

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



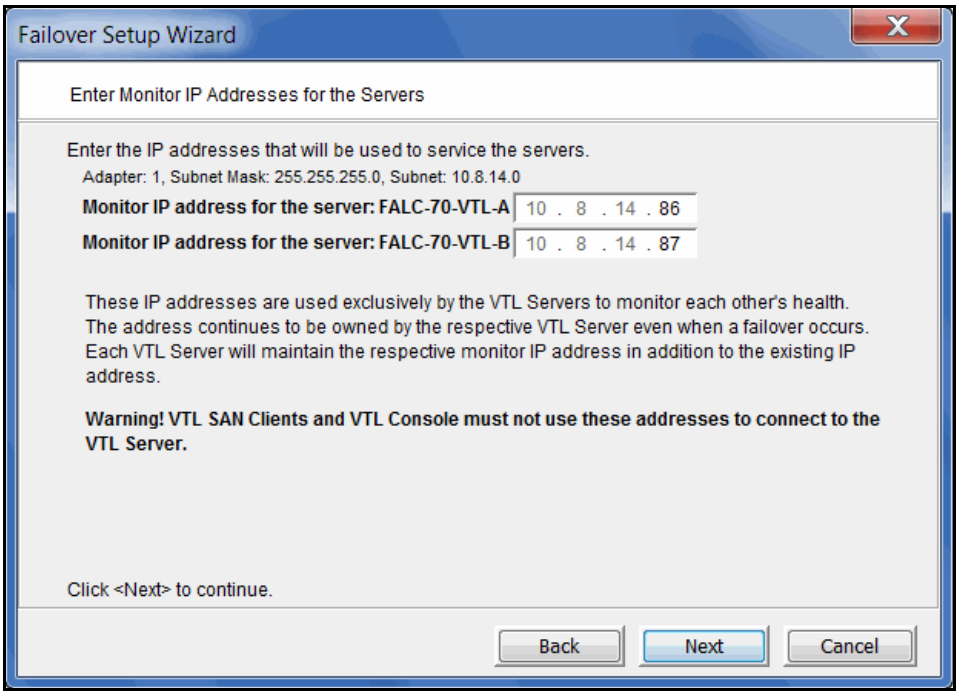
The dialog also shows the corresponding IP address on the secondary server, the IP address to which the system will fail over.

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

Notes:

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

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

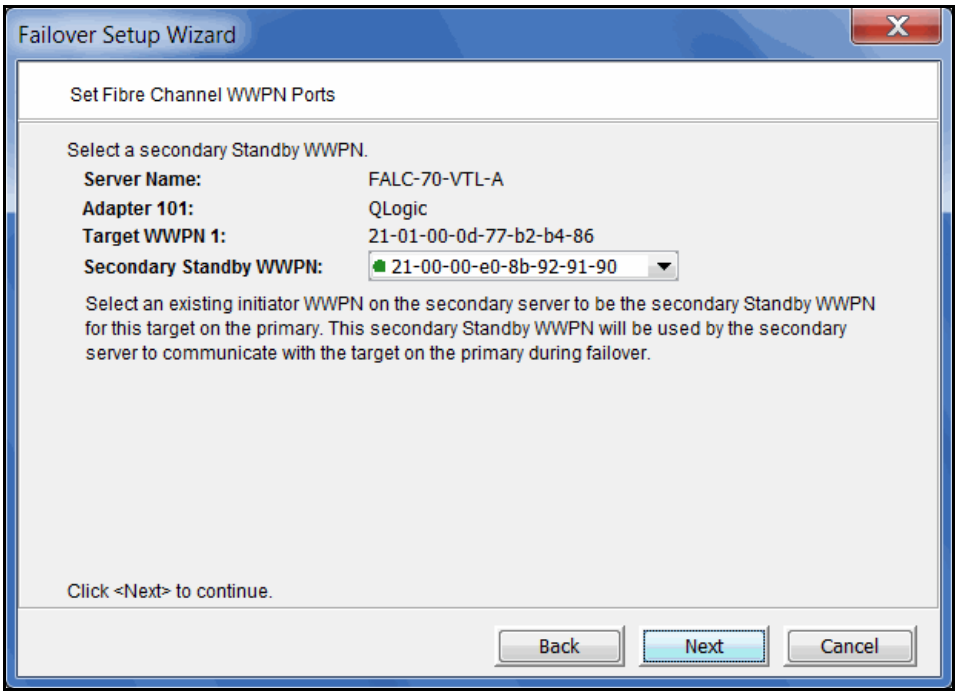


   This IP address will be used to continuously monitor the other server. The health monitoring IP address remains with the server in the event of failure so that the server's health can be continually monitored. After failover, the health monitoring IP address still exists until the network services are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

   You must use static IP addresses.

9. If you want to use additional network adapter cards, repeat steps 7 and 8.

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

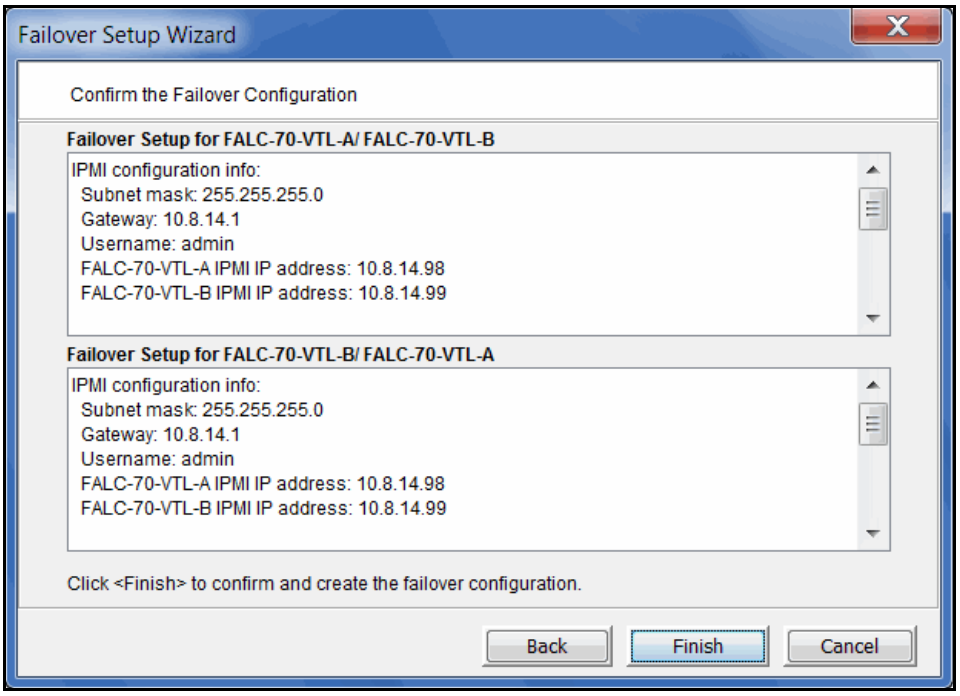


    The proper adapter is usually selected for you, but you should confirm that the adapter shown is not the initiator on your secondary server that is connected to the storage array, and also that it is not the target adapter on your secondary server.

    There should not be any devices attached to this initiator.

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

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

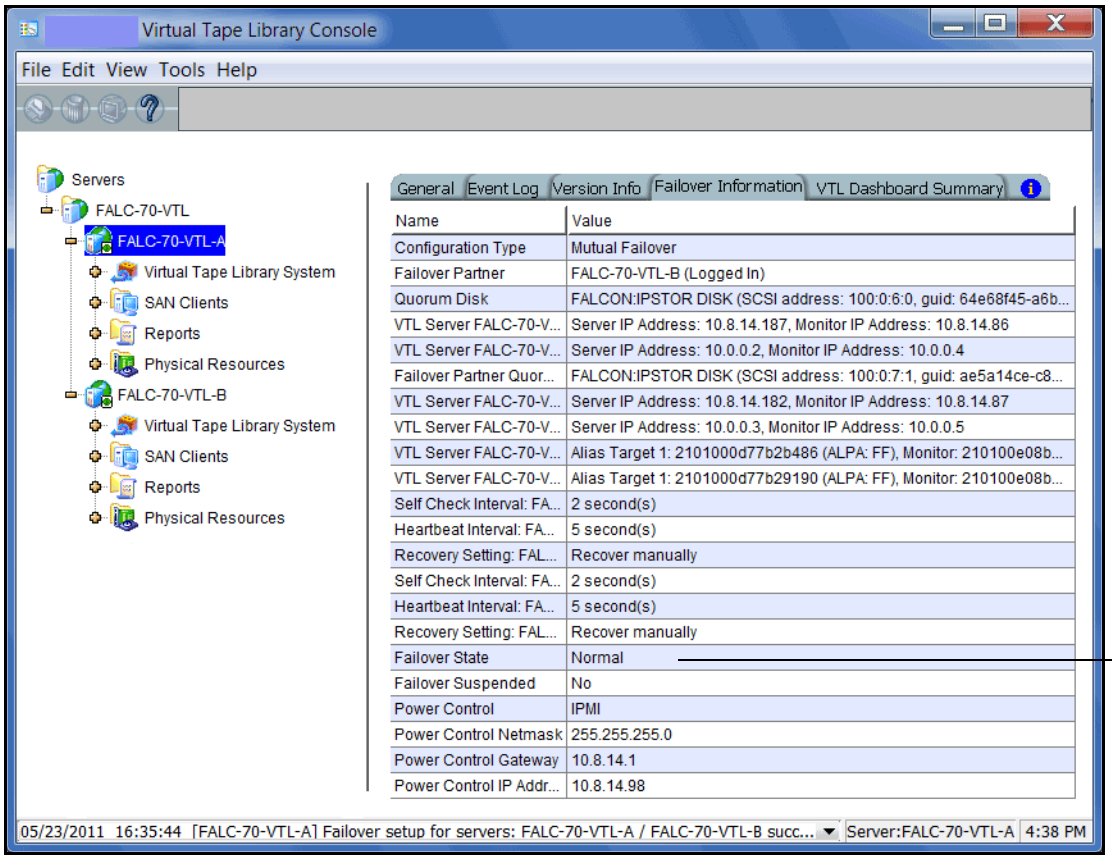


Once your configuration is complete, each time you connect to either server in the Console, you will automatically be connected to the other as well.

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

Check failover status

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



In addition, COPAN 400 uses different colors to indicate the failover status:

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

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

Make changes to the servers in your failover configuration

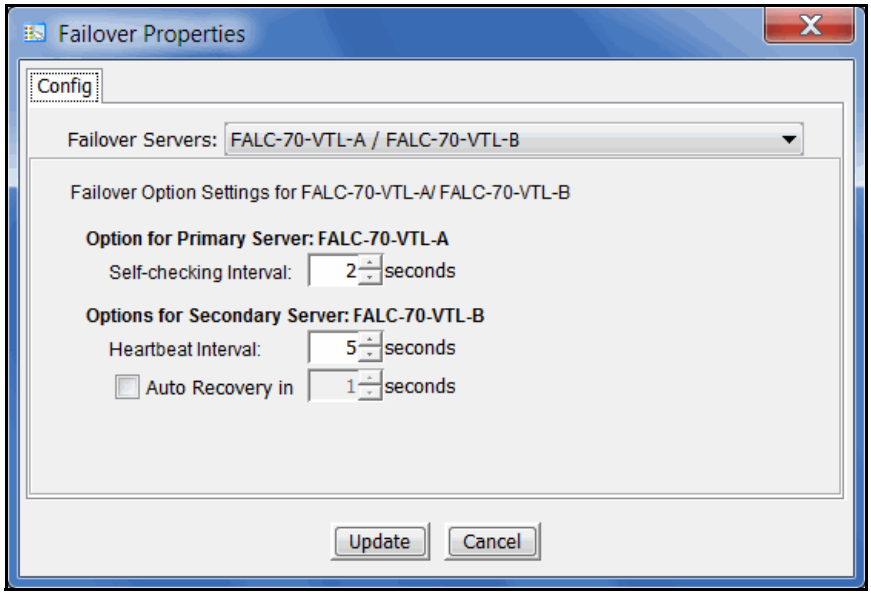
The first time you set up your failover configuration, the secondary server cannot have any logical resources (tape or Replica Resources) or clients assigned to it. Afterwards, you may want to add resources, create virtual devices, and assign clients to the server.

In order to make any of these changes, you must be running the console with write access to both servers. COPAN 400 will automatically "log on" to the failover pair when you attempt any configuration on the failover set. While it is not required that both servers have the same username and password, the system will try to connect to both servers using the same username and password. If the servers have different usernames/passwords, it will prompt you to enter them before you can continue.

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

Change your failover properties

Right-click the failover group and select *Failover --> Properties* to change the self-checking, heartbeat, and auto recovery properties for this configuration.



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

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

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

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

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

Change the power control password

If you need to change the password that is used for power control, right-click the failover group and select *Failover --> Power Control --> Change Power Control Password.*

Force a takeover by a secondary server

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

Manually initiate a recovery to your primary server

Right-click the server and select *Failover --> Stop Takeover* if your failover configuration was not set up to use COPAN 400's Auto Recovery feature and you want to force control to return to your primary server or if you manually forced a takeover and now want to recover to your primary server.

Suspend/resume failover

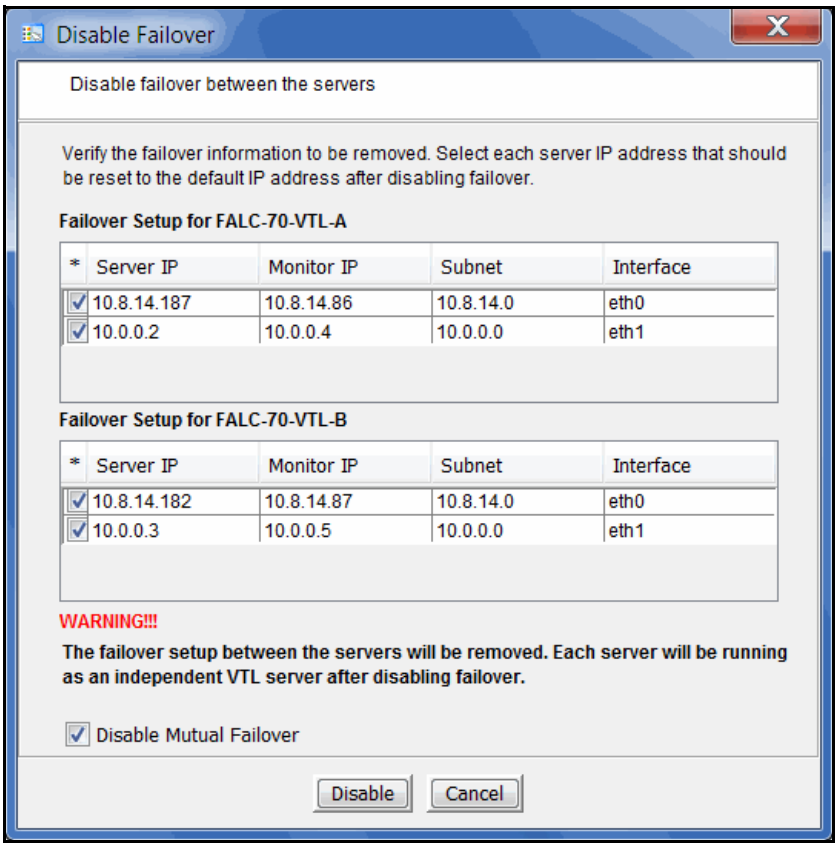
Right-click the failover group and select *Failover --> Suspend* to stop monitoring your servers. The server name will be displayed in yellow while failover is suspended. The server will NOT take over the primary server's resources even it detects an abnormal condition from the primary server.

Right-click the failover group and select *Failover --> Resume* to restart the monitoring.

Note: While failover is suspended, if your library, drive, or client configuration changes on either failover server, the changes will not be synchronized with the partner. Therefore, it is important to not change your library, drive, or client configuration while failover is suspended.

Disable failover

Right-click the failover group and select *Failover --> Disable* to disable failover.



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

If this is a mutual failover configuration and you want to eliminate the failover relationship from both sides, select the *Disable Mutual Failover* option.

If this is a mutual failover configuration, and you de-select the *Disable Mutual Failover* option, the failover configuration becomes active-passive. The first server listed will become the primary server and will be protected while the second server listed will become the secondary server and will not be protected anymore.

Resuming backups after failover/failback

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

While failover and failback are transparent for the COPAN 400 server, after failover/failback occurs, you may need to take some action in your backup application in order for it to work properly with COPAN 400. The action you take varies by backup application and operating system. We have described some of the actions we have used. Your environment may differ. Refer to the documentation that came with your backup application for more details.

Atempo 4.2

To resume a job after failover or failback:

1. While failover is triggered, wait for three minutes.
2. Reboot the Atempo client machine.
3. Manually move the failed job tape from the drive to the slot.
4. Restart the failed job from the Atempo console.

BakBone NetVault™

- After failover/failback occurs, if the Windows Device Manager hangs, you must reboot your NetVault server. Once devices are visible by both the operating system and NetVault, if the NetVault job hangs while waiting to connect to the tape media, reboot your NetVault server.
- (Windows 2000) Sometimes after failover or failback, individual drives are shown as offline with a red dot indicator (as noted in the NetVault Device Manager) instead of being idle and having a green dot or having a tape in the drive. If this occurs, right-click the affected drive and select *Check*. It may take more than one scan for the drive to come back online.
- Sometimes after failover or failback, a drive may be online but tapes that were previously in the drive or in the slots are missing. This is caused by an interruption of I/O, which causes the software to lose barcodes. To resolve this, the library, drives, and tapes need a complete rescan. Right-click the library (in the NetVault Device Manager) and select *Open Door*. Wait a few moments and select *Close Door*. You should now see all tapes properly labeled and back in their respective drives and/or slots.

CommVault Galaxy™

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

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

CA ARCserve®

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

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

HP OpenView Storage Data Protector

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

IBM® Tivoli® Storage Manager

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

EMC NetWorker®

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

Symantec Backup Exec™

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

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

Veritas NetBackup™

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

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

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

Fibre Channel port behavior during failover

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

Sample environment

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

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

Before failover

Appliance A

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

Appliance B

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

Port status

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

When failover occurs

Server A fails over to B

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

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

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

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

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

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

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

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

Note that there are never any duplicate WWPN entries in the FC switch.

When recovery occurs

Server B stops takeover of server A

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

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

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

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

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

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

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

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

Note that there are never any duplicate WWPN entries in the FC switch.

IP address behavior during failover

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

Sample environment

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

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

After failover is configured

Appliance A

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

Appliance B

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

When failover occurs

Server A fails over to B

A1 and A2 are unloaded from server A.

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

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

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

Note that there are never any duplicate IP addresses.

When recovery occurs

Server B Stops Takeover of Server A

A1 and A2 are unloaded from server B.

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

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

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

Note that there are never any duplicate IP addresses.

Port swapping for Brocade switches

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

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

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

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

Note that if you are using an HP-UX 11iv3 client, you do not need to configure portswapping.

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

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

Notes:

- Before you begin, you need to install expect-5.43.0-5.1.x86_64.rpm from your Linux installation CD.
- Tape drive multi-pathing is not supported with port swapping. Even though you can configure COPAN 400 to assign one drive to two paths, failover will not be transparent, meaning that when the backup job fails, the client will need to be reconfigured to use the device from the second path.
- Port swapping scripts are not valid for older McData switches.
- Port swapping scripts used on HP and AIX platforms are not supported with Multi-ID HBAs. This means that HP and AIX clients will not be supported in a failover set configured for Multi-ID.

To configure port swapping:

1. If you haven't already done so, set up failover on your COPAN 400 server.
2. Verify that SSH is installed on both COPAN 400 servers (SSH is installed by default).
3. Set up switch zoning.
4. Build SSH host-based authentication between COPAN 400 servers and the Brocade switch.

To do this:

- SSH to the Brocade switch using the "root" user account. (The default password is: *password* but you should contact your IT administrator for your password.)
- On both COPAN 400 servers, run: ssh root@<switch IP address>. After logging in to the switch, exit from SSH. This step will populate COPAN 400 servers as "known hosts" to the Brocade switch.

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

5. Copy portswap.sh to both COPAN 400 servers and change its mode.

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

6. Copy port_enable_disable.sh to both COPAN 400 servers and change its mode.

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

7. Copy preRecovery.portswap to the primary server and rename.

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

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

8. Copy preTakeOver.portswap to the secondary server and rename.

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

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

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

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

10. Confirm switch port connection(s) and fill in the following information in preRecovery and preTakeOver accordingly:
    - Local IP address used by the ssh to connect to the switch. *Note for preRecovery only*: You must set LOCALIP to the local heartbeat IP address because the preRecovery script will be called when the primary IP address is not ready. LOCALIP is set automatically in the preTakeOver script.
    - Password of root user for switch(es).
    - IP address for switch(es).
    - Area ID. If no area ID, put any one of the ports to be swapped.
    - All ports to be swapped, one pair after another.

Note: You will need one portswap line for each switch.

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

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

13. Take x-rays of COPAN 400 servers for your records.

HP-UX

HP-UX is very sensitive to "target ID", not only switch port ID but also the COPAN 400 target port's hard_loop ID. If the target is using loop mode, the hard_loop ID for the target port and its standby port must match. The default HBA BIOS setting will not provide you a pair of identical hard_loop IDs.

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

For Brocade 3900 and 4100 switches, area_id must be one of the port IDs that will swap.

```
portswap.sh normal $LOCALIP <switch IP> <switch password> <area id>
<port1> <port2> <port3> <port4> ... &
```

For example:

```
portswap.sh swapped $LOCALIP 10.1.1.60 switch_password 10 10 11 2 5 &
```

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

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

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

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

```
portswap.sh normal $LOCALIP 10.1.1.60 switch_password 10 10 11 2 5
portswap.sh normal $LOCALIP 10.1.1.70 switch_password 12 12 13 &
```

PreTakeOver script

The following is a sample preTakeOver script:

```
#!/bin/sh

logger -p daemon.notice preTakeOver: start

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

```
portswap.sh normal $LOCALIP xx.xx.xx.xx switch_password area_xx port1
port2 &
sleep 10

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

PreRecovery script

The following is a sample preRecovery script:

```
#!/bin/sh

logger -p daemon.notice preRecovery: start

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

portswap.sh swapped $LOCALIP xx.xx.xx.xx switch_password area_xx port1
port2 &
sleep 10

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

Data Replication

Replicating data protects the information on a virtual tape by maintaining a copy of the virtual tape on the same COPAN 400 server or on another COPAN 400 server.

There are three methods to replicate data in COPAN 400; 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.

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 can be 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.

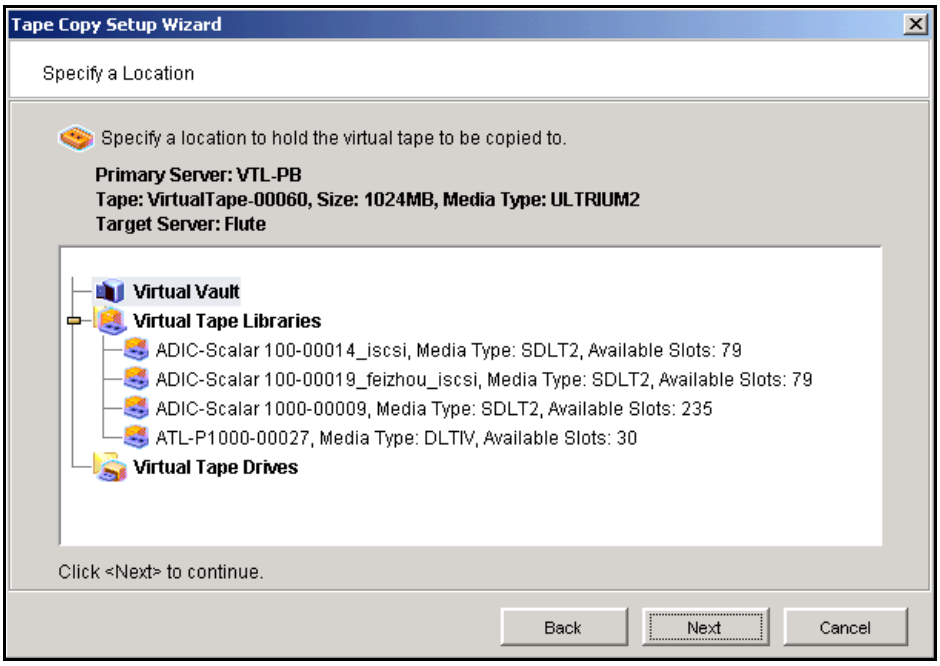
Remote Copy

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 tape that is configured for replication or *Auto Replication/Auto Archive*.

1. Right-click a tape and select *Remote Copy*.
2. Select if you want to copy to a local or remote server.

   If you select to copy to a remote server, you will have to select the server. If the server you want does not appear on the list, click the *Add* button.
3. Confirm/enter the target server's IP address.
4. Select a location for the copied tape.



   You can select a tape library or the virtual vault.

   If you select a tape library, the media must be compatible.
5. Confirm that all information is correct and then click *Finish* to create the copy.

Replication of virtual tapes

Replication is a process that protects the information on a virtual tape by maintaining a copy of a virtual tape on the same COPAN 400 server or on another COPAN 400 server.

At prescribed intervals, when the tape is not in use, changed data from the *primary* virtual tape on the source server is transmitted to the *replica resource* on the target server so that they are synchronized. The target COPAN 400 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.

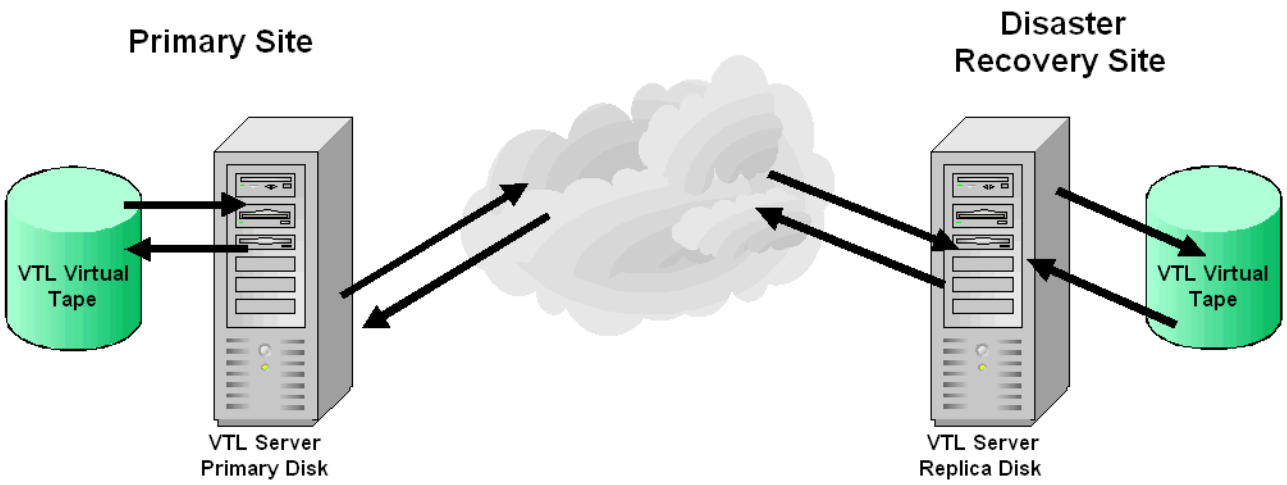
If a disaster occurs and the replica is needed, the administrator can *promote* the replica to become the primary virtual tape so that clients can access it.

COPAN 400 offers two types of replication, *Remote Replication* and *Local Replication*.

Remote Replication

Remote Replication allows fast, data synchronization of storage volumes from one COPAN 400 server to another over the IP network.

With Remote Replication, the replica disk is located on a separate target COPAN 400 server.

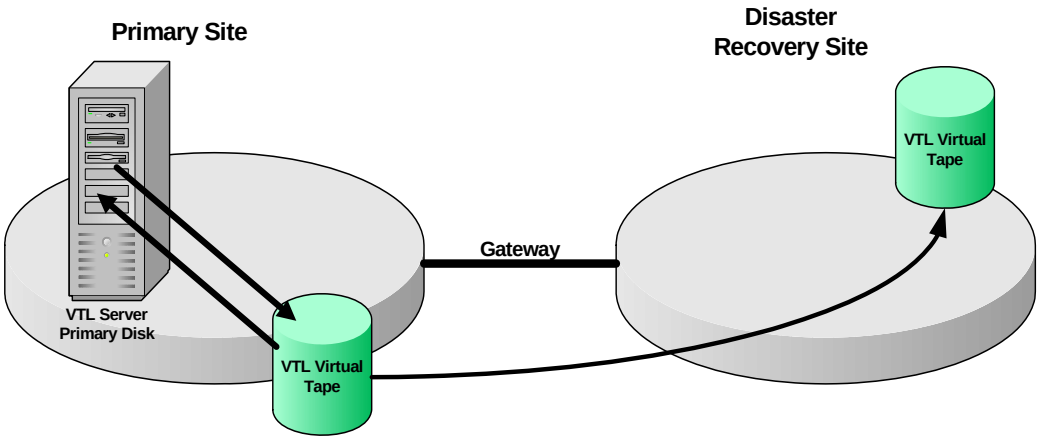


Local Replication

Local Replication allows fast, data synchronization of storage volumes within one COPAN 400 server. Because there is only one COPAN 400 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 COPAN 400 server via a gateway using edge routers or protocol converters.


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

Replication requirements

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

- (Remote Replication) You must have two COPAN 400 servers.
- (Remote Replication) You must have administrative rights on both servers.
- (Remote Replication) An IP connection is required for replication of virtual tapes (even if you are using Fibre Channel for replication).
- You must have enough space on the target server for the replica resource.

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 COPAN 400 appliance, you must do so before configuring replication.

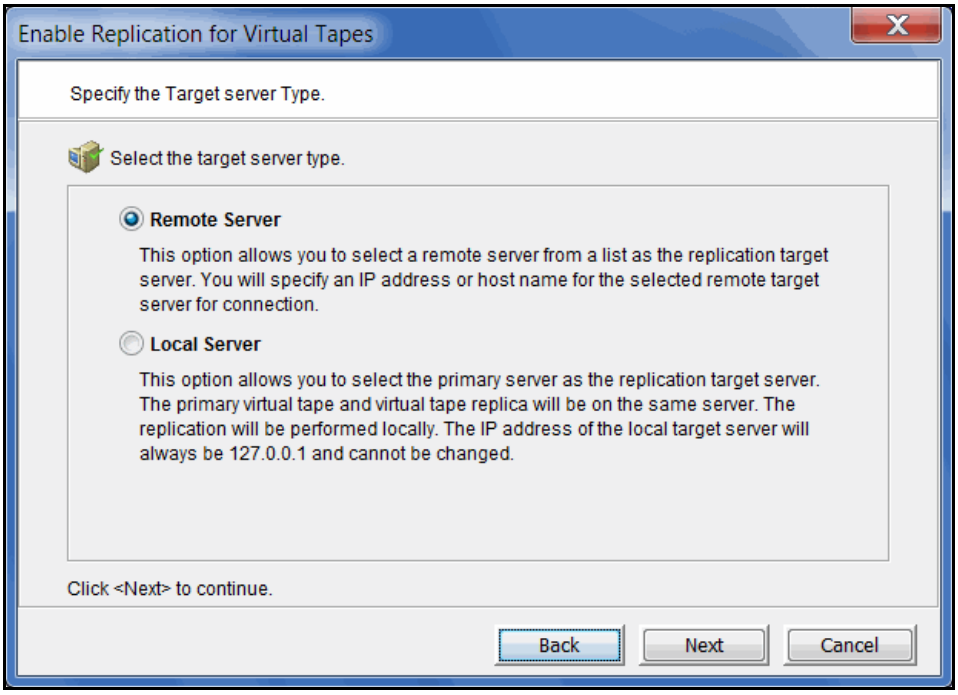
1. Right-click one or more virtual tapes in a virtual tape library or in the virtual vault and select *Replication --> Add*.

   You can also right-click the virtual tape library and select *Replication --> Add.*

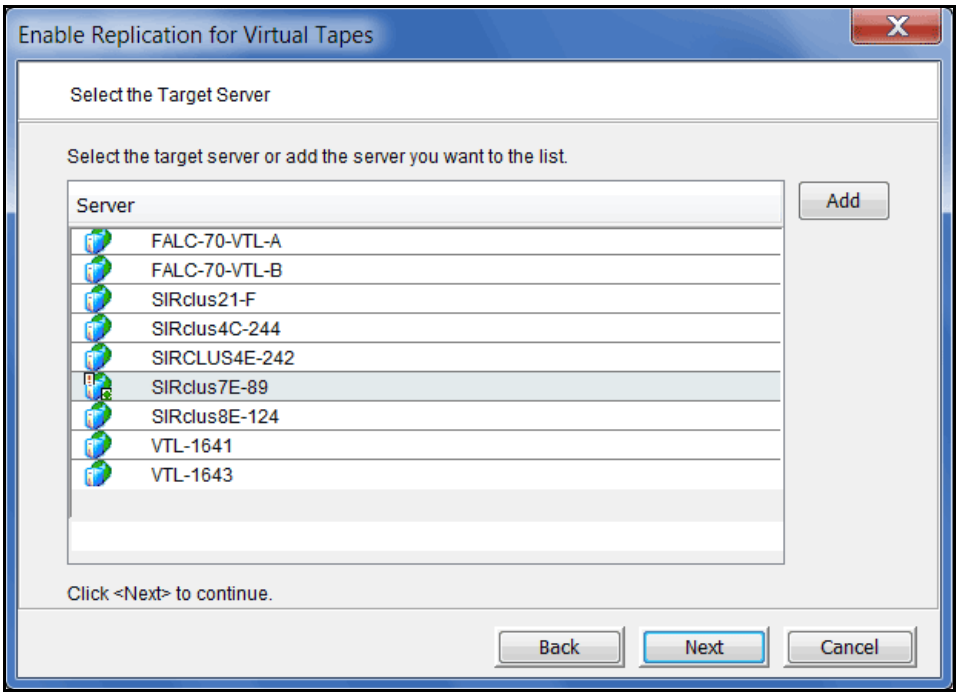
   Each virtual tape can only have one replica resource.

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

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

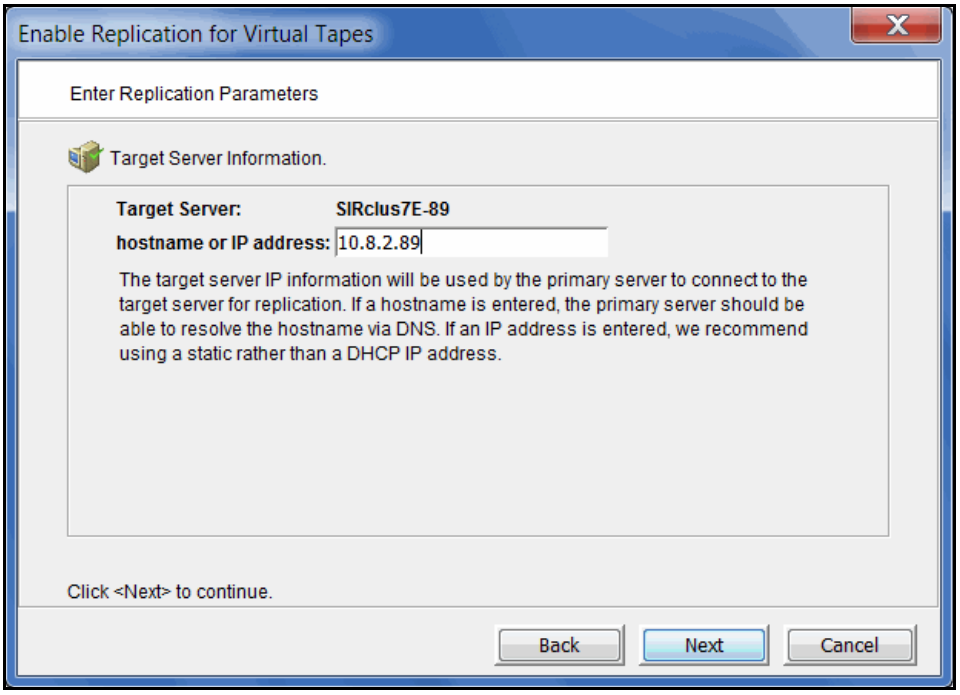


3. Select the server that will contain the replica.

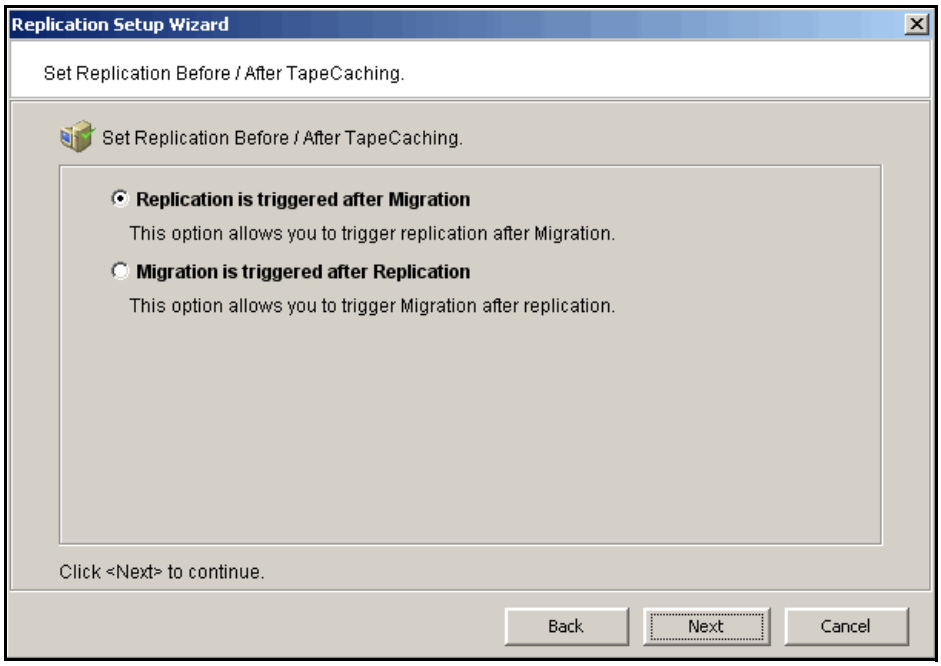


If the server you want does not appear on the list, click the *Add* button.

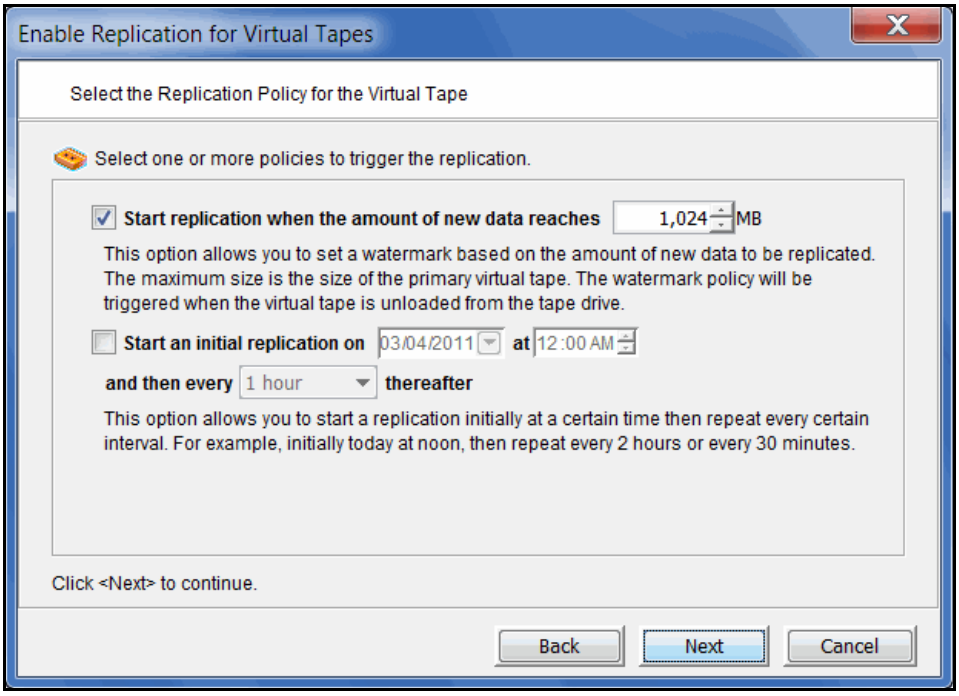
4. Confirm/enter the target server's IP address.



5. (Tape caching is enabled for these tapes) Configure when replication should occur.



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



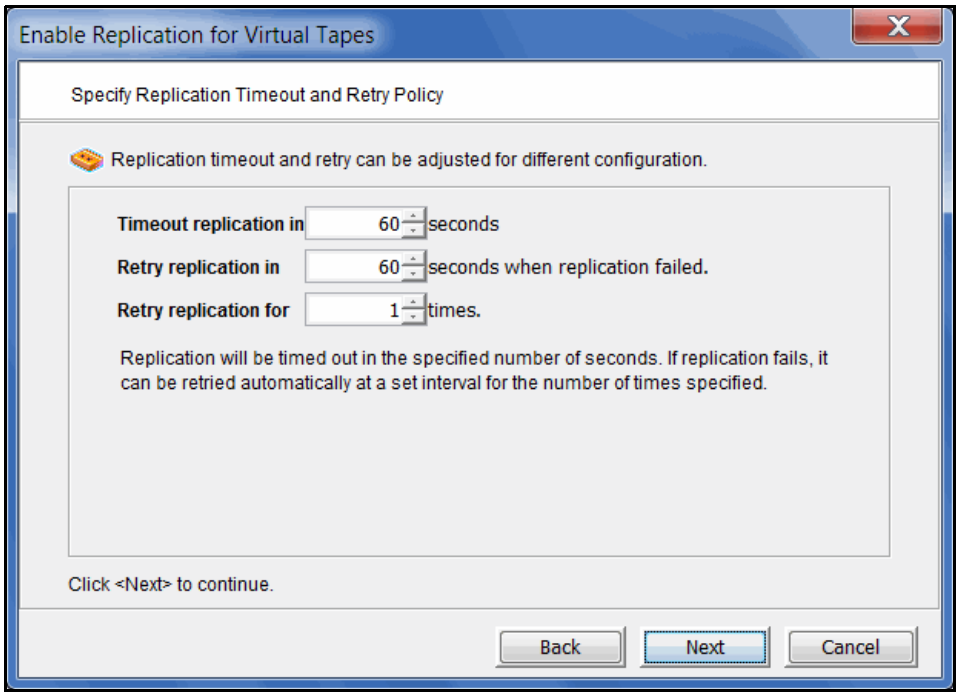
You must select at least one policy, but you can have multiple.

Start replication when the amount of new data reaches - If you enter a watermark value, when the value is reached, replication of the changed data will begin as soon as the virtual tape is ejected from the tape drive after backup.

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

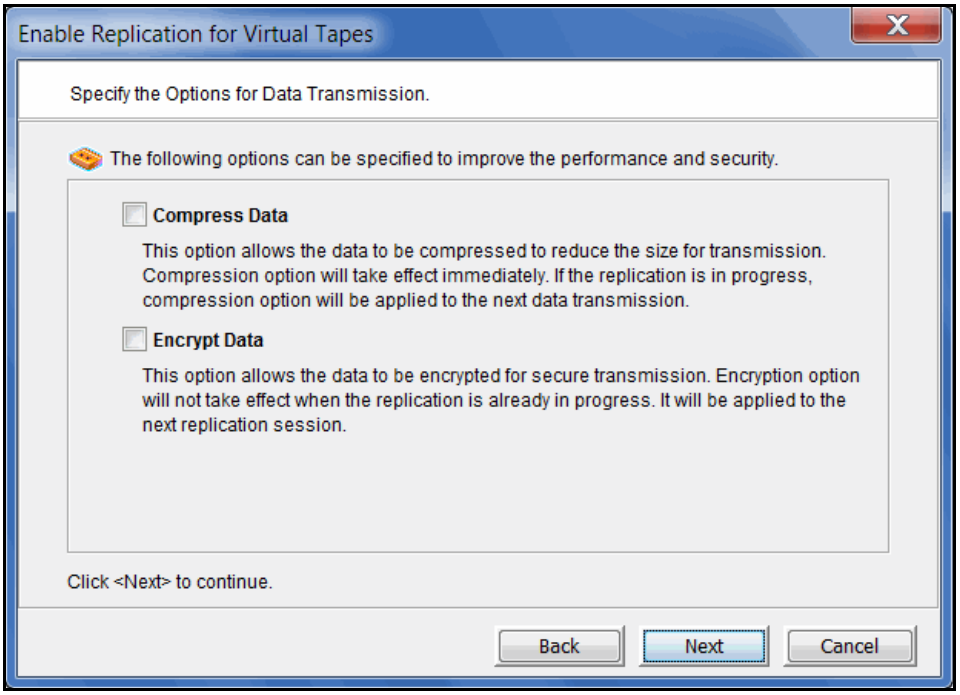
If a replication is already occurring when the next time interval is reached, the new replication request will be ignored.

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



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

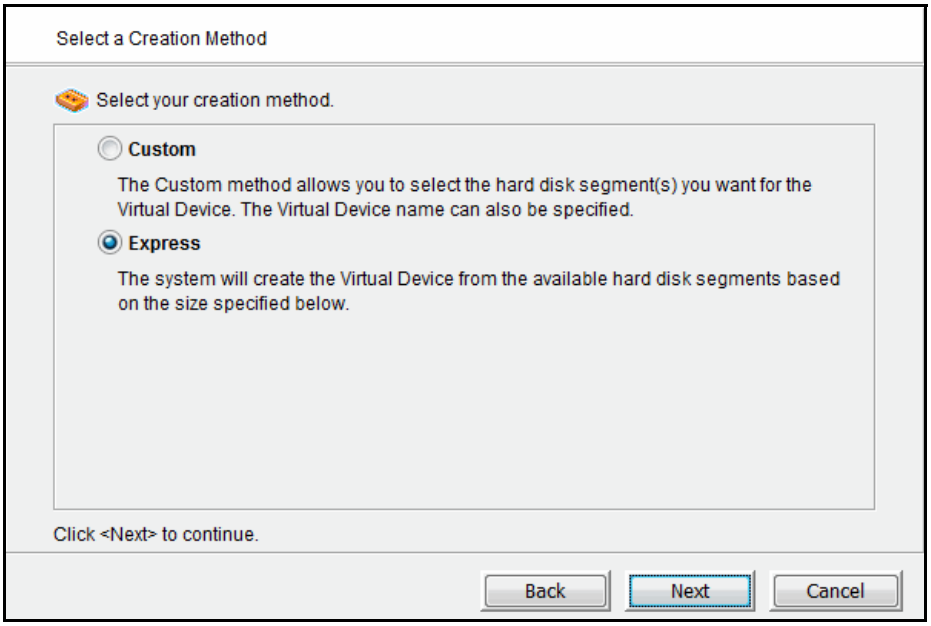
8. (Remote Replication only) Indicate if you want to use *Compression* and/or *Encryption*.



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

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

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

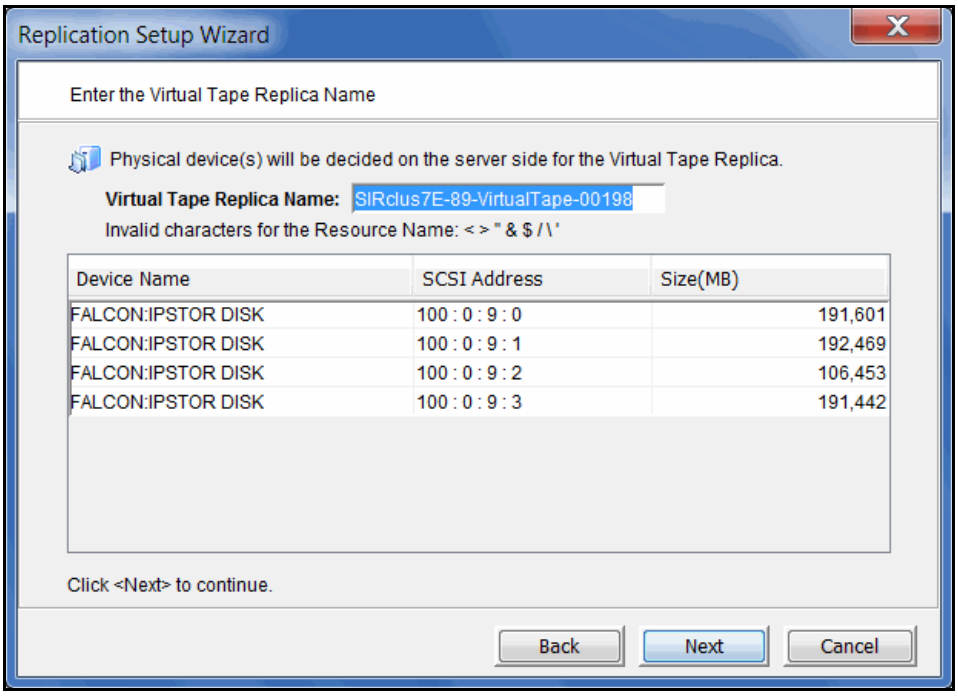


Custom lets you select which physical device(s) to use.

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

The replica resource will be created on the target replica server the first time replication is triggered for this tape.

10. (Local Replication only) Enter a name for the replica resource.



The name is not case sensitive.

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

Check replication status

There are several ways to check replication status:

- *Replication* tab of the primary virtual tape - displays information about the target replica server, the policies set for replication, and the replication status.
- *General* tab of the Replica Resource on the target server - displays status of replication in progress.
- Event Log of a server - 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).

Replication performance

You can set global replication options that affect bandwidth during replication on COPAN 400 servers. To do this:

1. Right-click a server and select *Properties*.

2. On the *Performance* tab, enter the maximum number of KBs per second that should be used for bandwidth.

   You can limit the amount of available network bandwidth that is used for replication on the source server side. Transmission will not exceed the set value. This is a global server parameter and affects all resources.

   Once enabled, the default is 10 KBs per second. If throttling is not used, the maximum bandwidth that is available will be used. Besides 0, valid input is 10-1,000,000 KB/s (1G).

Promote a replica resource

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

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

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

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

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

Change your replication configuration options

You can change the following for your replication configuration:

- Static IP address of your target server
- Policies that trigger replication (watermark, interval, time)
- Timeout and retry policies
- Data transmission options (encryption, compression)

To change the configuration:

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

Suspend/resume replication schedule

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

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

Stop a replication in progress

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

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

Remove a replication configuration

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.

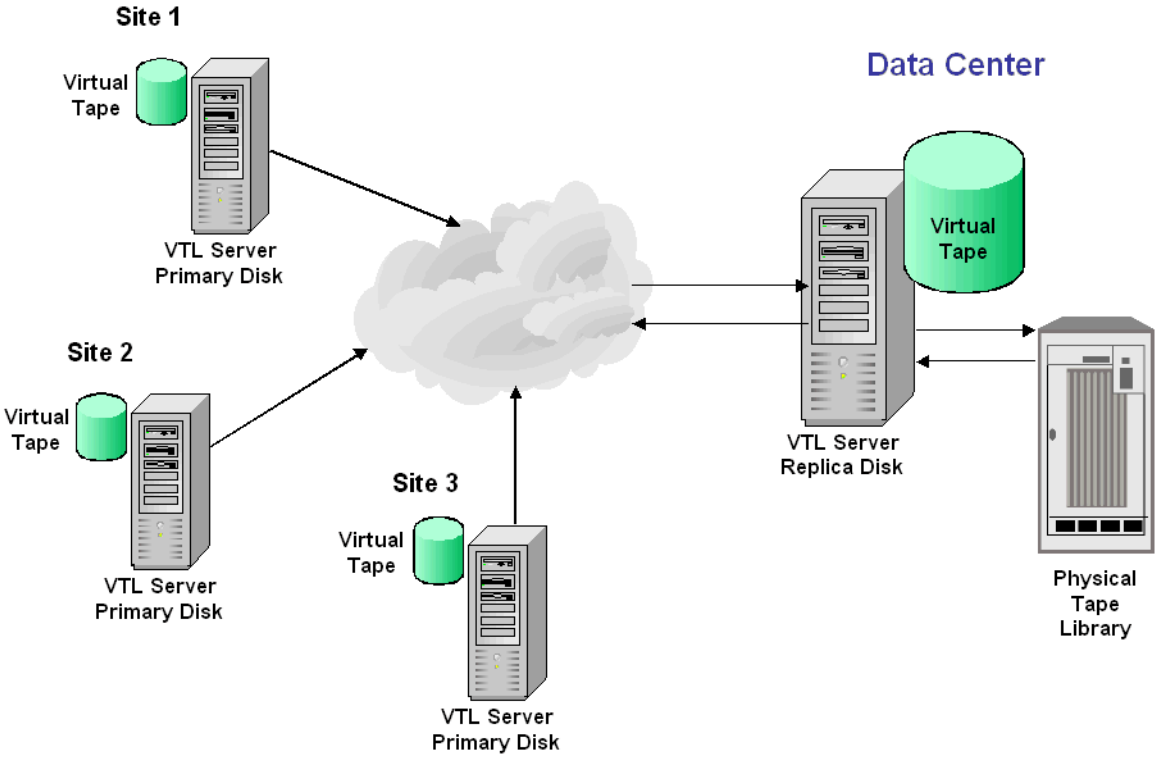
1. Right-click the primary virtual tape and select *Replication --> Remove*.
2. Determine if you want to promote or delete the replica.
3. If deleting, confirm that you want to remove the replica.

Replication and Failover

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

If you use the console to manually initiate take over of a primary server and then stop the take over while a replication job is running, you will need to “stop” the replication job before restarting it.

Consolidate tapes from multiple locations to a single data center



The following information is for environments with multiple COPAN 400 locations *without* physical tape libraries that replicate tape data to a remote COPAN 400 server that *has* a physical tape library that supports barcodes.

In this environment, if you will be exporting tapes from the remote COPAN 400 server to the physical tape library, you want to make sure that when you create tapes on the primary servers (at the multiple COPAN 400 locations *without* physical tape libraries), you match the barcodes of the tapes on the physical library attached to the target server.

Reports

COPAN 400 provides a wide variety of pre-defined reports that help you manage your COPAN 400 servers. Some reports focus on server conditions and individual hardware component configuration and behavior, such as disk space usage, physical resource allocation, and Fibre Channel configuration. Others are related to COPAN 400 features and gather comprehensive status information about virtual tapes and libraries and replication.

You can generate all reports from the *Reports* object in the SGI Management Console navigation tree. Below the *Reports* object is the *Scheduled Reports* object, which lets you schedule some of these reports to run repeatedly.

If you have configured a multi-node group, the *Group Reports* object is available under the group object. Reports generated from this object reflect only the servers in the group.

The report wizard displayed from each object lets you choose a report to create and select report-specific views and options to refine displayed data.

You can also set general report properties such as whether all or selected reports should be emailed and how long to retain them on the server.

Report types

Reports are available for these categories:

Libraries and tapes	• Import/Export Jobs • LUNs • Physical Tape Usage • Virtual Library Information • Virtual Tape Activity • Virtual Tape Information
Replication	• Replication Status
SAN Clients	• Virtual Library and Drive Assignment
Physical resources	• Disk Space Allocation for Virtual Tapes in Libraries • Disk Space Usage History • Fibre Channel Adapters Configuration • Physical Resource Allocation • Physical Resources Configuration
Performance	• SCSI Device Throughput • SCSI/Fibre Channel Throughput • COPAN 400 Performance

Create a report

Create a one-time report

Each report can be created for a specific server and will run only once.

1. To create a report, right-click the *Reports* object and select *New*.
2. Select a report type.
3. If applicable, choose the period of time to include in the report and other selection criteria, based on server dates:
   - *Today* - activity for the current server date
   - *Yesterday* - activity for the day prior to the current server date
   - *Past 7 days* - activity for the 7 days prior to the current server date
   - *Past 30 days* - activity for the 30 days prior to the current server date
   - *Past 365 days* - activity for the 365 days prior to the current server date
   - *Date range* - specify a beginning and end date within the 365 days prior to the current server date.
4. If applicable, choose the interval between data points in the report or, depending on the type of report, the interval represented by a bar in a bar chart. This can be an hour, a day, a week, a month, or a quarter. Depending on the report, the data point/bar can represent one of the following:
   - an average of the data measured during the interval
   - the total data measured during the interval
   - the total measured as of a specific point in time

   Note: When selecting an interval value for a report, consider the length of time the server or cluster has been in operation. Do not select an interval that is larger than that period of time. For instance, if your system has not been in operation for at least three months prior to the date on which you are creating the report, do not choose the *quarter* interval.
5. If applicable, indicate what items to include in the report, such as specific tape libraries/drives, physical resources, barcodes, tape locations, adapters, devices, and/or SCSI devices.
6. Enter a name for the report.
7. 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 and specify a format (.txt, .csv, .pdf, .xls, .html) for the report attachment.
8. Confirm all information and click *Finish* to create the report.

Schedule a report

You can schedule most reports to run at regular intervals. To do this:

1. Right-click the *Scheduled Reports* object under *Reports* and select *New*.
2. Select a report.
3. Set the schedule for how often this report should run.

   You can 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 the frequency (in hours).
4. Depending upon which report you select, additional windows appear to allow you to filter the information it will include.

   For instance, set the date or date range for the report and select display options, as described for one-time reports.
5. Enter a name for the report.
6. If email is configured for reports, provide email options.
7. Confirm all information and click *Finish* to create the schedule.

Create a group report

When you have configured a multi-node group, the *Group Reports* object is available below the group object.

1. Right-click the *Group Reports* object under the group object and select *New*.
2. Choose one of the two group report options:

   Regular Report - All standard reports are available. The report will be generated for specified servers in the group. In the console, the report will be listed below the *Reports* object for each individual server.

   Consolidated Report - Generates only the *Group Disk Space Usage Report*, which will collect disk space usage information from all servers in the group and present it in a single report that will be listed below the *Group Reports* object.
3. For a *Regular Report*, choose the report you want to create and the period of time and options for data you want the report to include.

   There are no options for the *Consolidated Report*. By default, data will be based on the current server date and all servers are included.
4. Enter a name for the report.
5. If email is configured for reports, provide email options.
6. For a *Regular Report*, select the servers for which you want to generate the report.
7. Confirm all information and click *Finish* to create the report.

View a report

After a report is created, it is categorized by report category in the tree. Expand the *Reports* (or *Group Reports*) object and (when applicable) the report category to see existing reports.

When you select an existing report in the tree, the report is displayed in the right-hand pane. In every report, the server name appears in the upper left corner and the date on which the report was created appears in the upper right corner. The period of time represented in the report is displayed below the report title. Any display options appear below the report table.

Manage reports

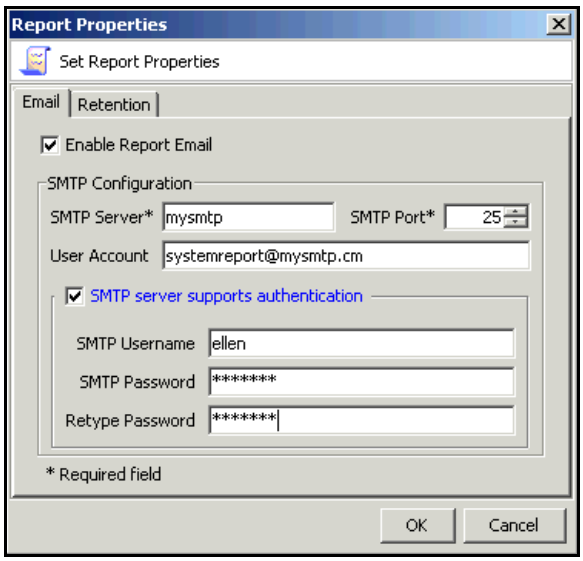
Set report properties

You can set email and retention properties for all or individual 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.



SMTP Server - Specify the mail server that should be used. You can enter an IP address or hostname consisting of alphabet letters, numbers, "_", "-", or ".". The maximum length is 255 characters.

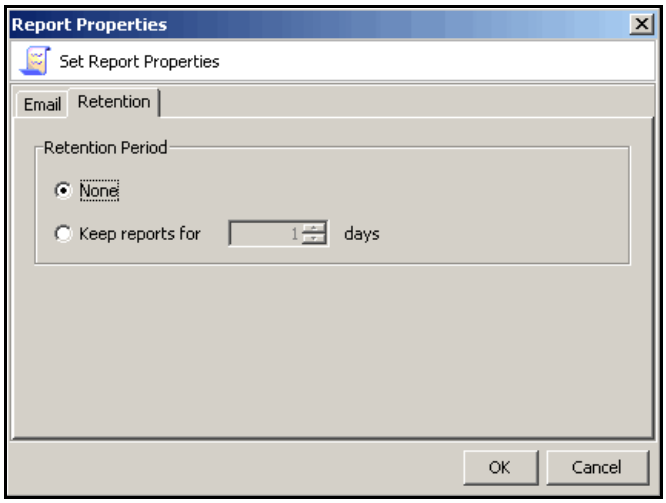
SMTP Port - Specify the mail server port that should be used.

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.



Export data from a report

You can export a report from the server to another location. To do this, right-click a generated report object and select *Export,* then choose from one of the available formats: comma delimited (.csv), tab delimited (.txt) text, Excel spreadsheet (.xls), PDF (.pdf), web page(.html, a .zip file is created).

Email a report

In order to be able to email a report, email properties for reports must be configured before you create the report (refer to 'Set report properties'). If this has been done, you can set the report to be emailed in the Reports 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 displayed reports. 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.*

Print a report

You can print individual reports. To do this, right-click an existing report and select *Print.*

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.

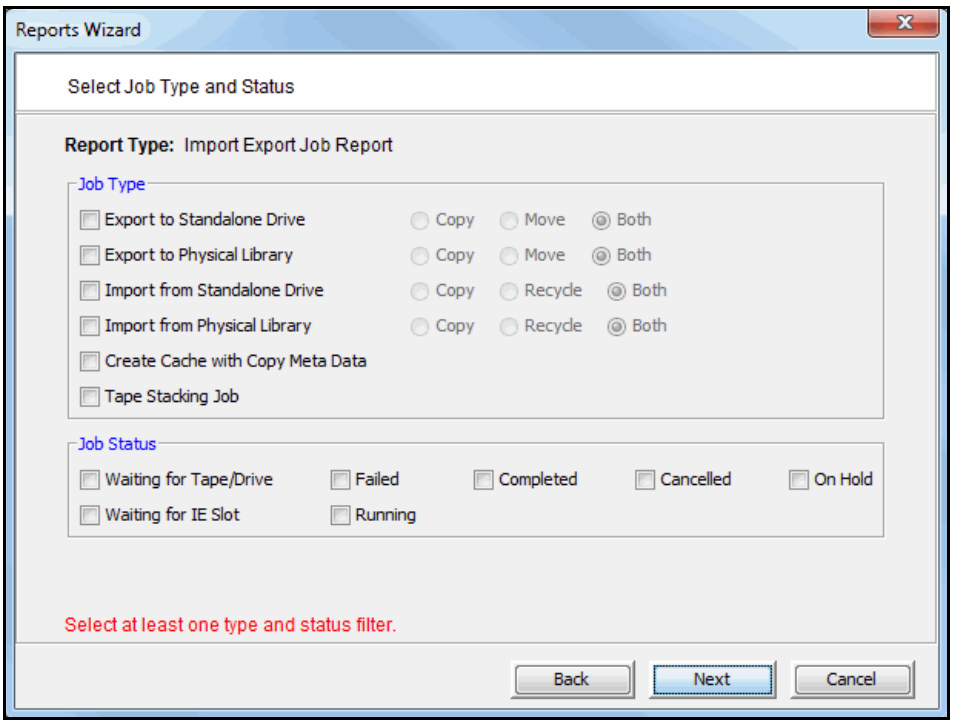
Reports and Failover

Reports cannot be generated from a server when it is in a failed state (the server name is displayed in red in the management console). After failback, reports generated from the original node can include data generated during the failover period, as long as the specified report dates include that period of time.

Reports for libraries and tapes

Import/Export Jobs

This history report lists all import/export and tape caching jobs that were placed in the queue during the specified period of time, regardless of job status. An option screen in the wizard includes the possible job types and statuses.



You must select at least one job type and one job status.

Job type

- Export to Standalone Drive/Export to Physical Library - For these jobs, you can include results for jobs that used *Copy Mode*, *Move Mode*, or both.
- Import from Standalone Drive/Import from Physical Library - For these jobs, you can include results for jobs that used *Copy Mode*, *Recycle Mode*, or both.

Job status

For all selected job types, the report will include information on jobs with the selected status(es).

The summary page displays the number of jobs found for all job types and all job statuses.

VTL-1643 06/03/2011 17:34

Import Export Job Report

05/04/2011 00:00 - 06/02/2011 23:59

	Running	Failed	Completed	Cancelled	On Hold	Waiting for Tape/Drive	Waiting for I/E Slot
Export to Standalone Drive	0	0	0	0	0	0	0
Export to Physical Library	0	0	20	0	0	3	0
Import from Standalone Drive	0	0	0	0	0	0	-
Import from Physical Library	0	0	0	0	0	0	-
Create Cache with Copy Meta Data	0	0	0	0	0	0	-
Tape Stacking	0	0	0	0	0	0	0

The detail pages display results based on the job type(s) and job status(es) you selected. Jobs are ordered by job ID. For each job, the report lists job ID, the job type, barcodes of source/destination tapes; locations of source/destination tapes, import/export mode, job status, start/end time of job, amount of data transferred, and job throughput.

VTL-1643 06/03/2011 17:34

Import Export Job Report

05/04/2011 00:00 - 06/02/2011 23:59

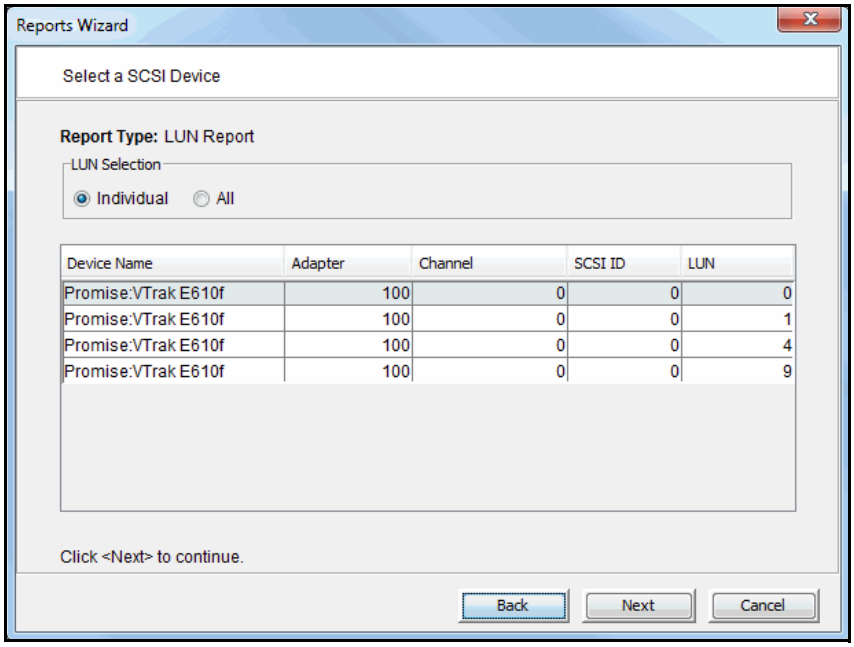
Job Id	Type	From Tape / To Tape	From Location / To Location	Mode	Status	Start Time / End Time	Transfer (MB)	Throughput (MB/sec)
2790	Export	286400L1	Vault	Copy	Completed	05/19/2011 12:42	2,243	20
		286400L1	PLIB: 375			05/19/2011 12:44		
2791	Export	286400L1	Vault	Copy	Completed	05/19/2011 22:44	2,456	21
		286400L1	PLIB: 375			05/19/2011 22:46		
2792	Export	286400L1	Vault	Copy	Completed	05/20/2011 00:45	2,459	21
		286400L1	PLIB: 375			05/20/2011 00:47		
2793	Export	286400L1	Vault	Copy	Completed	05/20/2011 02:45	2,462	22
		286400L1	PLIB: 375			05/20/2011 02:47		
2794	Export	286400L1	Vault	Copy	Completed	05/20/2011 04:46	2,465	21
		286400L1	PLIB: 375			05/20/2011 04:48		
2795	Export	286400L1	Vault	Copy	Completed	05/20/2011 06:46	2,263	20
		286400L1	PLIB: 375			05/20/2011 06:48		
2796	Export	286400L1	Vault	Copy	Completed	05/20/2011 08:46	2,266	21
		286400L1	PLIB: 375			05/20/2011 08:48		
2813	Export	286400L1	Vault	Copy	Waiting for Tape/Drive	05/21/2011 19:01	0	0
		286400L1	PLIB: 375					
2852	Export	286401L1	Vault	Copy	Waiting for Tape/Drive	05/24/2011 23:12	0	0
		286401L1	PLIB: 375					
2883	Export	286402L1	Vault	Copy	Waiting for Tape/Drive	05/27/2011 11:28	0	0
		286402L1	PLIB: 375					

Type: Export to Standalone Drive, Export to Physical Library, Import from Standalone Drive, Import from Physical Library, Create Cache with Copy Meta Data, Tape Stacking
Status: Running, Completed, Waiting for Tape/Drive, Waiting for I/E Slot

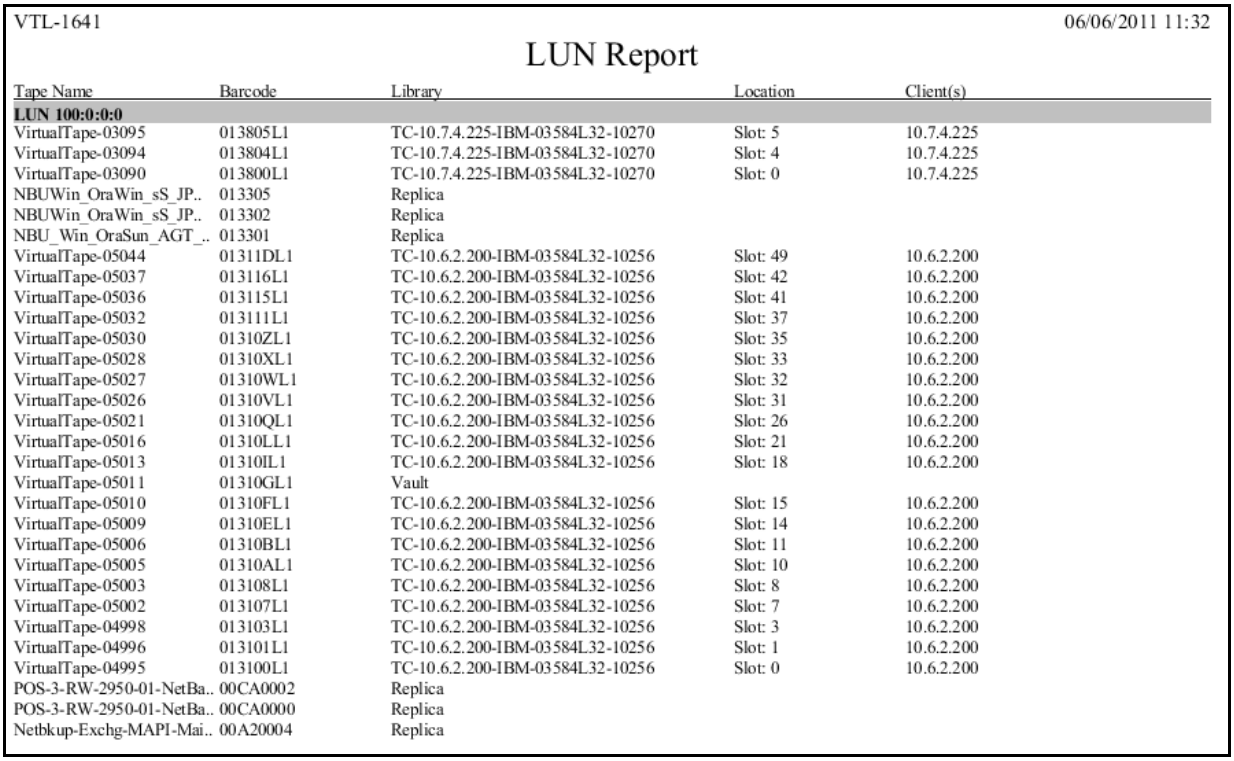
3 / 3

LUNs

This status report displays all virtual tapes that are currently allocated on all or specified LUNs. In the wizard, click *Individual* and select the device(s) you want to include in the report, or click *All* to include all devices (device selection is not necessary).



Results include the tape name and barcode, the library to which it belongs (including whether the tape is a replica resource or is in the vault), its current location, and assigned clients.



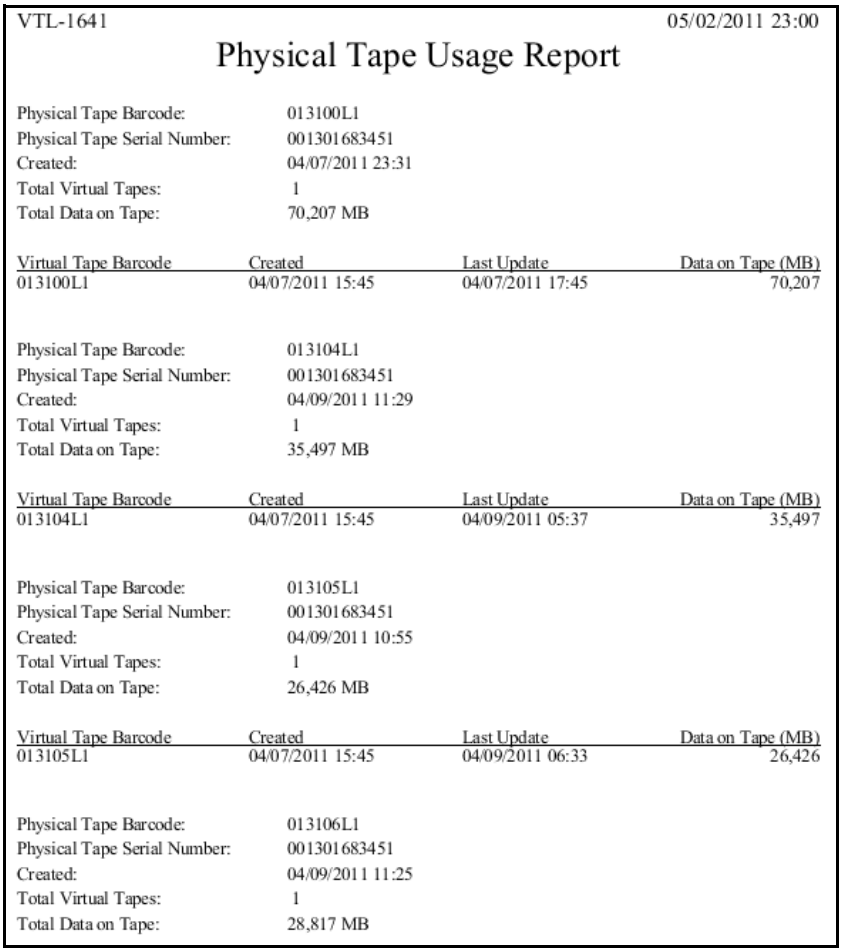
VTL-1641 06/06/2011 11:32

LUN Report

Tape Name	Barcode	Library	Location	Client(s)
LUN 100:0:0:0				
VirtualTape-03095	013805L1	TC-10.7.4.225-IBM-03584L32-10270	Slot: 5	10.7.4.225
VirtualTape-03094	013804L1	TC-10.7.4.225-IBM-03584L32-10270	Slot: 4	10.7.4.225
VirtualTape-03090	013800L1	TC-10.7.4.225-IBM-03584L32-10270	Slot: 0	10.7.4.225
NBUWin_OraWin_sS_JP..	013305	Replica		
NBUWin_OraWin_sS_JP..	013302	Replica		
NBU_Win_OraSun_AGT_..	013301	Replica		
VirtualTape-05044	01311DL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 49	10.6.2.200
VirtualTape-05037	013116L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 42	10.6.2.200
VirtualTape-05036	013115L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 41	10.6.2.200
VirtualTape-05032	013111L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 37	10.6.2.200
VirtualTape-05030	01310ZL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 35	10.6.2.200
VirtualTape-05028	01310XL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 33	10.6.2.200
VirtualTape-05027	01310WL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 32	10.6.2.200
VirtualTape-05026	01310VL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 31	10.6.2.200
VirtualTape-05021	01310QL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 26	10.6.2.200
VirtualTape-05016	01310LL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 21	10.6.2.200
VirtualTape-05013	01310IL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 18	10.6.2.200
VirtualTape-05011	01310GL1	Vault		
VirtualTape-05010	01310FL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 15	10.6.2.200
VirtualTape-05009	01310EL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 14	10.6.2.200
VirtualTape-05006	01310BL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 11	10.6.2.200
VirtualTape-05005	01310AL1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 10	10.6.2.200
VirtualTape-05003	013108L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 8	10.6.2.200
VirtualTape-05002	013107L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 7	10.6.2.200
VirtualTape-04998	013103L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 3	10.6.2.200
VirtualTape-04996	013101L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 1	10.6.2.200
VirtualTape-04995	013100L1	TC-10.6.2.200-IBM-03584L32-10256	Slot: 0	10.6.2.200
POS-3-RW-2950-01-NetBa..	00CA0002	Replica		
POS-3-RW-2950-01-NetBa..	00CA0000	Replica		
Netbkup-Exchg-MAPI-Mai..	00A20004	Replica		

Physical Tape Usage

This status report displays information about how each physical tape in the physical tape database is mapped to a virtual tape, including barcode, serial number, creation date, the number of virtual tapes configured from the physical tape, and the total amount of data on the tape. The date/time of the most recent update to the tape is also displayed. Tapes without data are not included in report results.



VTL-1641 05/02/2011 23:00

Physical Tape Usage Report

Physical Tape Barcode: 013100L1
Physical Tape Serial Number: 001301683451
Created: 04/07/2011 23:31
Total Virtual Tapes: 1
Total Data on Tape: 70,207 MB

Virtual Tape Barcode	Created	Last Update	Data on Tape (MB)
013100L1	04/07/2011 15:45	04/07/2011 17:45	70,207

Physical Tape Barcode: 013104L1
Physical Tape Serial Number: 001301683451
Created: 04/09/2011 11:29
Total Virtual Tapes: 1
Total Data on Tape: 35,497 MB

Virtual Tape Barcode	Created	Last Update	Data on Tape (MB)
013104L1	04/07/2011 15:45	04/09/2011 05:37	35,497

Physical Tape Barcode: 013105L1
Physical Tape Serial Number: 001301683451
Created: 04/09/2011 10:55
Total Virtual Tapes: 1
Total Data on Tape: 26,426 MB

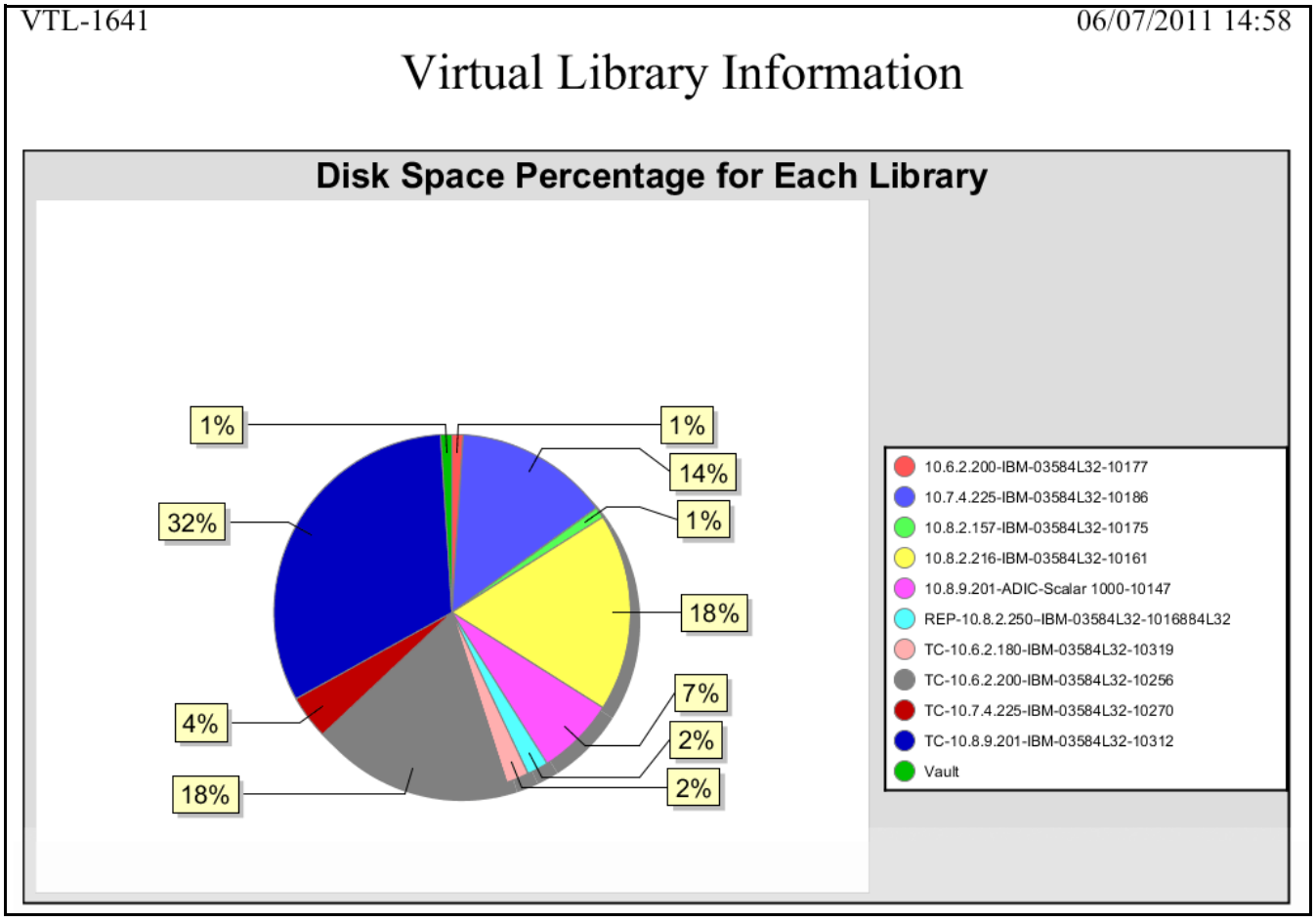
Virtual Tape Barcode	Created	Last Update	Data on Tape (MB)
013105L1	04/07/2011 15:45	04/09/2011 06:33	26,426

Physical Tape Barcode: 013106L1
Physical Tape Serial Number: 001301683451
Created: 04/09/2011 11:25
Total Virtual Tapes: 1
Total Data on Tape: 28,817 MB

Virtual Library Information

This status report displays information about each virtual tape library on the system, including the physical library it emulates, the amount of storage it occupies, and information about its drives, tapes, and slots. Results are displayed in a pie chart as well as in tabular format.

In the pie chart, the amount of disk space occupied by each library, including space occupied by the Virtual Vault, is displayed as a percentage of all available storage.



The results table lists all configured COPAN 400 libraries and for each one displays its name and virtual ID; the library and drive vendor/product it emulates; the number of drives, tapes, slots, and IE slots, the amount of storage it occupies, and its SAN IP address.

VTL-1641 06/07/2011 14:58

Virtual Library Information

Name	VID	Library Vendor:Product	Drive Vendor:Product	#Drives	#Tapes	#Slots	#IE Slots	Storage (MB)	SAN Client
10.6.2.200-IBM-03584L32-..	10177	IBM:03584L32	IBM:ULT3580-TD4	6	50	253	10	79,872	10.6.2.200
10.7.4.225-IBM-03584L32-..	10186	IBM:03584L32	IBM:ULT3580-TD3	6	100	253	10	987,136	10.7.4.225
10.8.2.157-IBM-03584L32-..	10175	IBM:03584L32	IBM:ULT3580-TD1	1	100	241	10	77,824	10.8.2.157
10.8.2.216-IBM-03584L32-..	10161	IBM:03584L32	IBM:ULT3580-TD3	6	200	253	10	1,323,008	
10.8.9.201-ADIC-Scalar 10..	10147	ADIC:Scalar	IBM:ULTRIUM-TD3	6	100	237	4	482,304	10.8.9.201
REP-10.8.2.250-IBM-03584.	10168	IBM:03584L32	IBM:ULT3580-TD2	6	100	253	10	164,864	
TC-10.6.2.180-IBM-03584..	10319	IBM:03584L32	IBM:ULT3580-TD1	50	50	253	10	128,000	
TC-10.6.2.200-IBM-03584..	10256	IBM:03584L32	IBM:ULT3580-TD1	6	48	253	10	1,304,576	10.6.2.200
TC-10.7.4.225-IBM-03584..	10270	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	260,096	10.7.4.225
TC-10.8.2.157-IBM-03584..	10284	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	0	
TC-10.8.2.157-IBM-03584..	10326	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	0	
TC-10.8.2.216-IBM-03584..	10298	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	0	10.8.2.216-SIR24G
TC-10.8.9.201-IBM-03584..	10312	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	2,357,248	10.8.9.201
TC-10.8.9.204-IBM-03584..	10333	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	0	
TC-10.8.9.208-IBM-03584..	10340	IBM:03584L32	IBM:ULT3580-TD1	6	50	253	10	1,024	
Vault		N/A	N/A	N/A	20	N/A	N/A	135,168	

This report does not include tape segments used for some types of internal tracking and processing when calculating used or allocated space.

Virtual Tape Activity

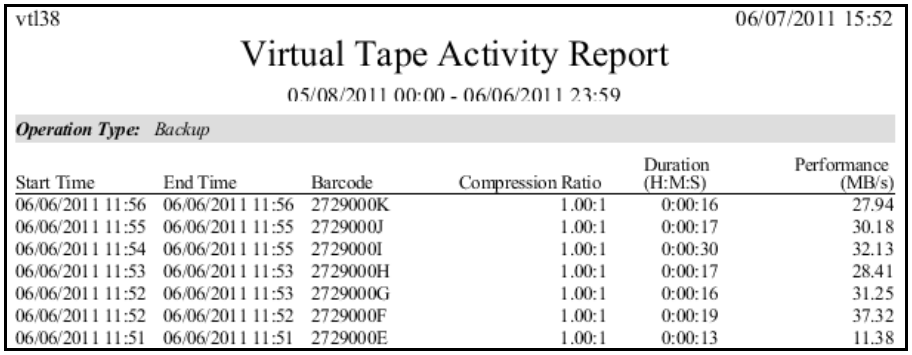
This history report shows activity for all virtual tapes within the specified period of time for three types of operations: Backup, Tape Import (*WRITE* operations), and Tape Export (*READ* operations).

You can filter report data by specifying barcode information: tapes within a specified bar code range, with a specified prefix, or containing a specified text string.

Regardless of the operation, the information for each report item includes the start and end time of the job, tape barcode, tape compression ratio, job duration, and the speed of the operation in megabytes per second.

Typical displays include:

- For backup operations,



vtl38 06/07/2011 15:52

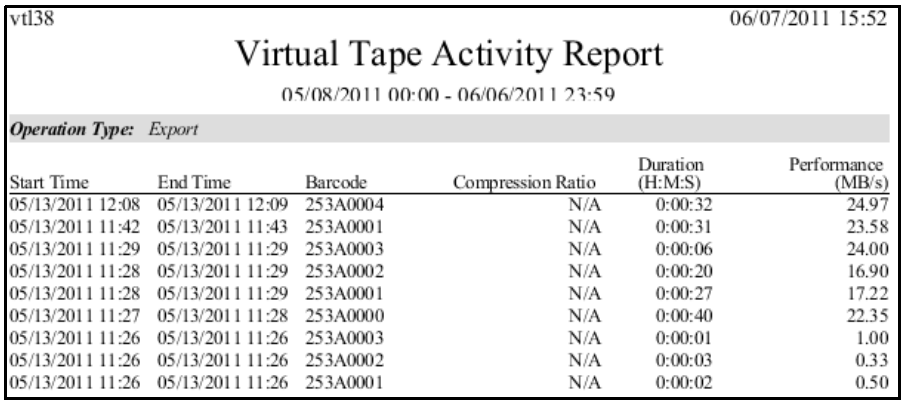
Virtual Tape Activity Report

05/08/2011 00:00 - 06/06/2011 23:59

Operation Type: *Backup*

Start Time	End Time	Barcode	Compression Ratio	Duration (H:M:S)	Performance (MB/s)
06/06/2011 11:56	06/06/2011 11:56	2729000K	1.00:1	0:00:16	27.94
06/06/2011 11:55	06/06/2011 11:55	2729000J	1.00:1	0:00:17	30.18
06/06/2011 11:54	06/06/2011 11:55	2729000I	1.00:1	0:00:30	32.13
06/06/2011 11:53	06/06/2011 11:53	2729000H	1.00:1	0:00:17	28.41
06/06/2011 11:52	06/06/2011 11:53	2729000G	1.00:1	0:00:16	31.25
06/06/2011 11:52	06/06/2011 11:52	2729000F	1.00:1	0:00:19	37.32
06/06/2011 11:51	06/06/2011 11:51	2729000E	1.00:1	0:00:13	11.38

- For export operations,



vtl38 06/07/2011 15:52

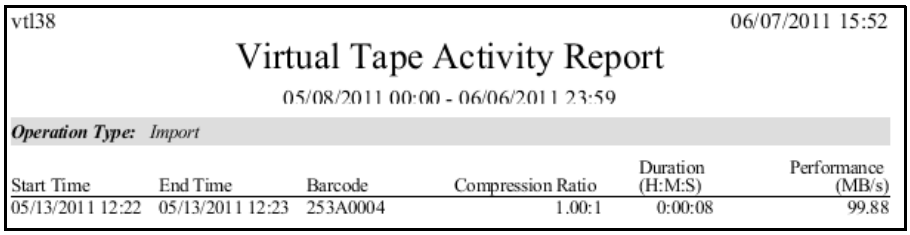
Virtual Tape Activity Report

05/08/2011 00:00 - 06/06/2011 23:59

Operation Type: *Export*

Start Time	End Time	Barcode	Compression Ratio	Duration (H:M:S)	Performance (MB/s)
05/13/2011 12:08	05/13/2011 12:09	253A0004	N/A	0:00:32	24.97
05/13/2011 11:42	05/13/2011 11:43	253A0001	N/A	0:00:31	23.58
05/13/2011 11:29	05/13/2011 11:29	253A0003	N/A	0:00:06	24.00
05/13/2011 11:28	05/13/2011 11:29	253A0002	N/A	0:00:20	16.90
05/13/2011 11:28	05/13/2011 11:29	253A0001	N/A	0:00:27	17.22
05/13/2011 11:27	05/13/2011 11:28	253A0000	N/A	0:00:40	22.35
05/13/2011 11:26	05/13/2011 11:26	253A0003	N/A	0:00:01	1.00
05/13/2011 11:26	05/13/2011 11:26	253A0002	N/A	0:00:03	0.33
05/13/2011 11:26	05/13/2011 11:26	253A0001	N/A	0:00:02	0.50

- For import operations,



vtl38 06/07/2011 15:52

Virtual Tape Activity Report

05/08/2011 00:00 - 06/06/2011 23:59

Operation Type: *Import*

Start Time	End Time	Barcode	Compression Ratio	Duration (H:M:S)	Performance (MB/s)
05/13/2011 12:22	05/13/2011 12:23	253A0004	1.00:1	0:00:08	99.88

Virtual Tape Information

This report displays the current status of all virtual tapes. The wizard lets you select the virtual tape libraries that you want to include; all libraries policies are selected by default. You can filter report data by specifying barcode information: tapes within a specified bar code range, with a specified prefix, or containing a specified text string.

Because of the amount of information available for virtual tapes, multiple sub-reports, referred to as *views*, present information related to a single COPAN 400 feature. In addition to the *Overall Summary*, you can choose the following: Tape Caching View, Replica Resources View, Vault View, and Detailed Tape View.

This report does not include tape segments used for some types of internal tracking and processing when calculating used or allocated space.

Overall Summary View

This view is selected by default. For each tape, the report displays the bar code; amount of data written; whether or not the tape is full; tape caching status; whether migration and replication are required; and tape location.

VTL-1641 06/07/2011 16

Virtual Tape Information Report

06/07/2011 00:00 - 06/07/2011 16:12

Overall Summary of Tapes

Barcode	Written (GB)	Tape Full	Caching Enabled	Needs Migration	Needs Deduplication	Needs Replication	Remote Export Configured	Tape Location	SIR Policy
013818L1	0.864	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
013819L1	0.862	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
01381AL1	0.873	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
01381BL1	0.829	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
01381CL1	0.828	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
01381DL1	0.972	Yes	Yes	Yes	Yes		No	TC-10.7.4.225-IBM-03584L32-1..	TC-10.7.4.225-IBM-03584L32-10270
013F00L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F01L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F02L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F03L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F04L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F05L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F06L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F07L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F08L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F09L1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0AL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0BL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0CL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0DL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0EL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0FL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0GL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284
013F0HL1	0.000	No	Yes	No	No		No	TC-10.8.2.157-IBM-03584L32-1..	TC-10.8.2.157-IBM-03584L32-10284

Filters
Barcode: All
Included libraries(id): All
Included policies(id): All
Views: Overall Summary, Deduplication View, Tape Caching View, Replica Resources View, Vault View, Detailed Tape View

Tape Caching View

This view displays information related to tape caching. For each tape, the report displays the library to which it belongs, its bar code, amount of data written, whether or not the tape is full, and whether migration is required.

VTL-1641 06/07/2011 16:12

Virtual Tape Information Report

06/07/2011 00:00 - 06/07/2011 16:12

Tape Caching View

Tape Library	Barcode	Written (GB)	Tape Full	Needs Migration	Needs Deduplication	SIR Policy
TC-10.8.2.216-IBM-03584L32-1..	014618L1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.2.216-IBM-03584L32-1..	014619L1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.2.216-IBM-03584L32-1..	01461AL1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.2.216-IBM-03584L32-1..	01461BL1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.2.216-IBM-03584L32-1..	01461CL1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.2.216-IBM-03584L32-1..	01461DL1	0.000	No	No	No	TC-10.8.2.216-IBM-03584L32-10298
TC-10.8.9.201-IBM-03584L32-1..	014D00L1	143.422	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D01L1	111.257	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D02L1	111.599	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D03L1	149.572	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D04L1	109.547	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D05L1	111.743	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D06L1	111.516	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D07L1	136.997	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D08L1	109.904	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D09L1	112.013	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0AL1	144.092	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0BL1	109.504	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0CL1	111.901	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0DL1	149.323	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0EL1	109.770	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0FL1	111.614	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0GL1	112.105	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312
TC-10.8.9.201-IBM-03584L32-1..	014D0HL1	145.051	Yes	Yes	Yes	TC-10.8.9.201-IBM-03584L32-10312

Filters
Barcode: All
Included libraries(id): All
Included policies(id): All
Views: Overall Summary, Deduplication View, Tape Caching View, Replica Resources View, Vault View, Detailed Tape View 163 / 221

Vault View

This view is similar to the *Overall Summary View*, with the exception that instead of *Tape Location*, this view identifies the library to which each tape belongs. For each tape, the report displays the bar code, amount of data written, whether or not the tape is full, whether tape caching is configured, whether migration or replication is required, and the parent library.

VTL-1641 06/07/2011 16:12

Virtual Tape Information Report

06/07/2011 00:00 - 06/07/2011 16:12

Vault View

Barcode	Written (GB)	Tape Full	Caching Enabled	Needs Migration	Needs Deduplication	Needs Replication	Remote Export Configured	Parent Library	SIR Policy
001B2ZL2	204.825	Yes	No				No	REP-10.8.2.250-Frankenstein-IB..	
01310GL1	79.099	No	No		Yes		No		TC-10.6.2.200-IBM-03584L32-10256
01310HL1	40.028	No	No		Yes		No		TC-10.6.2.200-IBM-03584L32-10256
7T0001RT	340.726	No	No				No		
7T8001RX	149.670	No	No				No		
7T8001RZ	227.679	No	No				No		
7T8001WF	0.000	No	No				No		
7T80021X	14.484	No	No				No		
7TA001RD	342.357	No	No				No		
7TC001T6	79.332	No	No				No		
7TE001PE	78.164	No	No				No		
7TG001QE	77.911	No	No				No		
7TI001S5	77.794	No	No				No		
7TK001Q8	406.823	No	No				No		
7TM001SV	346.958	No	No				No		
7TO001QT	342.888	No	No				No		
7TQ001RG	345.304	No	No				No		
7TQ00203	78.851	No	No				No		
7TS001S8	335.857	No	No				No		
7TU001QK	345.709	No	No				No		

Filters
Barcode: All
Included libraries(id): All
Included policies(id): All
Views: Overall Summary, Deduplication View, Tape Caching View, Replica Resources View, Vault View, Detailed Tape View 166 / 221

Replica Resources View

This view presents information for tapes that are displayed when you select the *Replica Resources* object in the console. For each tape, the report displays the bar code, allocation size, whether or not the tape is full, the source COPAN 400 server, and the tape ID.

VTL-1641 06/07/2011 16:12

Virtual Tape Information Report

06/07/2011 00:00 - 06/07/2011 16:12

Replica View

Barcode	Allocation Size (GB)	Tape Full	Source VTL	Tape ID	FVIT	LVIT ID	Remote Export Configured
001B3HL2	1.000	No	SIR-200	10013240	No	No	No
00030000	5.000	No	SIRclus4C-244	10001603	No	No	No
00030034	100.000	No	SIRclus4C-244	10001477	No	No	No
00030036	70.000	No	SIRclus4C-244	10001478	No	No	No
0004002O	7.000	No	SIRclus4C-244	10001724	No	No	No
000400L1	6.000	No	SIRclus4C-244	10001516	No	No	No
000401L1	6.000	No	SIRclus4C-244	10001517	No	No	No
000402L1	6.000	No	SIRclus4C-244	10001518	No	No	No
000404L1	1.000	No	SIRclus4C-244	10001519	No	No	No
00040AL1	6.000	No	SIRclus4C-244	10001520	No	No	No
00040BL1	6.000	No	SIRclus4C-244	10001521	No	No	No
00040FL1	1.000	No	SIRclus4C-244	10001522	No	No	No
00040GL1	1.000	No	SIRclus4C-244	10001523	No	No	No
000809L4	5.000	No	SIRclus4C-244	10001734	No	No	No
00080AL4	5.000	No	SIRclus4C-244	10001735	No	No	No
000C0RL3	1.000	No	SIRclus4C-244	10001524	No	No	No
000C0SL3	1.000	No	SIRclus4C-244	10001525	No	No	No
000C0ZL3	1.000	No	SIRclus4C-244	10001526	No	No	No
000C10L3	1.000	No	SIRclus4C-244	10001527	No	No	No
000C16L3	1.000	No	SIRclus4C-244	10000808	No	No	No
000E02L4	5.000	No	SIRclus4C-244	10001736	No	No	No
000E03L4	5.000	No	SIRclus4C-244	10001737	No	No	No
000F0000	10.000	No	SIRclus4C-244	10001602	No	No	No
0013000L	6.000	No	SIRclus4C-244	10001626	No	No	No

Filters
Barcode: All
Included libraries(id): All
Included policies(id): All
Views: Overall Summary, Deduplication View, Tape Caching View, Replica Resources View, Vault View, Detailed Tape View 167 / 221

Tape Detail View

This view presents information for tapes in a specific library, including bar codes, tape ID, location (library), whether or not the tape is full, current allocation, maximum capacity, used size, amount of data written, compression ratio, and number of segments used.

VTL-1641 06/07/2011 16:12

Virtual Tape Information Report

06/07/2011 00:00 - 06/07/2011 16:12

Tape Detail View

Barcode	Tape ID	Location	Tape Full	Current Allocation (GB)	Maximum Capacity (GB)	Used Size (GB)	Written (GB)	Used Segments
284F1AL1	20003504	TC-10.6.2.180-IBM-03584L32-1..	No	1.000	85.000	0.664	84.827	1
284F1BL1	20003505	TC-10.6.2.180-IBM-03584L32-1..	No	1.000	85.000	0.663	84.827	1
284F1CL1	20003506	TC-10.6.2.180-IBM-03584L32-1..	No	1.000	85.000	0.761	84.826	1
284F1DL1	20003507	TC-10.6.2.180-IBM-03584L32-1..	No	1.000	85.000	0.698	84.827	1
013100L1	20004995	TC-10.6.2.200-IBM-03584L32-1..	Yes	42.000	100.000	36.958	107.072	10
013101L1	20004996	TC-10.6.2.200-IBM-03584L32-1..	Yes	100.000	100.000	99.828	107.053	19
013102L1	20004997	TC-10.6.2.200-IBM-03584L32-1..	Yes	100.000	100.000	99.829	106.867	21
013103L1	20004998	TC-10.6.2.200-IBM-03584L32-1..	Yes	100.000	100.000	99.830	106.927	21
013104L1	20004999	TC-10.6.2.200-IBM-03584L32-1..	Yes	71.000	100.000	67.987	106.936	15
013105L1	20005000	TC-10.6.2.200-IBM-03584L32-1..	Yes	76.000	100.000	75.742	107.466	16
013106L1	20005001	TC-10.6.2.200-IBM-03584L32-1..	Yes	100.000	100.000	99.828	107.185	20
013107L1	20005002	TC-10.6.2.200-IBM-03584L32-1..	Yes	52.000	100.000	49.307	106.630	14
013108L1	20005003	TC-10.6.2.200-IBM-03584L32-1..	Yes	47.000	100.000	44.833	107.146	12
013109L1	20005004	TC-10.6.2.200-IBM-03584L32-1..	Yes	52.000	100.000	48.558	106.508	11
01310AL1	20005005	TC-10.6.2.200-IBM-03584L32-1..	Yes	86.000	100.000	83.250	106.485	36
01310BL1	20005006	TC-10.6.2.200-IBM-03584L32-1..	Yes	76.000	100.000	71.093	106.975	29
01310CL1	20005007	TC-10.6.2.200-IBM-03584L32-1..	Yes	56.000	100.000	52.687	106.507	12
01310DL1	20005008	TC-10.6.2.200-IBM-03584L32-1..	Yes	42.000	100.000	41.562	107.355	10
01310EL1	20005009	TC-10.6.2.200-IBM-03584L32-1..	Yes	27.000	100.000	23.616	106.612	12
01310FL1	20005010	TC-10.6.2.200-IBM-03584L32-1..	Yes	56.000	100.000	55.432	106.745	28
01310IL1	20005013	TC-10.6.2.200-IBM-03584L32-1..	Yes	11.000	11.000	10.828	11.214	7
01310JL1	20005014	TC-10.6.2.200-IBM-03584L32-1..	Yes	1.000	1.000	0.828	0.932	1
01310KL1	20005015	TC-10.6.2.200-IBM-03584L32-1..	Yes	1.000	1.000	0.014	0.902	1
01310LL1	20005016	TC-10.6.2.200-IBM-03584L32-1..	Yes	1.000	1.000	0.828	0.976	1

Filters
Barcode: All
Included libraries(id): All
Included policies(id): All
Views: Overall Summary, Deduplication View, Tape Caching View, Replica Resources View, Vault View, Detailed Tape View

204 / 221

Reports about Replication

Replication Status

This history report displays information about virtual tapes enabled for replication and for virtual tape replicas, during the selected period of time. The wizard provides the following report options:

For virtual tapes

- **Sort by target server name** - For each target server, the report lists all virtual tape replicas and for each replica, the log dates and times of all replication activity.
- **Sort by log date and time** - The report lists log dates and times of all replication activity in ascending order. Details are arranged by virtual tape replica names for each target server.

For virtual tape replicas

- **Sort by primary server name** - For each primary server, the report lists all primary virtual tapes and for each tape, the log dates and times of all replication activity.
- **Sort by log date and time** - The report lists log dates and times of all replication activity in ascending order. Details are arranged by virtual tape names for each primary server.

Report results always identify the primary and target server, the name of the primary virtual tape and virtual tape replica, and the associated policy name and its replication options. Log information always incudes the log time, current replication

activity status, start and end time, the amount of data analyzed, the percentage of data analyzed, the trigger, and comments. The sample below shows typical report layout, irrespective of sorting options.

SIR-200 06/06/2011 14:13

Replication Status Report

05/07/2011 00:00 - 06/05/2011 23:59

Primary Server: SIR-200 (10.8.2.200)
Primary Virtual Tape: NB-Evolv-00072 (10000072)
Target Server: VTL-1641 (10.8.16.41)
Virtual Tape Replica: NB-Evolv-00072-SIR- (20007835)
Policy: Watermark: N/A, Retry: N/A, Replication Time: N/A, Interval: 0 Minutes, Suspended: no

Log Time	Status	Start Time	End Time	Data (KB)	% Complete	Trigger	Comments
05/20/2011 17:03	Idle	05/20/2011 17:00	05/20/2011 17:03	2,097,152	100	admin	

Primary Server: SIR-200 (10.8.2.200)
Primary Virtual Tape: NB-Evolv-00072 (10000072)
Target Server: VTL-1641 (10.8.16.41)
Virtual Tape Replica: NB-Evolv-00072-SIR- (20000007)
Policy: Watermark: N/A, Retry: N/A, Replication Time: N/A, Interval: 0 Minutes, Suspended: no

Log Time	Status	Start Time	End Time	Data (KB)	% Complete	Trigger	Comments
05/29/2011 17:00	Idle	05/29/2011 17:00	05/29/2011 17:00	599,680	100	admin	
05/29/2011 17:16	Idle	05/29/2011 17:16	05/29/2011 17:16	206,336	100	admin	
05/29/2011 17:27	Idle	05/29/2011 17:27	05/29/2011 17:27	206,336	100	admin	
05/29/2011 17:39	Idle	05/29/2011 17:39	05/29/2011 17:39	206,336	100	admin	
05/29/2011 17:51	Idle	05/29/2011 17:51	05/29/2011 17:51	206,336	100	admin	
05/29/2011 18:03	Idle	05/29/2011 18:03	05/29/2011 18:03	206,336	100	admin	
05/29/2011 18:16	Idle	05/29/2011 18:16	05/29/2011 18:16	206,336	100	admin	
05/29/2011 18:28	Idle	05/29/2011 18:28	05/29/2011 18:28	206,336	100	admin	
05/29/2011 18:40	Idle	05/29/2011 18:40	05/29/2011 18:40	206,336	100	admin	
05/29/2011 18:52	Idle	05/29/2011 18:52	05/29/2011 18:52	206,464	100	admin	
05/29/2011 19:04	Idle	05/29/2011 19:04	05/29/2011 19:04	206,464	100	admin	
05/29/2011 19:17	Idle	05/29/2011 19:17	05/29/2011 19:17	206,464	100	admin	

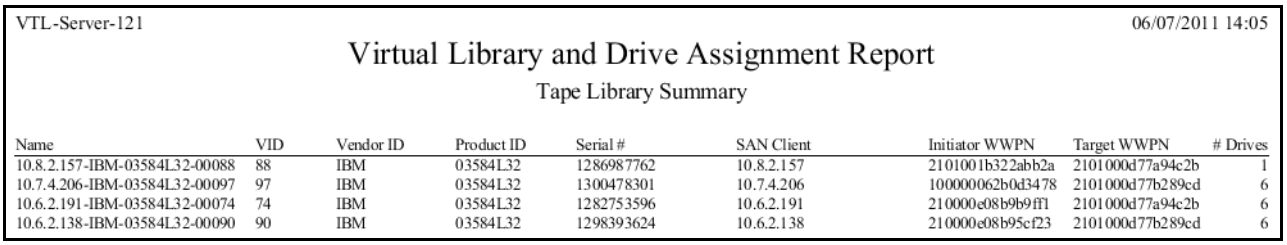
Note: Because the report wizard is not designed to identify a server as a primary server or target server, report results will not be generated if you run the report on a target server and select *Virtual Tapes* or if you run the report on a source server and select *Virtual Tape Replicas*.

Reports about SAN Clients

Virtual Library and Drive Assignment

This status report displays virtual tape library and drive assignments for all SAN Clients on the system, for the current server date. Results are presented from three different points of view: the Tape Library Summary, Drive Summary, and Client Summary.

The Tape Library Summary lists all virtual tape libraries on the system by name and ID and for each library displays its product ID, serial number, and assigned SAN Client, the initiator and target WWPNs assigned to the client, and the number of drives it includes.



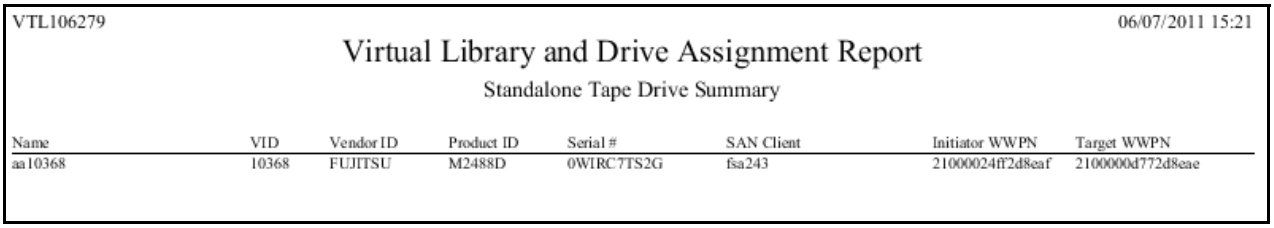
VTL-Server-121 06/07/2011 14:05

Virtual Library and Drive Assignment Report

Tape Library Summary

Name	VID	Vendor ID	Product ID	Serial #	SAN Client	Initiator WWPN	Target WWPN	# Drives
10.8.2.157-IBM-03584L32-00088	88	IBM	03584L32	1286987762	10.8.2.157	2101001b322abb2a	2101000d77a94c2b	1
10.7.4.206-IBM-03584L32-00097	97	IBM	03584L32	1300478301	10.7.4.206	100000062b0d3478	2101000d77b289cd	6
10.6.2.191-IBM-03584L32-00074	74	IBM	03584L32	1282753596	10.6.2.191	210000e08b9b9ff1	2101000d77a94c2b	6
10.6.2.138-IBM-03584L32-00090	90	IBM	03584L32	1298393624	10.6.2.138	210000e08b95cf23	2101000d77b289cd	6

The Tape Drive Summary lists all tape drives on the system by name and ID and for each tape drive displays its product ID, serial number, assigned SAN Client, and initiator and target WWPNs assigned to the client.



VTL106279 06/07/2011 15:21

Virtual Library and Drive Assignment Report

Standalone Tape Drive Summary

Name	VID	Vendor ID	Product ID	Serial #	SAN Client	Initiator WWPN	Target WWPN
aa10368	10368	FUJITSU	M2488D	0WIRC7TS2G	fsa243	21000024ff2d8eaf	2100000d772d8eae

Summary information for each SAN Client lists the name of all devices on the system and for each, displays the type of device (library or drive), ID, vendor, product ID, serial number, and initiator and target WWPNs assigned to the client.

VTL-1641 06/07/2011 13:57

Virtual Library and Drive Assignment Report

Summary for Client: 10.8.9.201

Client Name : 10.8.9.201
Assigned Libraries: 2
Assigned Drives: 12

Name	Type	VID	Vendor ID	Product ID	Serial #	Initiator WWPN	Target WWPN
TC-10.8.9.201-IBM-03584L32-103..	Library	10312	IBM	03584L32	001301684684	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10318	Drive	10318	IBM	ULT3580-TD1	1301684690	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10317	Drive	10317	IBM	ULT3580-TD1	1301684689	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10316	Drive	10316	IBM	ULT3580-TD1	1301684688	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10315	Drive	10315	IBM	ULT3580-TD1	1301684687	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10314	Drive	10314	IBM	ULT3580-TD1	1301684686	2100001b320a9c2a	2101000d772b0c40
IBM-ULT3580-TD1-10313	Drive	10313	IBM	ULT3580-TD1	1301684685	2100001b320a9c2a	2101000d772b0c40
10.8.9.201-ADIC-Scalar 1000-10147	Library	10147	ADIC	Scalar	7QGCS7PW0W	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10153	Drive	10153	IBM	ULTRIUM-TD3	1282748421	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10152	Drive	10152	IBM	ULTRIUM-TD3	1282748420	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10151	Drive	10151	IBM	ULTRIUM-TD3	1282748419	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10150	Drive	10150	IBM	ULTRIUM-TD3	1282748418	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10149	Drive	10149	IBM	ULTRIUM-TD3	1282748417	2100001b320a9c2a	2101000d772b0c40
IBM-ULTRIUM-TD3-10148	Drive	10148	IBM	ULTRIUM-TD3	1282748416	2100001b320a9c2a	2101000d772b0c40

Reports about physical resources

Disk Space Allocation for Virtual Tapes in Libraries

This report can generate the current status of space for use by tapes that are currently in all virtual tape libraries. It can also generate a historical view of space allocated for use by tapes in all or specified virtual tape libraries. In this report, the concept of *used space* is defined as *total allocated space*, which refers to storage consumed by virtual tapes for each virtual tape library.

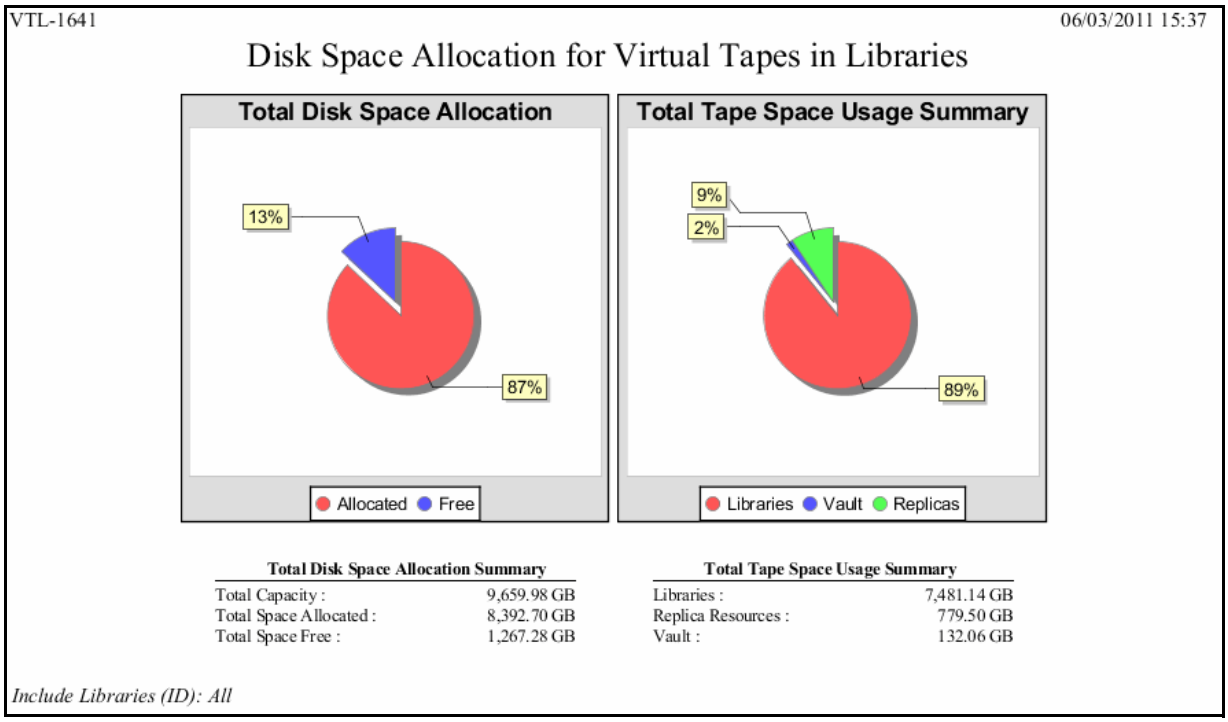
Results include tape segments used for some types of internal tracking and processing when calculating used or allocated space; however, these segments do not affect the maximum capacity available for tapes.

Status report

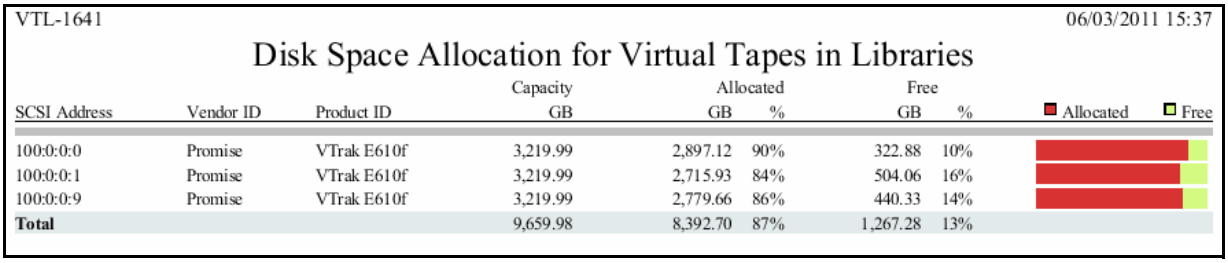
To display a status report, choose the *Current disk space allocation* option in the report wizard. By default, the report will include data for the current server date. Several results are displayed:

- Pie charts representing disk space allocated to tapes
- A table and bar graphs showing information for each LUN
- A table and bar graphs representing disk space allocated to each library

The *Total Disk Space Allocation chart* shows total disk space, the amount of space that has been allocated for tapes on all included disks, and free (not allocated) space. The *Total Tape Space Usage Summary* chart focuses on the distribution of the space allocated for tapes and shows where tapes are located: in libraries, in the virtual vault, and in replica resources.



LUN data on the next page of the report includes the SCSI address, vendor ID, and product ID of each LUN, plus the LUN's total capacity and allocated/free space. A bar chart further represents the total space on each LUN that is allocated to virtual tapes.



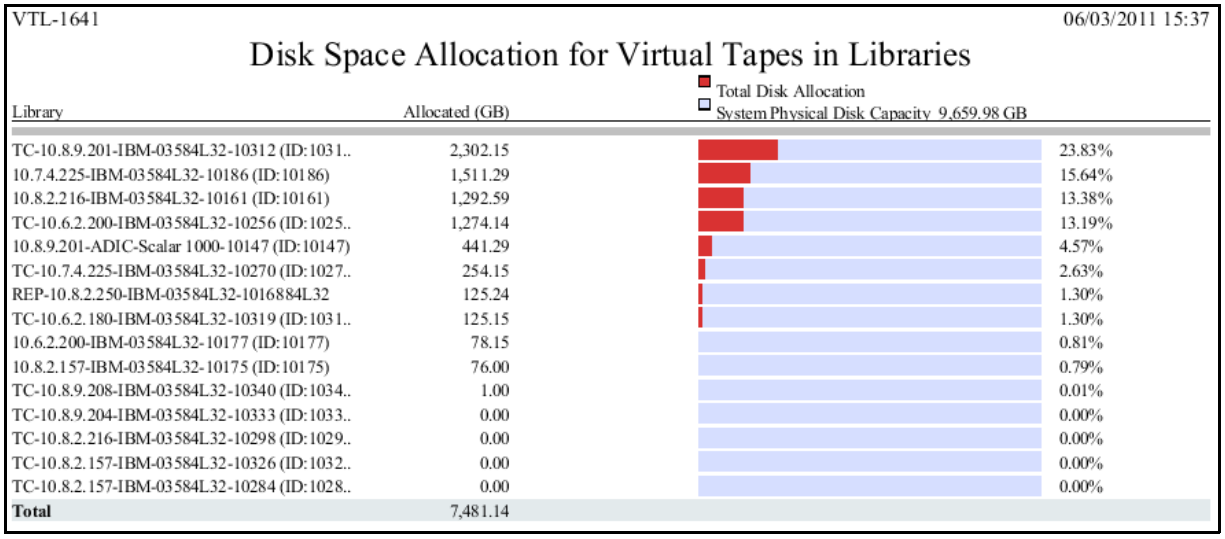
VTL-1641 06/03/2011 15:37

Disk Space Allocation for Virtual Tapes in Libraries

SCSI Address	Vendor ID	Product ID	Capacity GB	Allocated GB	Allocated %	Free GB	Free %
100:0:0:0	Promise	VTrak E610f	3,219.99	2,897.12	90%	322.88	10%
100:0:0:1	Promise	VTrak E610f	3,219.99	2,715.93	84%	504.06	16%
100:0:0:9	Promise	VTrak E610f	3,219.99	2,779.66	86%	440.33	14%
Total			9,659.98	8,392.70	87%	1,267.28	13%

Allocated Free

Library data includes tape space allocation for each selected library. A bar chart indicates the percentage of disk allocated to tapes.



VTL-1641 06/03/2011 15:37

Disk Space Allocation for Virtual Tapes in Libraries

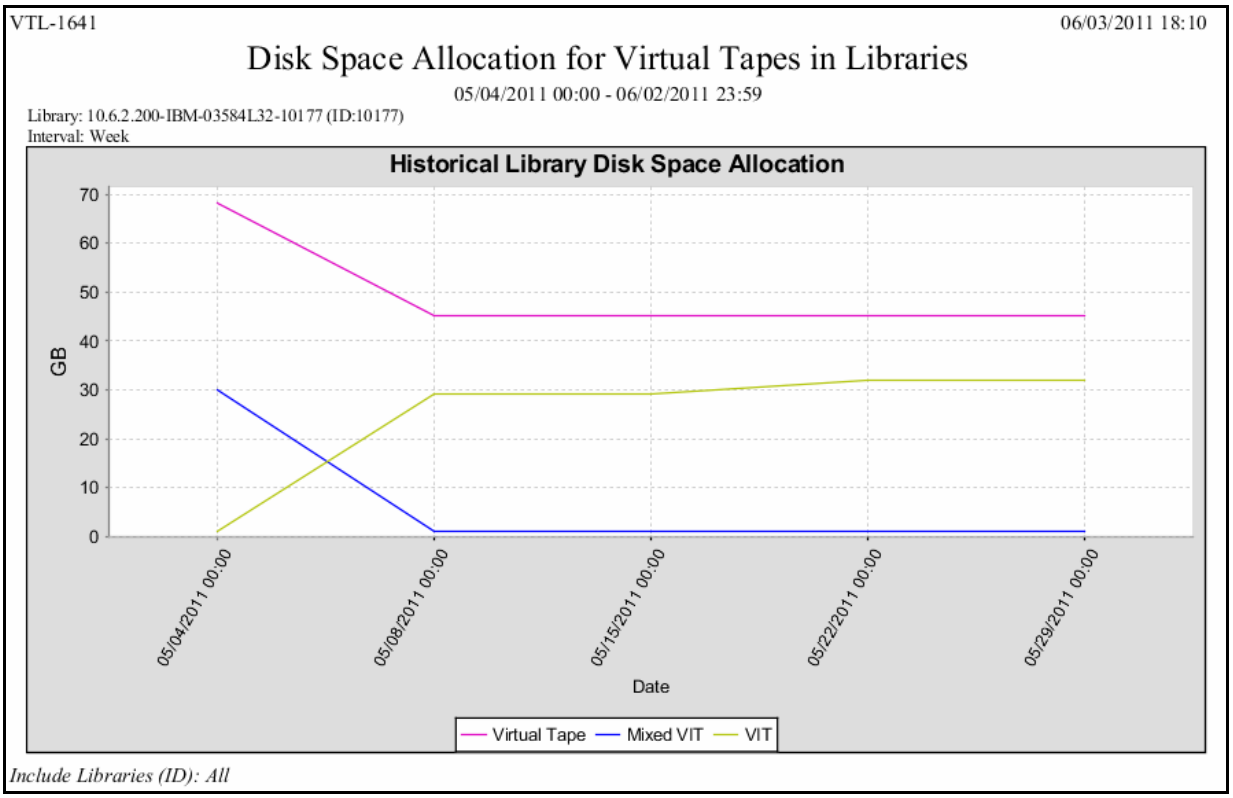
Total Disk Allocation
System Physical Disk Capacity 9,659.98 GB

Library	Allocated (GB)	
TC-10.8.9.201-IBM-03584L32-10312 (ID:1031..	2,302.15	23.83%
10.7.4.225-IBM-03584L32-10186 (ID:10186)	1,511.29	15.64%
10.8.2.216-IBM-03584L32-10161 (ID:10161)	1,292.59	13.38%
TC-10.6.2.200-IBM-03584L32-10256 (ID:1025..	1,274.14	13.19%
10.8.9.201-ADIC-Scalar 1000-10147 (ID:10147)	441.29	4.57%
TC-10.7.4.225-IBM-03584L32-10270 (ID:1027..	254.15	2.63%
REP-10.8.2.250-IBM-03584L32-1016884L32	125.24	1.30%
TC-10.6.2.180-IBM-03584L32-10319 (ID:1031..	125.15	1.30%
10.6.2.200-IBM-03584L32-10177 (ID:10177)	78.15	0.81%
10.8.2.157-IBM-03584L32-10175 (ID:10175)	76.00	0.79%
TC-10.8.9.208-IBM-03584L32-10340 (ID:1034..	1.00	0.01%
TC-10.8.9.204-IBM-03584L32-10333 (ID:1033..	0.00	0.00%
TC-10.8.2.216-IBM-03584L32-10298 (ID:1029..	0.00	0.00%
TC-10.8.2.157-IBM-03584L32-10326 (ID:1032..	0.00	0.00%
TC-10.8.2.157-IBM-03584L32-10284 (ID:1028..	0.00	0.00%
Total	7,481.14	

History report

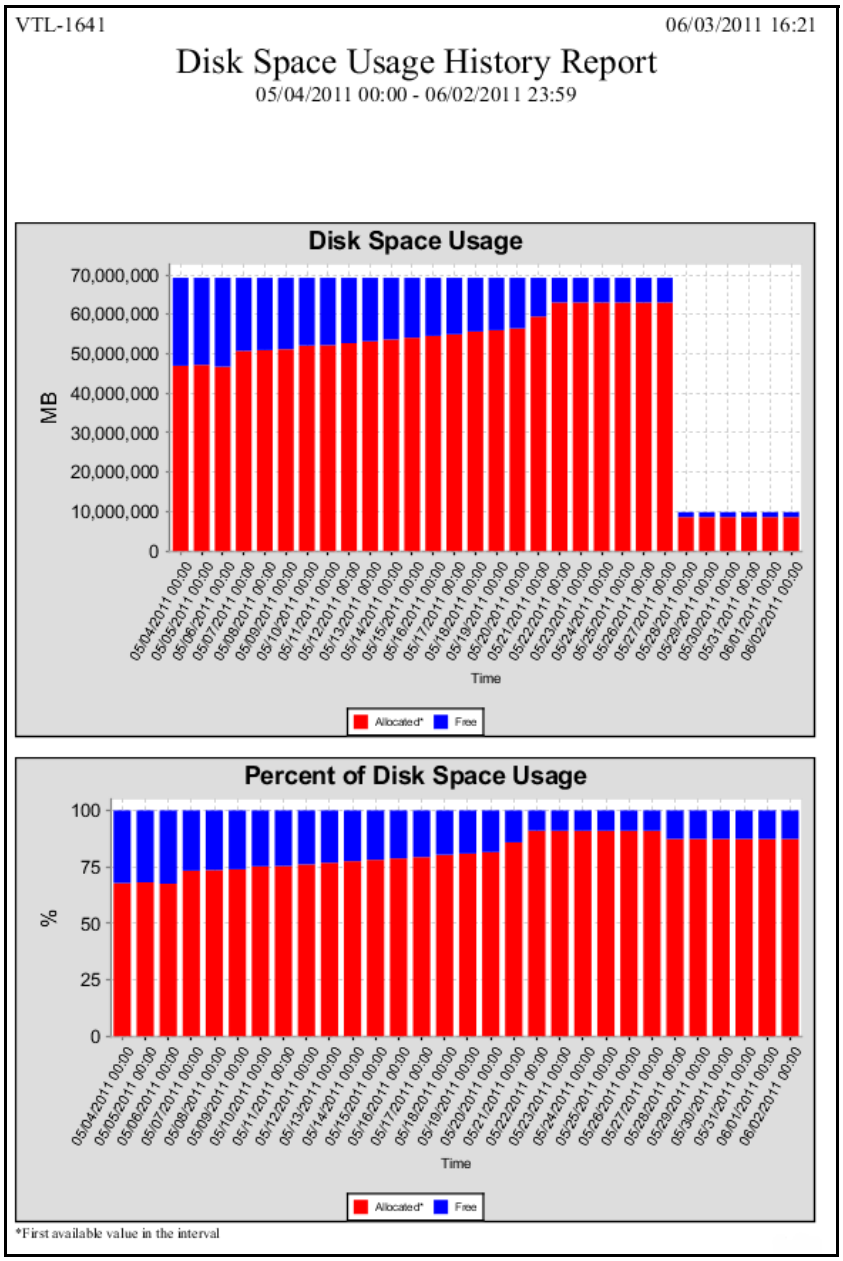
To display a history report, choose the *Historical library space allocation* option in the report wizard, then select the virtual tape libraries you want to include in the results. You can choose a report period of up to one year. Available interval(s) between data points depend on the period you select.

Each data point represents the allocation value for that point in time. Results include a line graph for each library included in the report, showing allocation over time for virtual tapes.



Disk Space Usage History

This status report shows the peak amount of disk space available/used during the specified date range. Available intervals are based on the range: for single days, disk usage is shown for each 60-minute period; for a week, usage is shown for each four-hour period; for a 30-day period (as in the example below), usage is shown for each day. Categories showing an asterisk (*) indicate that the displayed value is based on the first available data in the interval.



The results table includes a row of data for each interval in the graph: the start and stop time, the total capacity for all disks and the total allocated/free capacity expressed as a percentage of total capacity.

VTL-1641 06/03/2011 16:21

Disk Space Usage History Report

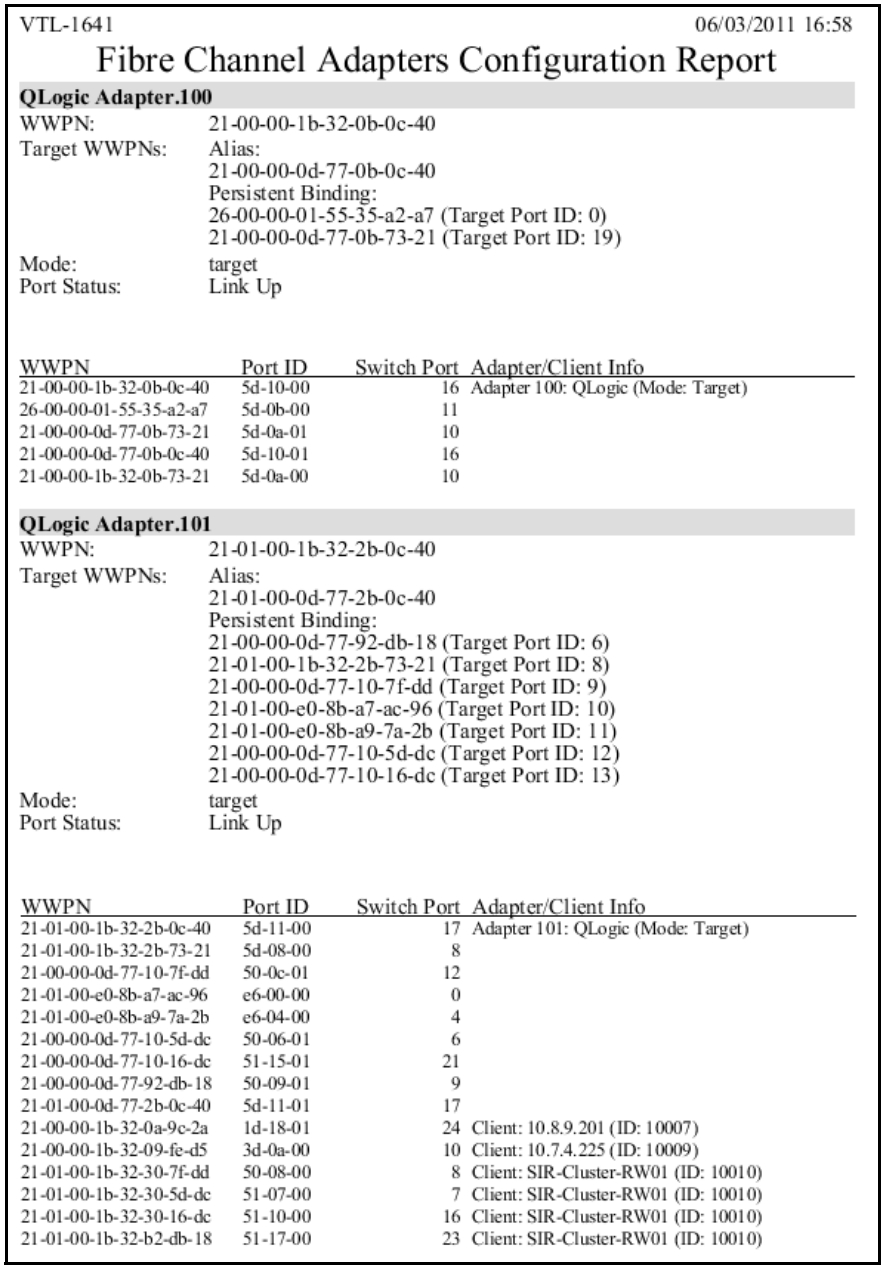
05/04/2011 00:00 - 06/02/2011 23:59

		Capacity*	Allocated*			Free
Start Time	Stop Time	MB	MB	%	MB	%
05/04/2011 00:00	05/04/2011 23:59	69,242,733	46,971,841	68%	22,270,892	32%
05/05/2011 00:00	05/05/2011 23:59	69,242,733	47,186,671	68%	22,056,062	32%
05/06/2011 00:00	05/06/2011 23:59	69,242,733	46,749,255	68%	22,493,478	32%
05/07/2011 00:00	05/07/2011 23:59	69,242,733	50,744,750	73%	18,497,983	27%
05/08/2011 00:00	05/08/2011 23:59	69,242,733	50,931,097	74%	18,311,636	26%
05/09/2011 00:00	05/09/2011 23:59	69,242,733	51,160,431	74%	18,082,302	26%
05/10/2011 00:00	05/10/2011 23:59	69,242,733	52,092,334	75%	17,150,399	25%
05/11/2011 00:00	05/11/2011 23:59	69,242,733	52,214,337	75%	17,028,396	25%
05/12/2011 00:00	05/12/2011 23:59	69,242,733	52,701,824	76%	16,540,909	24%
05/13/2011 00:00	05/13/2011 23:59	69,242,733	53,182,080	77%	16,060,653	23%
05/14/2011 00:00	05/14/2011 23:59	69,242,733	53,662,357	77%	15,580,376	23%
05/15/2011 00:00	05/15/2011 23:59	69,242,733	54,092,416	78%	15,150,317	22%
05/16/2011 00:00	05/16/2011 23:59	69,242,733	54,536,790	79%	14,705,943	21%
05/17/2011 00:00	05/17/2011 23:59	69,242,733	54,938,177	79%	14,304,556	21%
05/18/2011 00:00	05/18/2011 23:59	69,242,733	55,640,641	80%	13,602,092	20%
05/19/2011 00:00	05/19/2011 23:59	69,242,733	55,984,789	81%	13,257,944	19%
05/20/2011 00:00	05/20/2011 23:59	69,242,733	56,436,394	82%	12,806,339	18%
05/21/2011 00:00	05/21/2011 23:59	69,242,733	59,439,786	86%	9,802,947	14%
05/22/2011 00:00	05/22/2011 23:59	69,242,733	63,023,765	91%	6,218,968	9%
05/23/2011 00:00	05/23/2011 23:59	69,242,733	63,009,408	91%	6,233,325	9%
05/24/2011 00:00	05/24/2011 23:59	69,242,733	62,995,051	91%	6,247,682	9%
05/25/2011 00:00	05/25/2011 23:59	69,242,733	62,995,051	91%	6,247,682	9%
05/26/2011 00:00	05/26/2011 23:59	69,242,733	62,995,051	91%	6,247,682	9%
05/27/2011 00:00	05/27/2011 23:59	69,242,733	62,995,051	91%	6,247,682	9%
05/28/2011 00:00	05/28/2011 23:59	9,891,819	8,638,218	87%	1,253,601	13%
05/29/2011 00:00	05/29/2011 23:59	9,891,819	8,638,218	87%	1,253,601	13%
05/30/2011 00:00	05/30/2011 23:59	9,891,819	8,638,218	87%	1,253,601	13%
05/31/2011 00:00	05/31/2011 23:59	9,891,819	8,638,218	87%	1,253,601	13%
06/01/2011 00:00	06/01/2011 23:59	9,891,819	8,636,170	87%	1,255,649	13%
06/02/2011 00:00	06/02/2011 23:59	9,891,819	8,638,218	87%	1,253,601	13%

Fibre Channel Adapters Configuration

This status report shows the World Wide Port Name (WWPN) and port information for all Fibre Channel adapters; this report is useful for matching up WWPNs with clients.

This report is available only as a one-time report.



VTL-1641 06/03/2011 16:58

Fibre Channel Adapters Configuration Report

QLogic Adapter.100

WWPN: 21-00-00-1b-32-0b-0c-40

Target WWPNs: Alias:
21-00-00-0d-77-0b-0c-40
Persistent Binding:
26-00-00-01-55-35-a2-a7 (Target Port ID: 0)
21-00-00-0d-77-0b-73-21 (Target Port ID: 19)

Mode: target

Port Status: Link Up

WWPN	Port ID	Switch Port	Adapter/Client Info
21-00-00-1b-32-0b-0c-40	5d-10-00	16	Adapter 100: QLogic (Mode: Target)
26-00-00-01-55-35-a2-a7	5d-0b-00	11	
21-00-00-0d-77-0b-73-21	5d-0a-01	10	
21-00-00-0d-77-0b-0c-40	5d-10-01	16	
21-00-00-1b-32-0b-73-21	5d-0a-00	10	

QLogic Adapter.101

WWPN: 21-01-00-1b-32-2b-0c-40

Target WWPNs: Alias:
21-01-00-0d-77-2b-0c-40
Persistent Binding:
21-00-00-0d-77-92-db-18 (Target Port ID: 6)
21-01-00-1b-32-2b-73-21 (Target Port ID: 8)
21-00-00-0d-77-10-7f-dd (Target Port ID: 9)
21-01-00-e0-8b-a7-ac-96 (Target Port ID: 10)
21-01-00-e0-8b-a9-7a-2b (Target Port ID: 11)
21-00-00-0d-77-10-5d-dc (Target Port ID: 12)
21-00-00-0d-77-10-16-dc (Target Port ID: 13)

Mode: target

Port Status: Link Up

WWPN	Port ID	Switch Port	Adapter/Client Info
21-01-00-1b-32-2b-0c-40	5d-11-00	17	Adapter 101: QLogic (Mode: Target)
21-01-00-1b-32-2b-73-21	5d-08-00	8	
21-00-00-0d-77-10-7f-dd	50-0c-01	12	
21-01-00-e0-8b-a7-ac-96	e6-00-00	0	
21-01-00-e0-8b-a9-7a-2b	e6-04-00	4	
21-00-00-0d-77-10-5d-dc	50-06-01	6	
21-00-00-0d-77-10-16-dc	51-15-01	21	
21-00-00-0d-77-92-db-18	50-09-01	9	
21-01-00-0d-77-2b-0c-40	5d-11-01	17	
21-00-00-1b-32-0a-9c-2a	1d-18-01	24	Client: 10.8.9.201 (ID: 10007)
21-00-00-1b-32-09-fe-d5	3d-0a-00	10	Client: 10.7.4.225 (ID: 10009)
21-01-00-1b-32-30-7f-dd	50-08-00	8	Client: SIR-Cluster-RW01 (ID: 10010)
21-01-00-1b-32-30-5d-dc	51-07-00	7	Client: SIR-Cluster-RW01 (ID: 10010)
21-01-00-1b-32-30-16-dc	51-10-00	16	Client: SIR-Cluster-RW01 (ID: 10010)
21-01-00-1b-32-b2-db-18	51-17-00	23	Client: SIR-Cluster-RW01 (ID: 10010)

Physical Resource Allocation

This status report displays all virtual devices that have been allocated from all or selected virtualized LUNs. LUNs devoted to use by direct devices are excluded; SCSI aliases are not displayed. Results for each LUN begin with summary information about the physical device, including its name, its SCSI address, the type of physical resource, the category for which it is used (such as for virtual devices), its total capacity, the amount and percentage of allocated storage, the amount and percentage of free space, the number of segments on the device, and the number of virtual tapes allocated on the device.

The detail section lists all resources allocated from the device and for each resource displays the first and last sector allocated for the resources, the size of the resource (in MB and as a percentage of the entire device), the resource type and name, resource ID, and barcode (if the resource is a virtual tape).

VTL-1641 06/06/2011 15:05

Physical Resource Allocation Report

Physical Resource: *Promise:VTrak E610f*
SCSI Address: *100:0:0:0* Device Type: *Disk* Category: *Used by Virtual Device(s)*
Capacity: *3,297,273 MB* Allocated Space: *3,083,410 MB (94%)* Free Space: *213,863 MB (6%)*
Number of Segments: *1,417* Number of Tapes: *396*

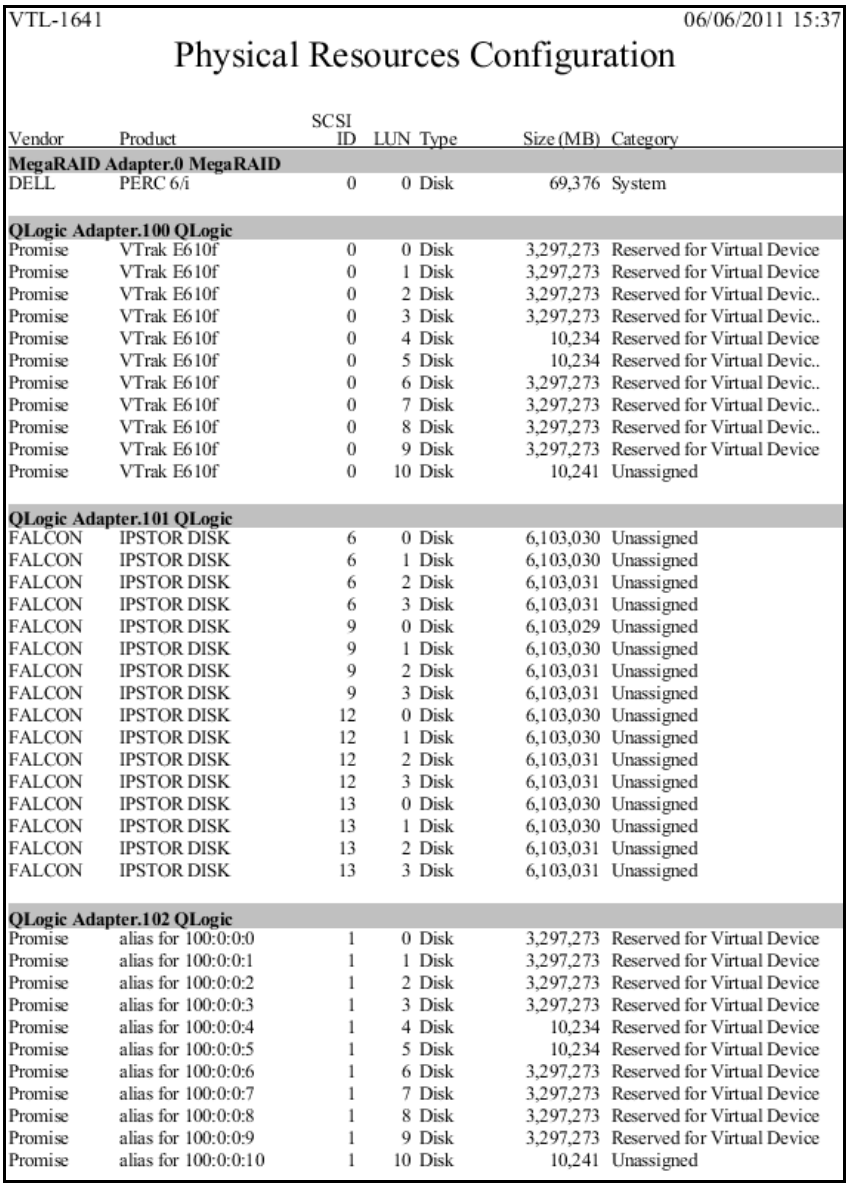
		Segment Size					
First Sector	Last Sector	MB	%	Type	Resource Name	ID	Barcode
14,336	10,500,095	5,120	0.16%	Tape	VirtualTape-05002	20005002	013107L1
10,500,096	20,985,855	5,120	0.16%	Tape	VirtualTape-03257	20003257	014D0GL1
20,985,856	25,180,159	2,048	0.06%	Tape	VirtualTape-05006	20005006	01310BL1
25,180,160	25,186,303	3	0.00%	Header	VirtualTape-04986	20004986	27A3005J
25,186,304	27,283,455	1,024	0.03%	Tape	VirtualTape-04986	20004986	27A3005J
31,490,048	31,496,191	3	0.00%	Header	VirtualTape-00347	20000347	27B10EL3
31,496,192	33,593,343	1,024	0.03%	Tape	VirtualTape-00347	20000347	27B10EL3
33,593,344	33,599,487	3	0.00%	Header	VirtualTape-00345	20000345	27B10CL3
33,599,488	35,696,639	1,024	0.03%	Tape	VirtualTape-00345	20000345	27B10CL3
35,696,640	46,182,399	5,120	0.16%	Tape	VirtualTape-00372	20000372	27B113L3
46,182,400	54,571,007	4,096	0.12%	Tape	VirtualTape-05005	20005005	01310AL1
54,577,152	54,583,295	3	0.00%	Header	VirtualTape-00371	20000371	27B112L3
54,583,296	56,680,447	1,024	0.03%	Tape	VirtualTape-00371	20000371	27B112L3
56,680,448	58,777,599	1,024	0.03%	Tape	VirtualTape-38045	20038045	27CA15L3
58,777,600	69,263,359	5,120	0.16%	Tape	VirtualTape-03456	20003456	014D1CL1
69,275,648	69,281,791	3	0.00%	Header	VirtualTape-00410	20000410	27B125L3
69,281,792	71,378,943	1,024	0.03%	Tape	VirtualTape-00410	20000410	27B125L3
71,378,944	83,961,855	6,144	0.19%	Tape	VirtualTape-38077	20038077	27CA21L3
83,961,856	92,350,463	4,096	0.12%	Tape	VirtualTape-03090	20003090	013800L1
92,350,464	92,356,607	3	0.00%	Tape	VirtualTape-03105	20003105	01380FL1
92,356,608	92,362,751	3	0.00%	Header	CoreServices-8011-1566-SIRclus4C	20003381	001A009O
92,362,752	107,042,815	7,168	0.22%	Tape Replica	CoreServices-8011-1566-SIRclus4C	20003381	001A009O
107,042,816	107,048,959	3	0.00%	Header	NTFSEncryt_WinData_winNB6mp4..	20003306	0017001F
107,048,960	119,631,871	6,144	0.19%	Tape Replica	NTFSEncryt_WinData_winNB6mp4..	20003306	0017001F

PDM segments are displayed with a *PDM* type. Allocated PDM and UMAP segments are shown in the management console in the right-panel display for *Physical Resources-->Storage Devices*.

Physical Resources Configuration

This status report lists all physical adapters on the COPAN 400 server. For each adapter, the report shows information about each physical device that has been configured to the adapter, including its vendor, product name, SCSI ID, LUN number, disk type and size, and category - whether it is a system disk, unassigned, or reserved for virtual device.

This report is available only as a one-time report.



VTL-1641 06/06/2011 15:37

Physical Resources Configuration

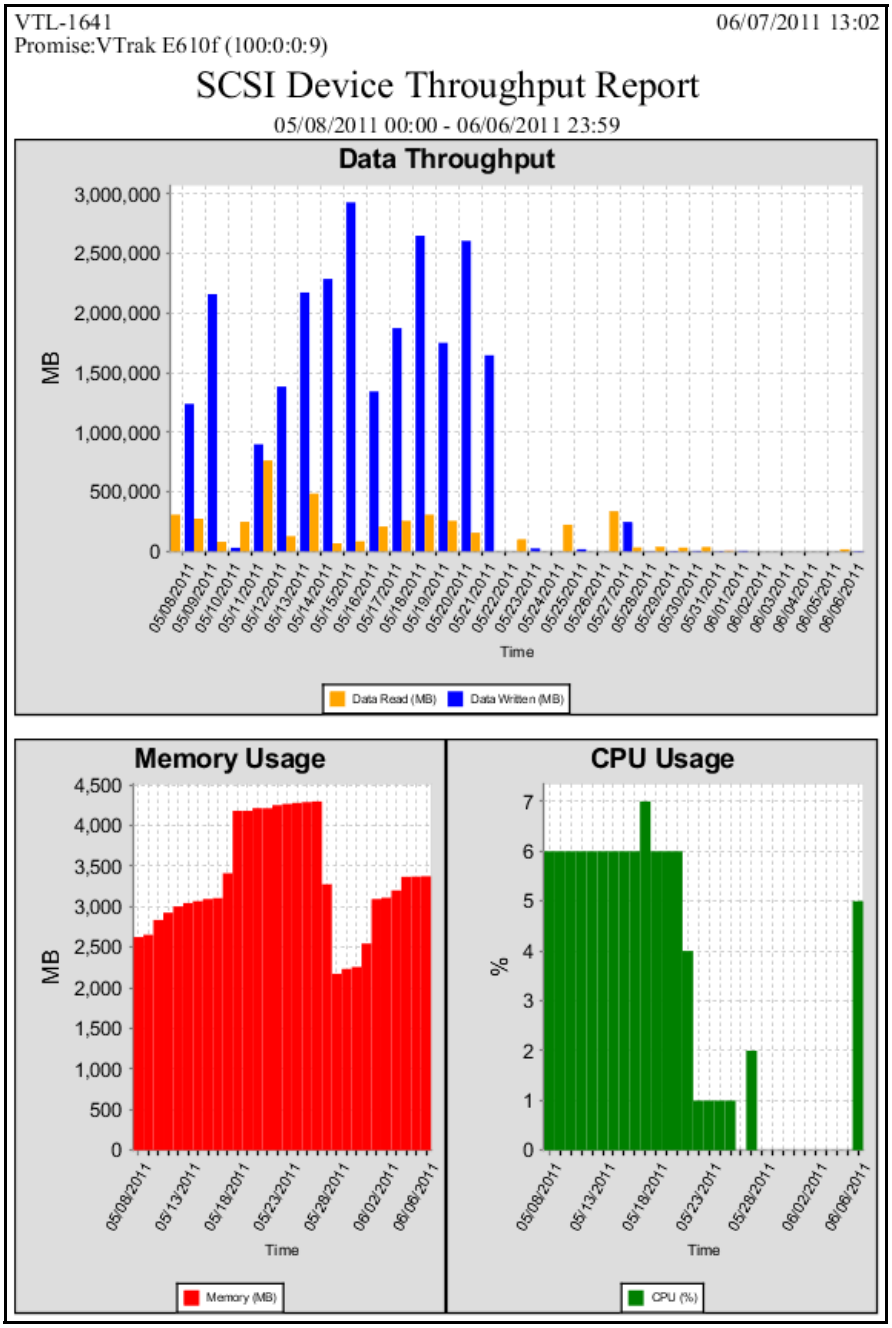
Vendor	Product	SCSI ID	LUN	Type	Size (MB)	Category
MegaRAID Adapter.0 MegaRAID						
DELL	PERC 6/i	0	0	Disk	69,376	System
QLogic Adapter.100 QLogic						
Promise	VTrak E610f	0	0	Disk	3,297,273	Reserved for Virtual Device
Promise	VTrak E610f	0	1	Disk	3,297,273	Reserved for Virtual Device
Promise	VTrak E610f	0	2	Disk	3,297,273	Reserved for Virtual Devic..
Promise	VTrak E610f	0	3	Disk	3,297,273	Reserved for Virtual Devic..
Promise	VTrak E610f	0	4	Disk	10,234	Reserved for Virtual Device
Promise	VTrak E610f	0	5	Disk	10,234	Reserved for Virtual Devic..
Promise	VTrak E610f	0	6	Disk	3,297,273	Reserved for Virtual Devic..
Promise	VTrak E610f	0	7	Disk	3,297,273	Reserved for Virtual Devic..
Promise	VTrak E610f	0	8	Disk	3,297,273	Reserved for Virtual Devic..
Promise	VTrak E610f	0	9	Disk	3,297,273	Reserved for Virtual Device
Promise	VTrak E610f	0	10	Disk	10,241	Unassigned
QLogic Adapter.101 QLogic						
FALCON	IPSTOR DISK	6	0	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	6	1	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	6	2	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	6	3	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	9	0	Disk	6,103,029	Unassigned
FALCON	IPSTOR DISK	9	1	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	9	2	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	9	3	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	12	0	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	12	1	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	12	2	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	12	3	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	13	0	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	13	1	Disk	6,103,030	Unassigned
FALCON	IPSTOR DISK	13	2	Disk	6,103,031	Unassigned
FALCON	IPSTOR DISK	13	3	Disk	6,103,031	Unassigned
QLogic Adapter.102 QLogic						
Promise	alias for 100:0:0:0	1	0	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:1	1	1	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:2	1	2	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:3	1	3	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:4	1	4	Disk	10,234	Reserved for Virtual Device
Promise	alias for 100:0:0:5	1	5	Disk	10,234	Reserved for Virtual Device
Promise	alias for 100:0:0:6	1	6	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:7	1	7	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:8	1	8	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:9	1	9	Disk	3,297,273	Reserved for Virtual Device
Promise	alias for 100:0:0:10	1	10	Disk	10,241	Unassigned

Reports about system performance

Note: Performance reports do not include information about iSCSI clients or iSCSI disks.

SCSI Device Throughput

This history report displays throughput information for the selected physical SCSI storage device during the specified period of time.



In the results table, each entry includes the start and stop time, the amount of data read and written, the amount of memory consumed, and the percentage of CPU processing used.

VTL-1641 06/07/2011 13:02
Promise:VTrak E610f (100:0:0:9)

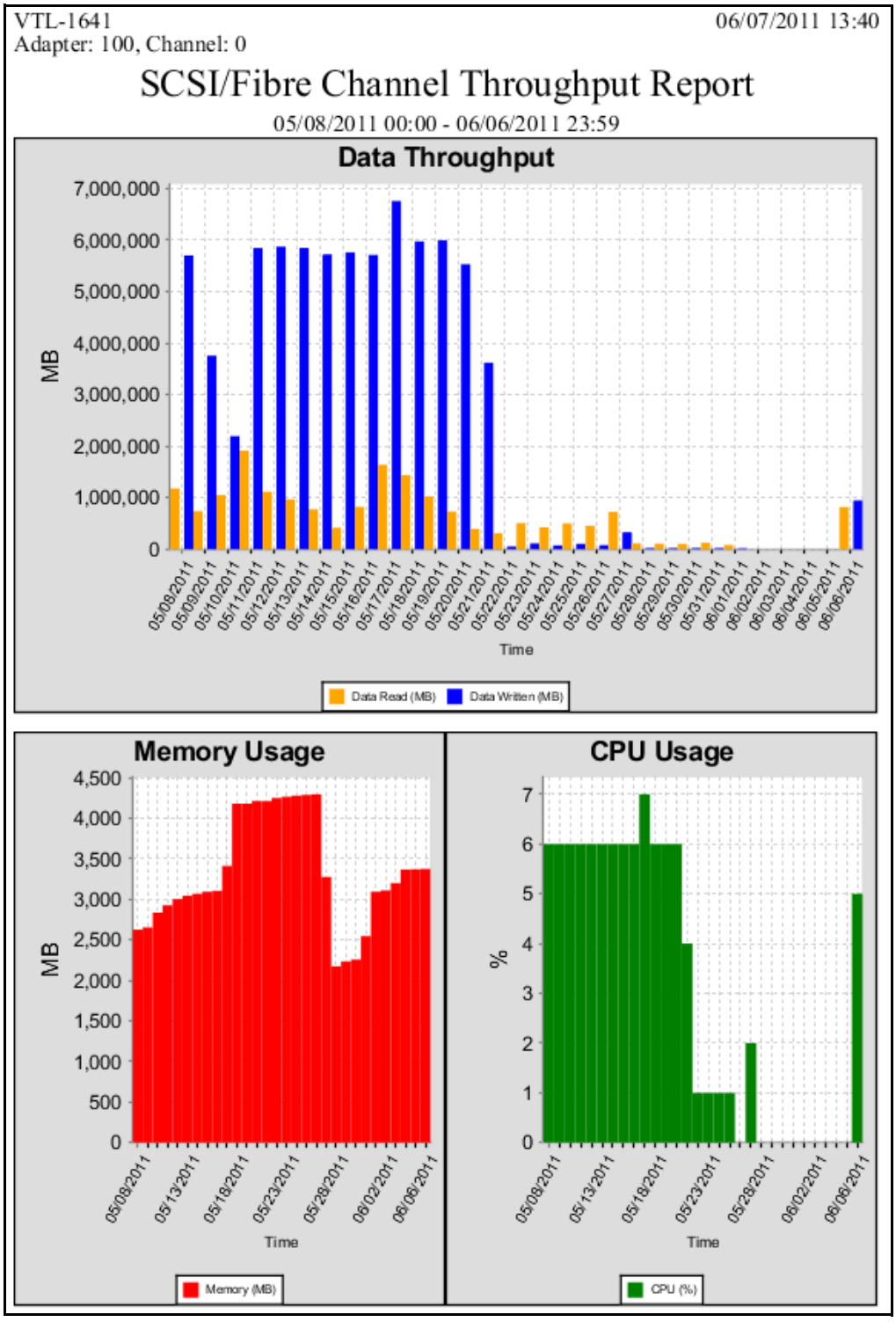
SCSI Device Throughput Report

05/08/2011 00:00 - 06/06/2011 23:59

Start Time	Stop Time	Data Read (MB)	Data Written (MB)	Memory (MB)	CPU (%)
05/08/2011 00:00	05/08/2011 23:59	307,540	1,238,239	2,626	6
05/09/2011 00:00	05/09/2011 23:59	274,634	2,158,890	2,654	6
05/10/2011 00:00	05/10/2011 23:59	80,106	30,422	2,836	6
05/11/2011 00:00	05/11/2011 23:59	247,385	899,810	2,926	6
05/12/2011 00:00	05/12/2011 23:59	763,005	1,383,176	3,003	6
05/13/2011 00:00	05/13/2011 23:59	128,829	2,172,718	3,044	6
05/14/2011 00:00	05/14/2011 23:59	484,657	2,286,416	3,068	6
05/15/2011 00:00	05/15/2011 23:59	67,998	2,928,600	3,093	6
05/16/2011 00:00	05/16/2011 23:59	85,162	1,342,037	3,105	6
05/17/2011 00:00	05/17/2011 23:59	208,634	1,873,792	3,410	7
05/18/2011 00:00	05/18/2011 23:59	257,778	2,648,764	4,179	6
05/19/2011 00:00	05/19/2011 23:59	307,240	1,751,098	4,179	6
05/20/2011 00:00	05/20/2011 23:59	257,108	2,606,075	4,212	6
05/21/2011 00:00	05/21/2011 23:59	156,144	1,646,138	4,211	4
05/22/2011 00:00	05/22/2011 23:59	0	0	4,248	1
05/23/2011 00:00	05/23/2011 23:59	100,509	25,567	4,264	1
05/24/2011 00:00	05/24/2011 23:59	0	0	4,277	1
05/25/2011 00:00	05/25/2011 23:59	223,810	18,459	4,287	1
05/26/2011 00:00	05/26/2011 23:59	0	0	4,295	0
05/27/2011 00:00	05/27/2011 23:59	336,811	246,731	3,277	2
05/28/2011 00:00	05/28/2011 23:59	34,425	1,778	2,174	0
05/29/2011 00:00	05/29/2011 23:59	39,495	3,116	2,234	0
05/30/2011 00:00	05/30/2011 23:59	31,996	4,492	2,258	0
05/31/2011 00:00	05/31/2011 23:59	36,524	2,492	2,546	0
06/01/2011 00:00	06/01/2011 23:59	6,175	4,971	3,094	0
06/02/2011 00:00	06/02/2011 23:59	0	0	3,109	0
06/03/2011 00:00	06/03/2011 23:59	0	0	3,200	0
06/04/2011 00:00	06/04/2011 23:59	0	0	3,367	0
06/05/2011 00:00	06/05/2011 23:59	0	0	3,370	0
06/06/2011 00:00	06/06/2011 23:59	18,167	3,202	3,374	5

SCSI/Fibre Channel Throughput

This history report displays information about data going through the selected SCSI or Fibre Channel adapter during the selected period of time.



In the results table, each entry includes the start and stop time, the amount of data read and written, the amount of memory consumed, and the percentage of CPU processing used.

VTL-1641 06/07/2011 13:40
Adapter: 100, Channel: 0

SCSI/Fibre Channel Throughput Report

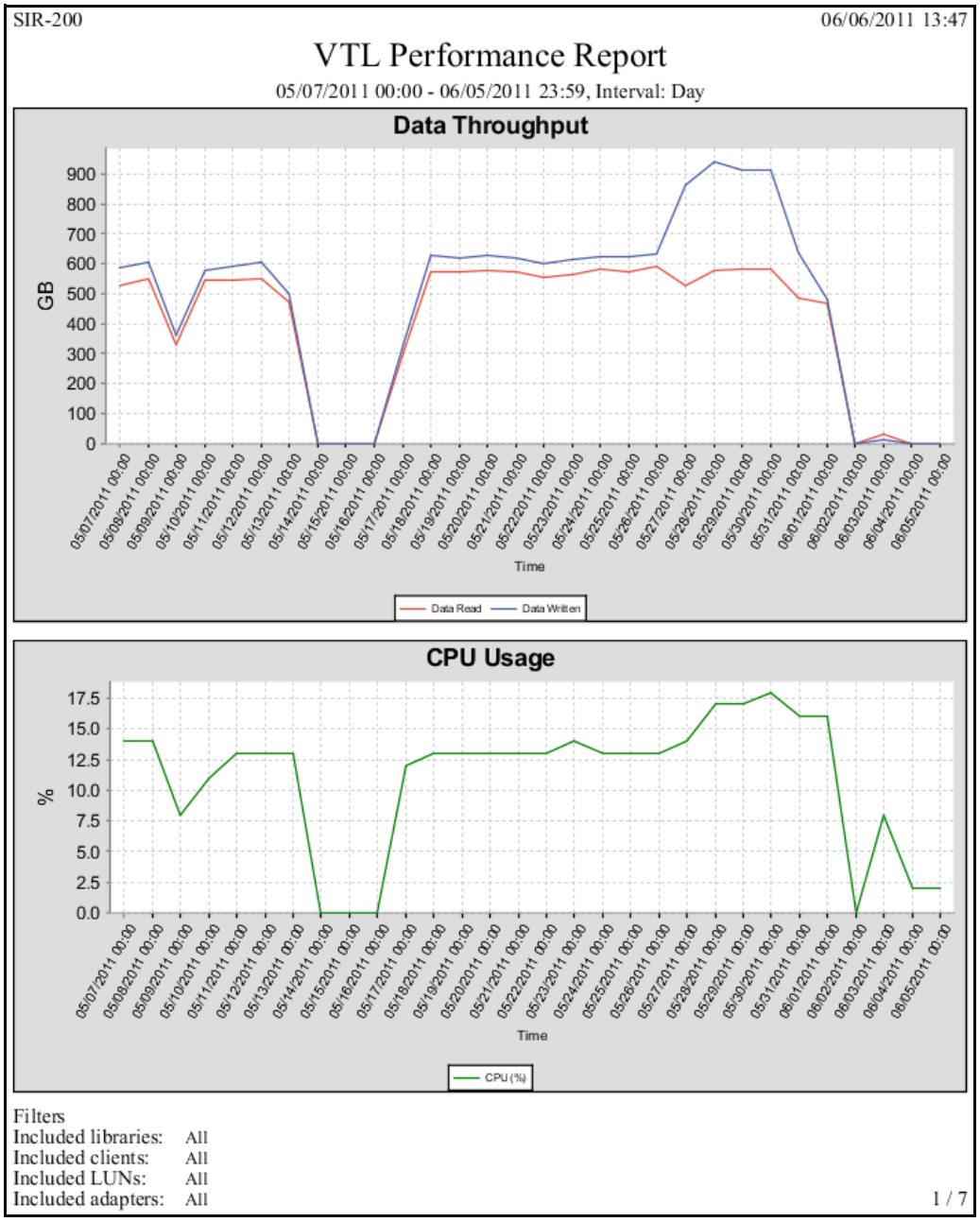
05/08/2011 00:00 - 06/06/2011 23:59

Start Time	Stop Time	Data Read (MB)	Data Written (MB)	Memory (MB)	CPU (%)
05/08/2011 00:00	05/08/2011 23:59	1,181,951	5,703,854	2,626	6
05/09/2011 00:00	05/09/2011 23:59	741,606	3,754,042	2,654	6
05/10/2011 00:00	05/10/2011 23:59	1,049,823	2,195,887	2,836	6
05/11/2011 00:00	05/11/2011 23:59	1,913,460	5,846,927	2,926	6
05/12/2011 00:00	05/12/2011 23:59	1,117,903	5,873,692	3,003	6
05/13/2011 00:00	05/13/2011 23:59	968,380	5,848,518	3,044	6
05/14/2011 00:00	05/14/2011 23:59	776,787	5,722,066	3,068	6
05/15/2011 00:00	05/15/2011 23:59	415,950	5,763,185	3,093	6
05/16/2011 00:00	05/16/2011 23:59	823,923	5,713,073	3,105	6
05/17/2011 00:00	05/17/2011 23:59	1,640,470	6,763,273	3,410	7
05/18/2011 00:00	05/18/2011 23:59	1,438,630	5,976,711	4,179	6
05/19/2011 00:00	05/19/2011 23:59	1,024,834	5,996,852	4,179	6
05/20/2011 00:00	05/20/2011 23:59	731,768	5,535,224	4,212	6
05/21/2011 00:00	05/21/2011 23:59	394,953	3,620,533	4,211	4
05/22/2011 00:00	05/22/2011 23:59	312,611	53,453	4,248	1
05/23/2011 00:00	05/23/2011 23:59	504,997	114,541	4,264	1
05/24/2011 00:00	05/24/2011 23:59	426,264	75,435	4,277	1
05/25/2011 00:00	05/25/2011 23:59	500,375	104,262	4,287	1
05/26/2011 00:00	05/26/2011 23:59	453,634	77,935	4,295	0
05/27/2011 00:00	05/27/2011 23:59	726,582	328,888	3,277	2
05/28/2011 00:00	05/28/2011 23:59	116,239	21,124	2,174	0
05/29/2011 00:00	05/29/2011 23:59	108,713	21,529	2,234	0
05/30/2011 00:00	05/30/2011 23:59	104,454	21,632	2,258	0
05/31/2011 00:00	05/31/2011 23:59	126,892	22,828	2,546	0
06/01/2011 00:00	06/01/2011 23:59	86,715	18,966	3,094	0
06/02/2011 00:00	06/02/2011 23:59	180	1	3,109	0
06/03/2011 00:00	06/03/2011 23:59	192	0	3,200	0
06/04/2011 00:00	06/04/2011 23:59	157	0	3,367	0
06/05/2011 00:00	06/05/2011 23:59	157	0	3,370	0
06/06/2011 00:00	06/06/2011 23:59	820,491	946,539	3,374	5

COPAN 400 Performance

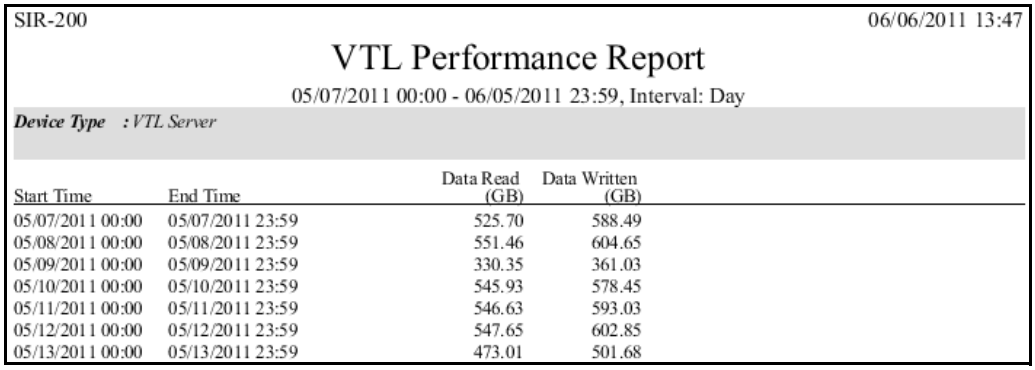
This report analyzes CPU/memory usage and total throughput performance for the entire COPAN 400 system, including all (the default) or selected adapters, LUNs, SAN Clients, and virtual tape libraries.

You can set the interval between data points to be an hour, a day, a week, a month, or a quarter (depending on the selected report dates). In the graphs, each data point represents the total throughput/usage during the interval since the previous data point.



Results for the server, adapters, LUNs, SAN Clients, and virtual tape libraries appear in dedicated sections of the report.

- Performance information for the COPAN 400 server, each adapter, each LUN, and each client device includes the start and end time of the interval, the amount of data read, and the amount of data written.



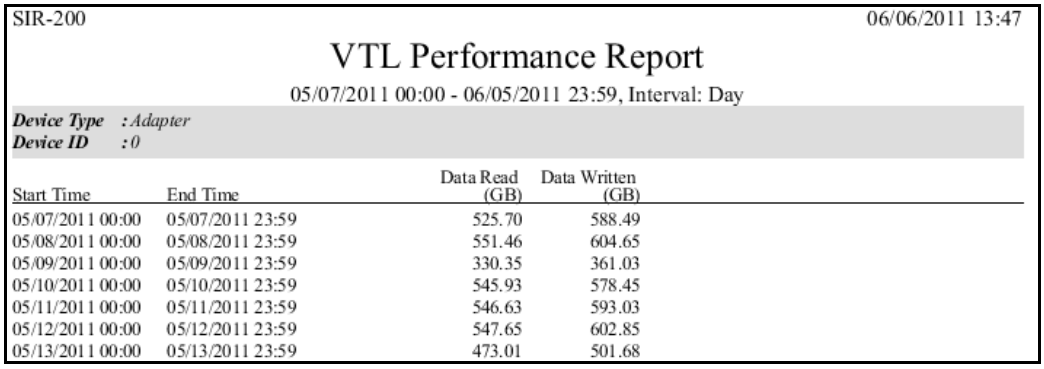
SIR-200 06/06/2011 13:47

VTL Performance Report

05/07/2011 00:00 - 06/05/2011 23:59, Interval: Day

Device Type *: VTL Server*

Start Time	End Time	Data Read (GB)	Data Written (GB)
05/07/2011 00:00	05/07/2011 23:59	525.70	588.49
05/08/2011 00:00	05/08/2011 23:59	551.46	604.65
05/09/2011 00:00	05/09/2011 23:59	330.35	361.03
05/10/2011 00:00	05/10/2011 23:59	545.93	578.45
05/11/2011 00:00	05/11/2011 23:59	546.63	593.03
05/12/2011 00:00	05/12/2011 23:59	547.65	602.85
05/13/2011 00:00	05/13/2011 23:59	473.01	501.68



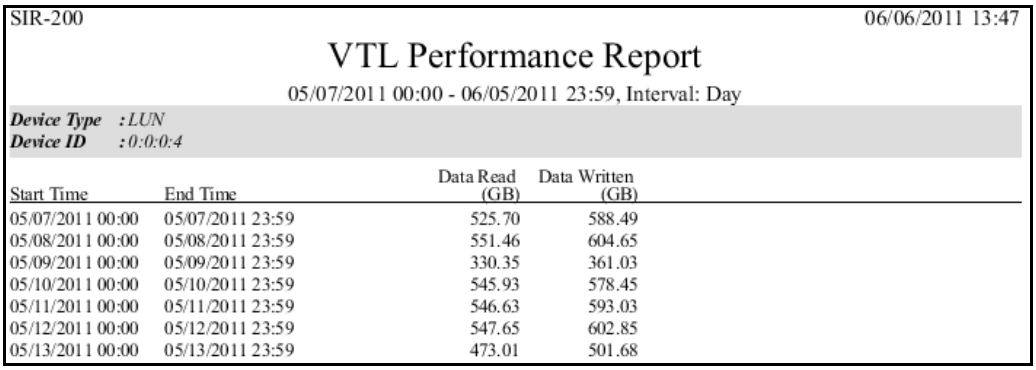
SIR-200 06/06/2011 13:47

VTL Performance Report

05/07/2011 00:00 - 06/05/2011 23:59, Interval: Day

Device Type *: Adapter*
Device ID *: 0*

Start Time	End Time	Data Read (GB)	Data Written (GB)
05/07/2011 00:00	05/07/2011 23:59	525.70	588.49
05/08/2011 00:00	05/08/2011 23:59	551.46	604.65
05/09/2011 00:00	05/09/2011 23:59	330.35	361.03
05/10/2011 00:00	05/10/2011 23:59	545.93	578.45
05/11/2011 00:00	05/11/2011 23:59	546.63	593.03
05/12/2011 00:00	05/12/2011 23:59	547.65	602.85
05/13/2011 00:00	05/13/2011 23:59	473.01	501.68



SIR-200 06/06/2011 13:47

VTL Performance Report

05/07/2011 00:00 - 06/05/2011 23:59, Interval: Day

Device Type *: LUN*
Device ID *: 0:0:0:4*

Start Time	End Time	Data Read (GB)	Data Written (GB)
05/07/2011 00:00	05/07/2011 23:59	525.70	588.49
05/08/2011 00:00	05/08/2011 23:59	551.46	604.65
05/09/2011 00:00	05/09/2011 23:59	330.35	361.03
05/10/2011 00:00	05/10/2011 23:59	545.93	578.45
05/11/2011 00:00	05/11/2011 23:59	546.63	593.03
05/12/2011 00:00	05/12/2011 23:59	547.65	602.85
05/13/2011 00:00	05/13/2011 23:59	473.01	501.68

SIR-200 06/06/2011 13:47

VTL Performance Report

05/07/2011 00:00 - 06/05/2011 23:59, Interval: Day

Device Type *: Client*
Device ID *: 4*

Start Time	End Time	Data Read (GB)	Data Written (GB)
05/07/2011 00:00	05/07/2011 23:59	0.00	622.57
05/08/2011 00:00	05/08/2011 23:59	0.00	614.17
05/09/2011 00:00	05/09/2011 23:59	0.00	358.91
05/10/2011 00:00	05/10/2011 23:59	0.00	588.46
05/11/2011 00:00	05/11/2011 23:59	0.00	593.93
05/12/2011 00:00	05/12/2011 23:59	0.00	587.93
05/13/2011 00:00	05/13/2011 23:59	0.00	486.36

- Performance information for a Virtual Tape Library includes the start and end time of each interval, the amount of uncompressed data read and written, and the amount of compressed data read and written.

SIR-200 06/06/2011 13:47

VTL Performance Report

05/07/2011 00:00 - 06/05/2011 23:59, Interval: Day

Device Type *: Virtual Tape Library*
Device ID *: 27*

		Uncompressed Data (GB)		Compressed Data (GB)	
Start Time	End Time	Read	Written	Read	Written
05/07/2011 00:00	05/07/2011 23:59	9,511.21	618.04	7,182.88	442.51
05/08/2011 00:00	05/08/2011 23:59	17,226.87	607.23	13,379.84	463.18
05/09/2011 00:00	05/09/2011 23:59	14,054.24	355.81	11,061.81	266.46
05/10/2011 00:00	05/10/2011 23:59	13,274.93	584.58	10,536.61	455.17
05/11/2011 00:00	05/11/2011 23:59	7,472.19	590.34	6,224.76	467.49
05/12/2011 00:00	05/12/2011 23:59	14,635.44	584.40	12,255.93	467.56
05/13/2011 00:00	05/13/2011 23:59	17,596.50	483.57	14,796.14	397.26

Automated Tape Caching

Overview

Automated Tape Caching enhances the functionality of COPAN 400 by acting as a cache to your physical tape library, providing transparent access to data regardless of its location.

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

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

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

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

In order to use Automated Tape Caching, you must enable the feature for your virtual library, set your migration and reclamation policies, and create a cache for each of your physical tapes. You may have done this during the initial setup wizard when you first launched COPAN 400 or when you first created a virtual tape library. If you want to add Automated Tape Caching to an existing virtual tape library, follow the instructions in the next section.

Note: You can use Automated Tape Caching **or** Auto Archive/Replication on a virtual tape library, but not both. Enabling Tape Caching on a library for which you previously selected Auto Archive/Replication will disable those features on all tapes in the library.

Tape caching policies

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

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

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

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

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

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

If the data has been written to physical tape and the virtual tape has been reclaimed, reads will be directly from the *direct link* tape. A *direct link* tape is not an actual tape but a link to a physical tape. If you overwrite the beginning of the tape, COPAN 400 will create a new virtual tape, which breaks the *direct link* tape and restarts the clock on the migration policy. If you try to append to the tape, COPAN 400 will append data on the physical tape.

Create/change a tape caching policy

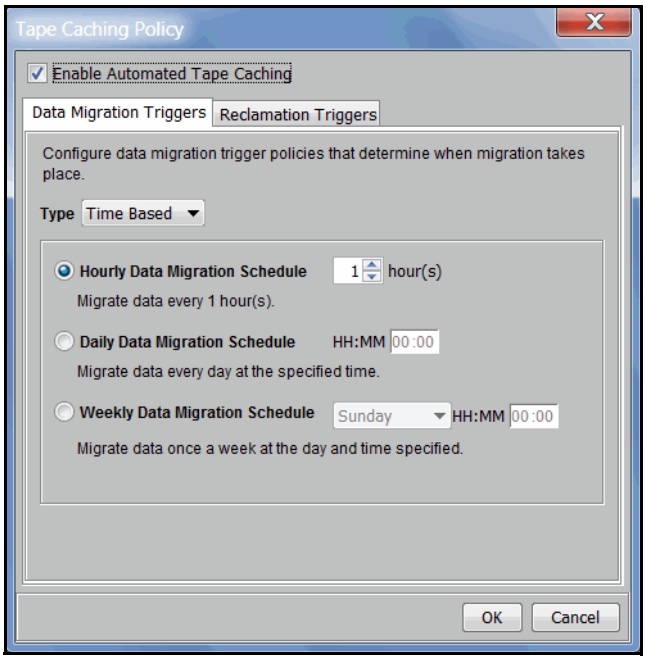
To create or change a tape caching policy:

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

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

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

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

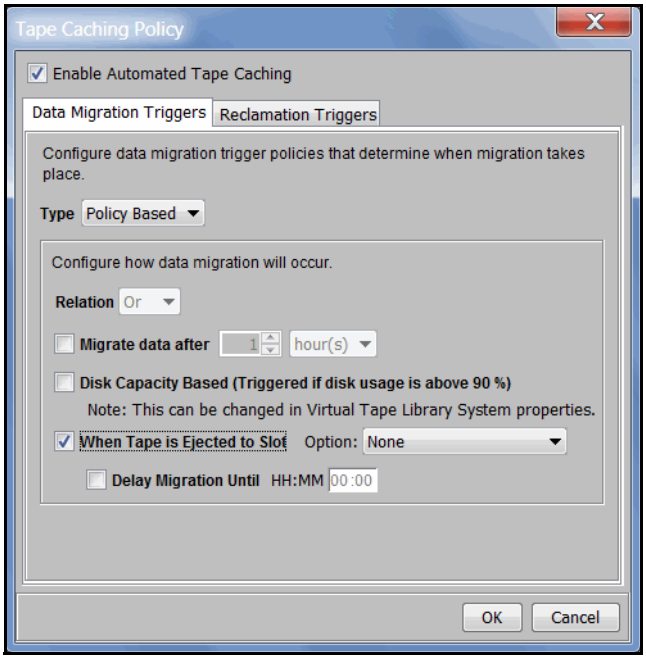


Hourly Data Migration Schedule - Migration occurs every *n* hours.

Daily Data Migration Schedule - Migration occurs at a specific time of day. Type the hour and minute (in 24-hour format) in the box. Note that if the trigger occurs past the specified time, the migration will occur at that time on the next day.

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

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



If multiple triggers are set, select *And* if all the triggers must be met to initiate the data migration or select *Or* if meeting any one of them will initiate the data migration.

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

Migrate data after - Migration will occur when the data has been on the virtual disk for a specified number of hours or days. Specify the desired number of hours/days in the list box.

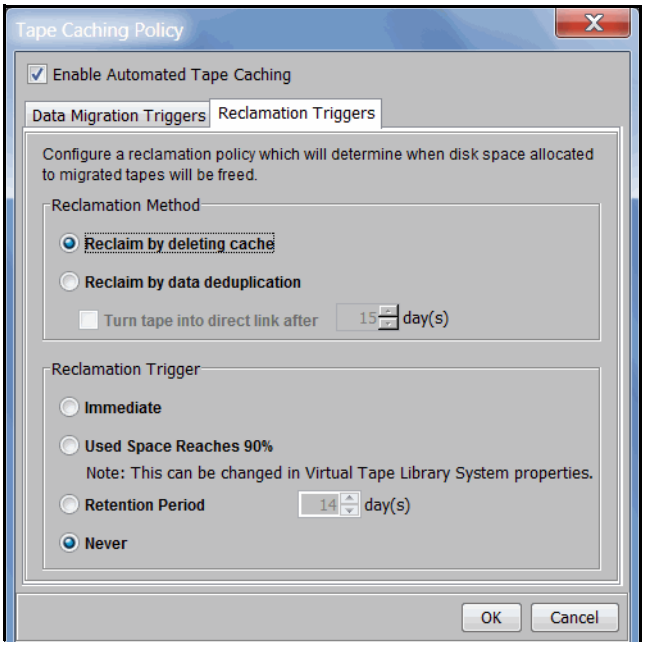
Disk Capacity Based - Migration will occur when the used disk space exceeds the specified disk capacity. The actual percentage is a global variable which is set for all virtual tape libraries. To change the number, right-click *Virtual Tape Library System* in the tree, click *Properties*, and type the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

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

When Tape is Ejected to Slot - Migration will occur when a backup has completed and the virtual tape is ejected to a slot. If you select the option *Only When Tape is Full*, migration will only occur if the tape is full.

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

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



Reclamation method

Reclaim by deleting cache - After the cache is deleted, tapes become *direct link* tapes. A direct link tape is not an actual tape but a link to a physical tape. If your backup application ever overwrites a direct link tape, COPAN 400 will automatically start caching the physical tape. Direct link tapes are only deleted if you disable tape caching on the library or if you delete the tape. If you unassign a physical library, the direct link tape will not be deleted.

Reclamation triggers

Immediate - Cache disk space is freed up as soon as the data migration is complete.

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

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

Never - Cache disk space is never freed up.

5. Click *OK*.

   The policy takes effect immediately.

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

Set global tape caching options

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

1. Right-click *Virtual Tape Library System* and select *Properties*.

   If the server is a member of a group, right-click the group and select *VTL Properties*.

2. Set the global migration and reclamation thresholds.

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

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

Disable a policy

When Automated Tape Caching is disabled for a library, all of the tapes in the library with tape caching policies will be disabled.

Note: You cannot disable tape caching for a library if:

- The library has any direct link tapes (in a slot, drive, or the virtual vault). A list of all direct link tapes will be displayed and you will need to manually delete them before disabling tape caching.
- There is a caching export job running on a cached tape from the library.
- A cached tape is loaded in a drive.

To disable a tape caching policy:

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

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

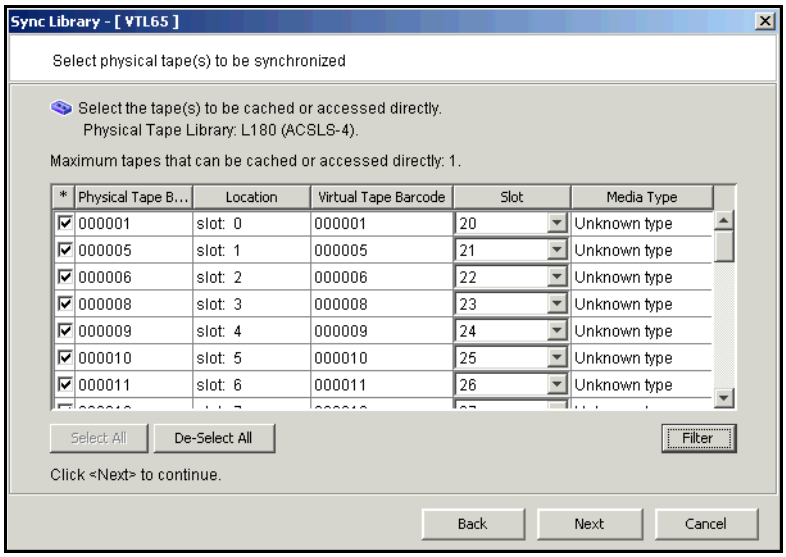
3. Click *OK*.

Create a cache for your physical tapes

Automated Tape Caching stores data on disk before it is migrated to physical tape. In order for this to happen, you must create a cache for each of your physical tapes. This is typically done after you create a virtual tape library. If this has not been done, you must sync the library to create a cache for your physical tapes. You also need to sync the library if a direct link tape was deleted and the associated physical tape is needed to recover data.

1. Right-click your virtual tape library and select *Sync Library*.
2. If you have multiple libraries, select the appropriate physical library.

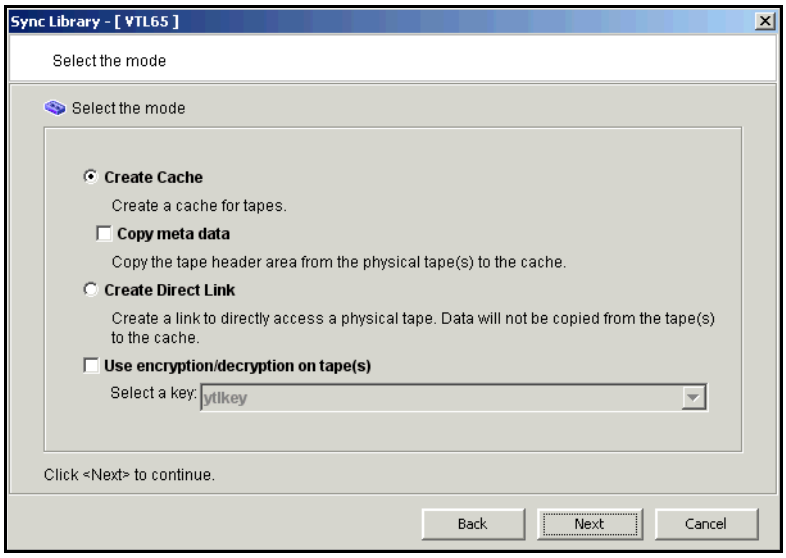
   A physical tape library can only be synchronized to one virtual tape library at a time, unless the ACSLS option is being used.
3. Select the physical tape(s) for which you want to create a cache.



To display specific tapes, click the *Filter* button to select a single barcode or a range of barcodes. If you want to specify a particular starting/ending range number, select *Start With* or *End With* in the *From/To* fields. You can then type the number in the box to the right.

Note: Make sure that you select physical tapes that use the same media type as your virtual tapes.

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



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

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

5. If applicable, specify how to create the cache.
6. If applicable, specify a prefix and size.
7. Confirm all information and click *Finish*.

Create uncached virtual tapes

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

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

Enable tape caching for existing virtual tapes

Tape caching can be enabled for existing uncached virtual tapes. This provides an easy way to migrate data on existing uncached virtual tapes to physical tapes without having to back up the data to new tapes.

Note that in order to migrate data to physical tapes, physical tape(s) with corresponding barcodes must exist in the physical library.

1. Right-click your virtual tape library and select *Enable Tape Caching on Tape(s)*.
2. Select the tapes you want and click *OK*.

   A job will be kicked off to migrate the data to physical tape.

Manually migrate cached data to physical tape

You can manually cause data in a cache to be migrated to physical tape even if the tape has been previously migrated. To do this, right-click a virtual tape cache and select *Migrate to Physical Tape*.

Force migration of an entire tape to physical tape

You can migrate an entire tape to physical tape. To do this, right-click a virtual tape cache and select *Force Migrate to Tape*.

Note: This will overwrite all data on the physical tape.

Reclaim disk space manually

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

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

Renew cache for a direct link tape

If your backup application ever overwrites the direct link tape, COPAN 400 will automatically start caching the physical tape.

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

Recover data using Automated Tape Caching

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

If the data is no longer on disk, when the direct link tape is to be mounted, the corresponding physical tape also needs to be mounted. When loading the physical tape, COPAN 400 will look for an available drive. If there are no free drives available, COPAN 400 will cancel any import or export jobs in an attempt to free a tape drive.

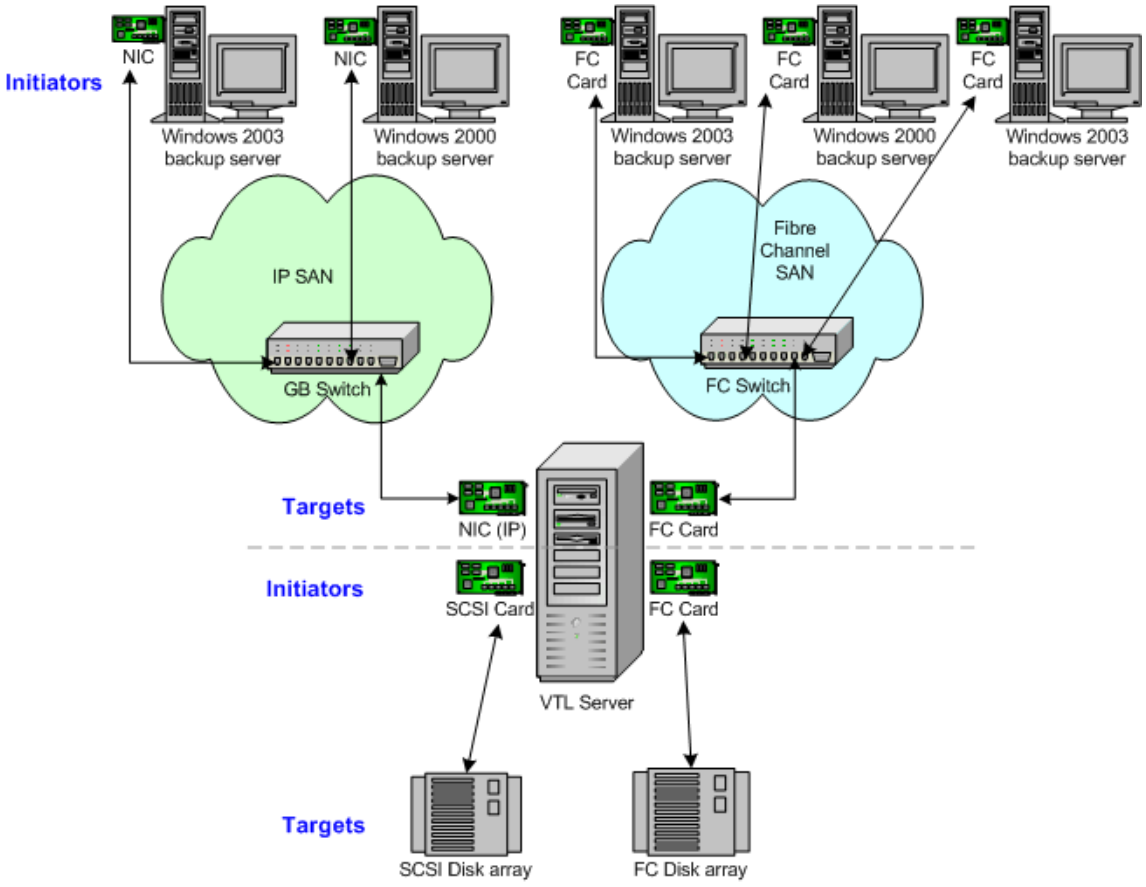
Note: If a direct link tape was deleted and the associated physical tape is needed to recover data, you will have to sync the library to create a direct link to the physical tape.

Fibre Channel Configuration

Overview

Just as the COPAN 400 server supports different types of storage devices (such as SCSI, Fibre Channel, and iSCSI), the COPAN 400 server is protocol-independent and supports multiple outbound target protocols, including Fibre Channel Target Mode.

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



As you can see from the illustration above, an application server can be either an iSCSI client or a Fibre Channel client, but not both. Using separate cards and switches, you can have all types of COPAN 400 Clients (FC and iSCSI) on your network.

Configure Fibre Channel hardware on server

COPAN 400 supports the use of QLogic HBAs for the COPAN 400 server. Refer to the certification matrix on the SGI website for a list of HBAs that are currently certified.

Ports

Your COPAN 400 appliance will be equipped with several Fibre Channel ports. Some of these ports will interface with storage arrays. Others will interface with physical tape libraries, while the remaining ports will interface with backup (media) servers.

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

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

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

HBA driver

QLogic NPIV driver

NPIV (N_Port ID Virtualization) is the default driver for COPAN 400 servers. NPIV allows a port to have the role of both initiator and target in full-duplex mode.

The following is required in order to use NPIV:

- You must have a supported HBA. COPAN 400 supports both 4G and 8G HBAs. Check the SGI certification matrix for a list of supported HBAs.
- The fabric switch must support NPIV.
- If a QLogic FC switch is being used, you must disable “IOStreamGuard” for any switch port that connects to an NPIV target port.

When using the NPIV driver, there are two WWPNs, the *base* port and the *alias*.

Important notes:

- With dual mode, clients will need to be zoned to the alias port (called *Target WWPN*). If they are zoned to the base port, clients will not see any devices.
- You will only see the alias port when that port is in target mode.
- You will only see the alias once all of the COPAN 400 services are started.

QLogic driver

The QLogic driver is the single-mode, point-to-point driver where targets and initiators reside on separate ports.

Zoning

Note: If a port is connected to a switch, we highly recommend the port be in at least one zone so it will display in your SNS table.

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

Soft zoning

Soft zoning is required for the QLogic NPIV driver and 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.

The rules for soft zoning between COPAN 400 servers using the QLogic NPIV driver are:

- No COPAN 400 server target can be zoned with another of its own targets.
- No COPAN 400 server target can be zoned with one of its own initiators.
- No COPAN 400 server initiators can be zoned with one of its own initiators.

Hard zoning

Hard zoning is only supported for QLogic drivers without NPIV. It uses the port number of the switches for zoning. 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.

If hard zoning is used, it is necessary to create zones for each standby target, doubling the number of upstream zones. This extra set of zones is not necessary in the case of soft zoning because zones are defined by WWPN combinations. In a failover event, the standby ports assume the WWPNs of the target ports of the failed COPAN 400 server. Therefore, the single set of soft zones is still valid.

General zoning requirements

COPAN 400 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. This does not apply in the case of FC connectivity between COPAN 400 appliances.

Additionally, make sure that storage devices to be used by COPAN 400 are not zoned to clients (backup servers). Ports on storage devices to be used by COPAN 400 should be zoned to COPAN 400's initiator ports while the clients are zoned to COPAN 400's target ports. Make sure that from the storage unit's management GUI (such as SANtricity and NaviSphere), the LUNs are re-assigned to COPAN 400 as the "host". COPAN 400 will virtualize these LUNS. COPAN 400 can then define virtual tapes out of these LUNS and further provision them to the clients.

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 Linux systems, you can reload HBAs by restarting COPAN 400 with the command:

```
revolution restart all
```

Without persistent binding, there is a risk that the wrong storage controller port will be accessed when the COPAN 400 appliance is rebooted (or COPAN 400 HBA driver is reloaded).

FSHBA.CONF file

The *fshba.conf* file is found in $ISHOME/etc and is used to adjust settings for FC adapters installed on the COPAN 400 appliance.

1. Determine the HBA settings to change.
2. Back up the *fshba.conf* file:
   ```
   cp fshba.conf fshba.conf.bak
   ```
3. Modify *fshba.conf* using the *vi* editor.
4. Save the *fshba.conf* file.
5. Start or restart COPAN 400 and its HBA module with the following command:
   ```
   revolution start all
   ```
   You must restart the HBA drivers and COPAN 400 modules on the COPAN 400 appliance for the changes in the *fshba.conf* file to take effect and to recognize the new settings.

Link speed

In the *fshba.conf* file, the link speed is set to auto-negotiate by default for every FC port. You must manually update this and match the link speed with the switch speed. It may be necessary to manually set the port switch speed on the FC switch as well.

If you are attaching a tape library or storage array directly to the COPAN 400 appliance, adjust the link speed for all FC ports (COPAN 400 and/or tape library). Check with your vendor to obtain any recommended FC HBA settings.

Device identification

Typically, Linux will assign its own device numbers, such as SCSI adapter0 and SCSI adapter1, etc. Therefore, if you have a single port QLogic HBA loading up AFTER two internal SCSI devices, it will become SCSI adapter2.

However, the COPAN 400 appliance may not identify the same devices in the same way. COPAN 400 will identify SCSI devices as hba0, hba1, hba2, and so on in the *fshba.conf* file. Settings for each individual FC port (for example, hba0 or hba1) can be modified in fshba.conf.

To identify which adapter belongs to which HBA in fshba.conf:

1. Run the following commands:

   ```
   ls /proc/scsi/qla2xxx
   ```

   This will output all adapter numbers (i.e. 100, 101, 102). Then, match up the adapter numbers: 100->hba0, 101->hba1, etc.

2. Run the following command to display the WWPN for that adapter:

   ```
   grep BIOSWWPN /proc/scsi/qla2xxx/###
   ```

3. Run the following command to determine which physical port belongs to each adapter number in fshba.conf:

   ```
   tail -f /var/log/messages
   ```

   and then unplug the FC port. You will see a loop down message like the one below. 100 is the adapter number in this example:

   ```
   Jan 23 13:40:03 <hostname> kernel: scsi(100): LOOP DOWN detected
   ```

Data rate

1. Scroll down to the appropriate adapter section.

2. Search for *data_rate-hbaX*.

   It should look like this:

   ```
   #data_rate-hbaX=2
   #comment=this option allow driver software to select a fixed rate or
   #        request that the firmware negotiate the
   #        data rate (1-2G,2-auto,3-4G,4-8G)
   #range=0 or 1 or 2
   #===============
   data_rate-hba0=2
   data_rate-hba1=2
   ```

3. For the adapter to be configured (i.e., hba0), change the value:

   ```
   data_rate-hba0=0 or 1 NOT 2 (auto)
   ```

4. Repeat for each adapter to be configured.

Configure Fibre Channel hardware on clients

Fabric topology

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

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

Load balance the path for each downstream storage LUN

For optimal performance, if you have more than one path available for your storage LUNs, you can set COPAN 400 to evenly distribute I/O between all storage LUNs. To do this:

1. Right-click on a Fibre Channel device under *Physical Resources --> Storage Devices --> Fibre Channel Devices* and select *Properties*.

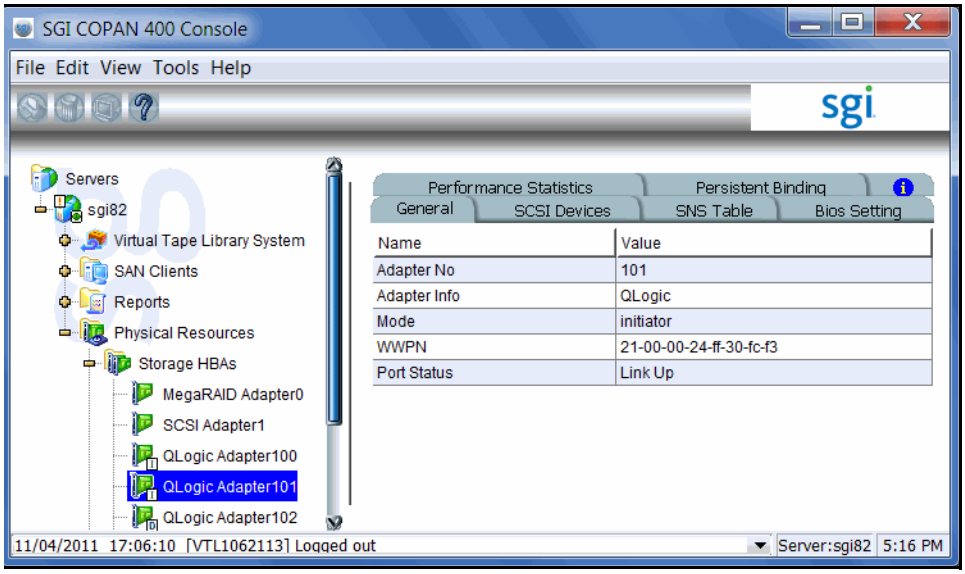
2. On the *I/O Path* tab, highlight a path and use the arrow keys to move it up or down in the list.

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 console by highlighting a port under *Physical Resources*.

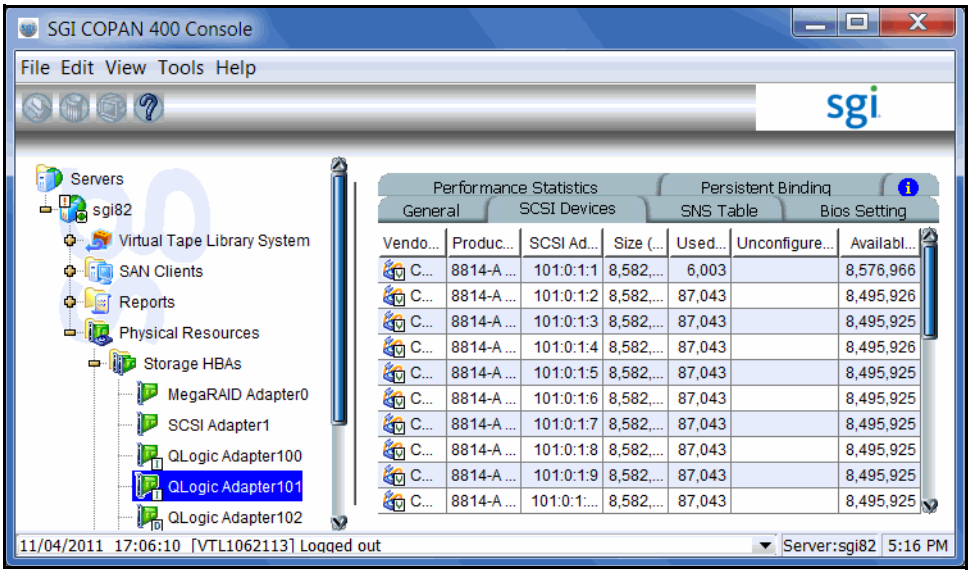
General tab

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



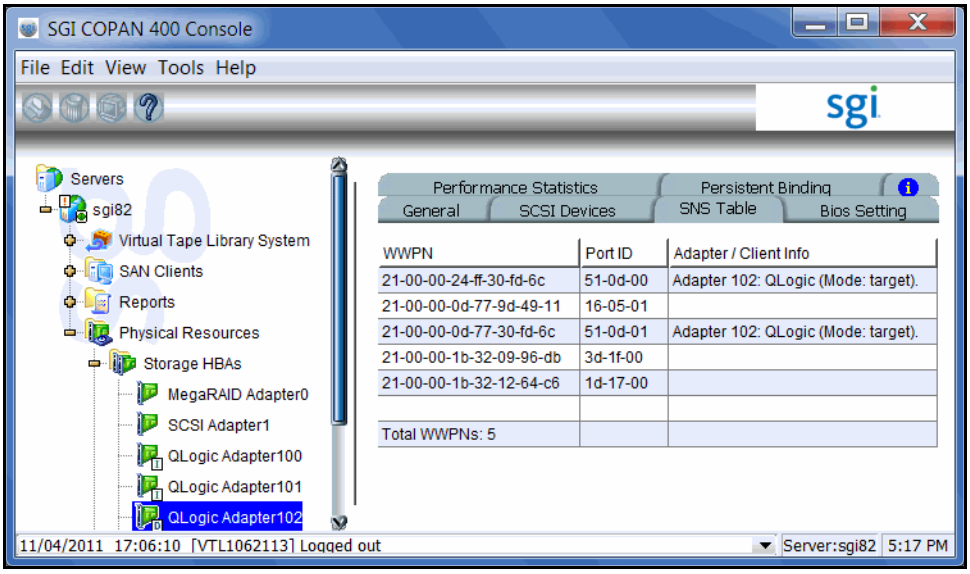
SCSI Devices tab

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



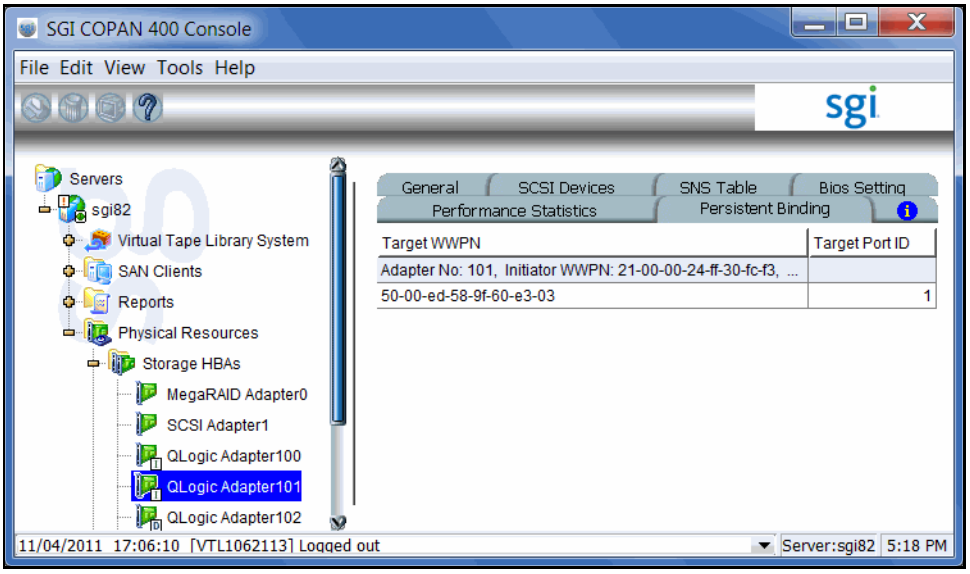
SNS Table tab

The SNS Table tab lists the ports to which this adapter is zoned. COPAN 400 queries the switch for its Simple Name Server (SNS) database and displays this information. If you expect to see a WWPN that is not listed, right-click the adapter and select *Refresh SNS.*



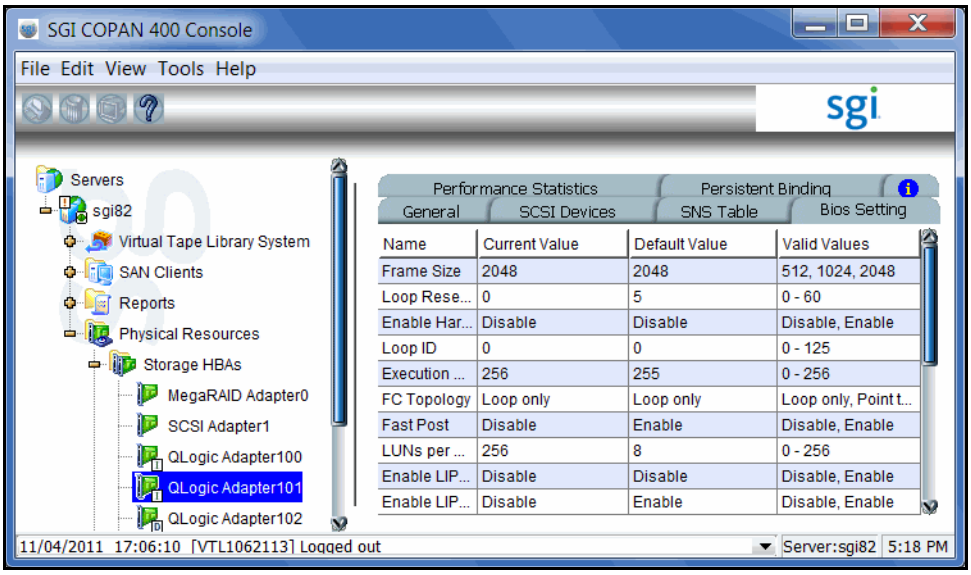
Persistent Binding tab

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



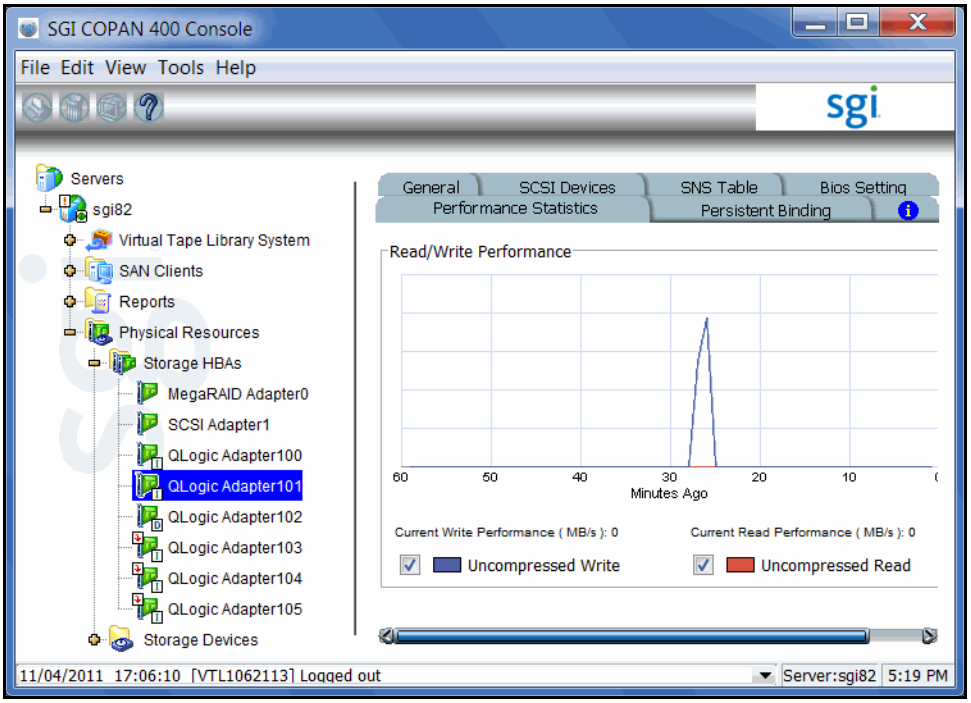
Bios Setting tab

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



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.



Set QLogic ports to target mode

Multi port QLogic HBAs

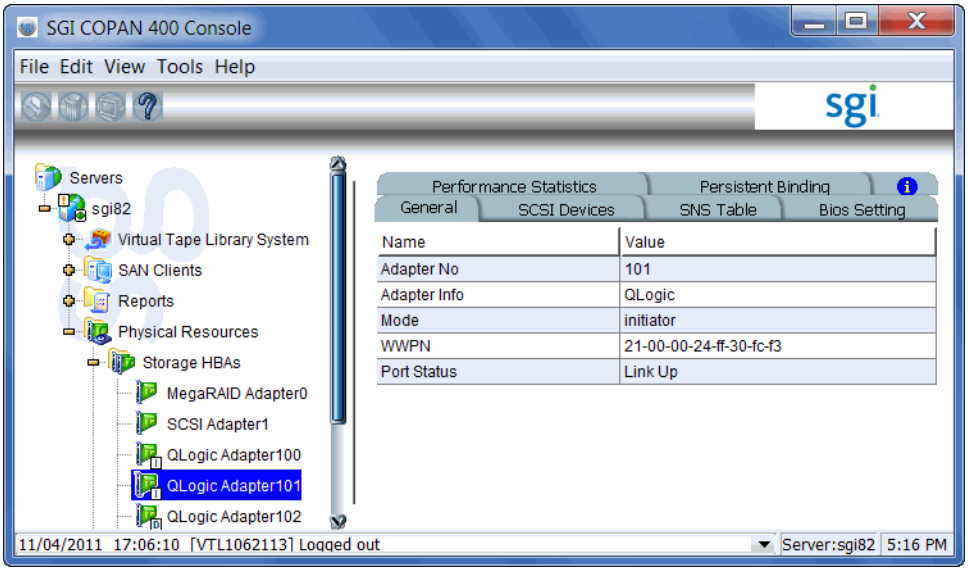
With a multi-ID HBA, each port can be both a target and an initiator. To use target mode, you must enable target mode on a port.

For Failover, if you are using multi-ID HBAs, you need a minimum of one port for client connectivity and one for storage.

To set target mode:

1. In the console, expand *Physical Resources*.
2. Right-click a multi-ID HBA and select *Options --> Enable Target Mode*.
3. Click *OK* to enable.

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



Single port QLogic HBAs

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

For Failover, if you are using single port HBAs, you minimally need two ports for client connectivity (one for normal operation, one for standby) and one initiator port to connect to storage.

You need to switch one of those initiators into target mode so your clients will be able to see the COPAN 400 server. You will then need to select the equivalent adapter on the secondary server and switch it to target mode.

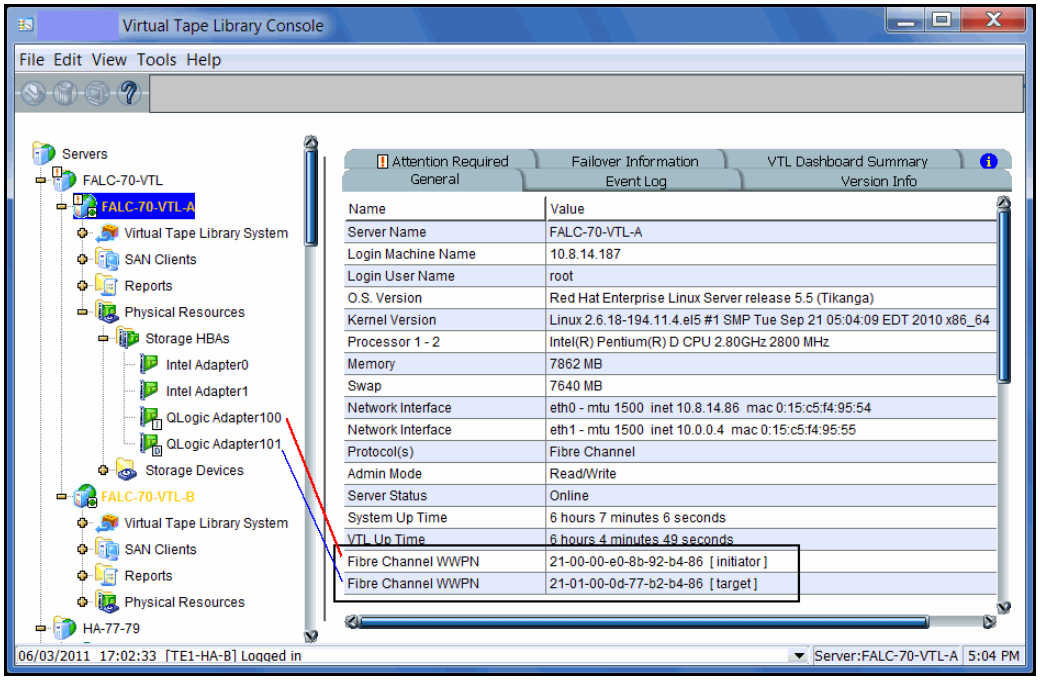
Note: If a port is in initiator mode and has devices attached to it, that port cannot be set for target mode.

To set a port:

1. In the console, expand *Physical Resources*.
2. Right-click an HBA and select *Options* --> *Enable Target Mode*.

   You will get a *Loop Up* message on your COPAN 400 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.



Associate World Wide Port Names with clients

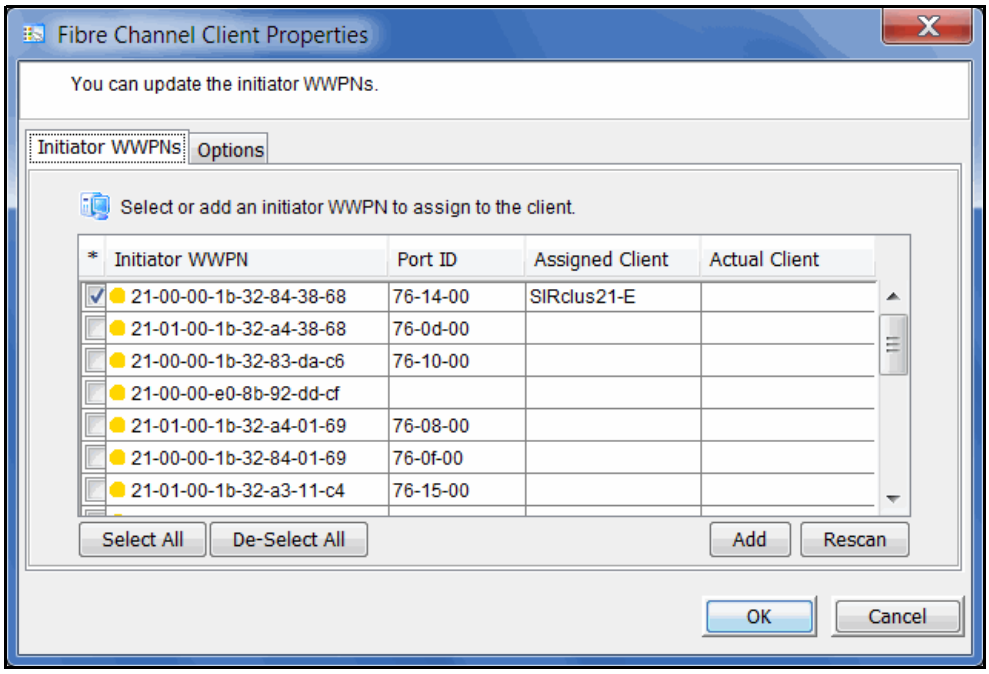
Similar to an IP address, the WWPN uniquely identifies a port in a Fibre Channel environment. Unlike an IP address, the WWPN is vendor assigned and is hardcoded and embedded.

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, COPAN 400 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 boot up or you may have to read it from the physical card. Check with your hardware vendor for their preferred method.

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

1. Highlight the Fibre Channel Client in the console.
2. Right-click the protocol under the client and select *Properties*.



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

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

   - Most Fibre Channel switches allow administration of the switch through an Ethernet port. These administration applications have utilities to reveal or allow

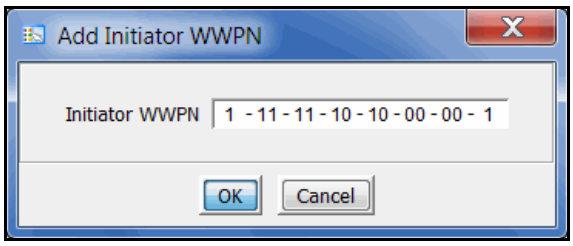
you to change the following: Configuration of each port on the switch, zoning configurations, the WWPNs of connected Fibre Channel cards, and the current status of each connection. You can use this utility to view the WWPN of each Client connected to the switch.

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

- The first time a new Client connects to the COPAN 400 server, the following message appears on the server screen:
FSQLtgt: New Client WWPN Found: 21 00 00 e0 8b 43 23 52

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

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



iSCSI Clients

Overview

The COPAN 400 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 COPAN 400 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

COPAN 400 iSCSI Users are used for iSCSI protocol login authentication from iSCSI backup servers. When you configure access for backup servers, you designate users who can authenticate for the client.

There are several ways to create iSCSI users:

- Use the *Account Management* function in the console and select *COPAN 400 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 COPAN 400 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 COPAN 400 server

Before a backup server (the client initiator) can communicate with a COPAN 400 server, the two entities need to mutually recognize each other. Use an iSCSI initiator on every backup server that will access the COPAN 400 server using iSCSI. This will let you add the COPAN 400 server as a target portal and log the client onto the iSCSI target you create on the COPAN 400 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 COPAN 400 server's IP address or name (if resolvable).

   To determine the IP address, go to the COPAN 400 console. Select the COPAN 400 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

Note: You cannot enable or disable iSCSI if you have already configured failover. If you want to change the state of iSCSI, you need to remove your failover configuration first.

In order to add a client using the iSCSI protocol, you must enable iSCSI for your COPAN 400 server.

If you haven't already done so, right-click your COPAN 400 server in the COPAN 400 console and select *Options* --> *Enable iSCSI*.

The following sections take you through the process of configuring iSCSI clients to work with the COPAN 400 server.

Add an iSCSI client

1. In the 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 COPAN 400 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 COPAN 400 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 COPAN 400 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 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.

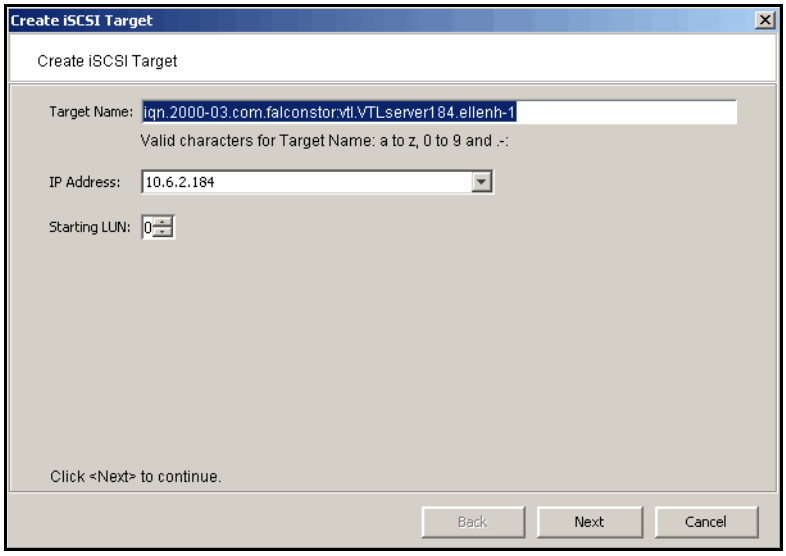
   For unauthenticated access, select *Allow unauthenticated access*. The COPAN 400 server will recognize the client as long as it has an authorized initiator name.
6. Confirm all information and click *Finish*.

Create targets for the iSCSI client to log onto

1. In the console, create at least one virtual iSCSI device (i.e. a virtual tape library) that can be used for iSCSI clients but do not assign it/them to the iSCSI clients until a target is created.

2. Expand the *SAN Clients* object until you see the *iSCSI* object.

3. Right-click the *iSCSI* object and select *Create Target*.



4. Enter a name for the target or accept the default and select the IP address of the adapter on the COPAN 400 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 COPAN 400 server.

   If you are using failover, be sure to select the server's IP address, not the heartbeat IP address, so that clients can see devices while in failover mode.

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 COPAN 400 server, right-click the server node in the console, and select *Options --> Disable iSCSI*.

Note that before disabling iSCSI, all iSCSI initiators and targets for this COPAN 400 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 version of the iSCSI initiator package.
   - If you are running RedHat Enterprise Linux 5.x on a server connected to the internet, you can install the iSCSI package by running the following as root:
     `yum install iscsi-initiator-utils`
   - If you are using a Debian-based distribution on a client connected to the internet, you may be able to install the iSCSI package by running the following as root:
     `apt-get install open-iscsi`
   - If you are using another distribution of Linux, or your client is not connected to the internet, contact your administrator for help in downloading and installing the iSCSI initiator package. If your Linux vendor does not provide a binary package of the iSCSI initiator, the source code is freely available from http://sourceforge.net/projects/linux-iscsi/. Note that you will have to manually compile and install the iSCSI initiator if you chose this method.
2. 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 COPAN 400 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 COPAN 400 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 console.
3. 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:

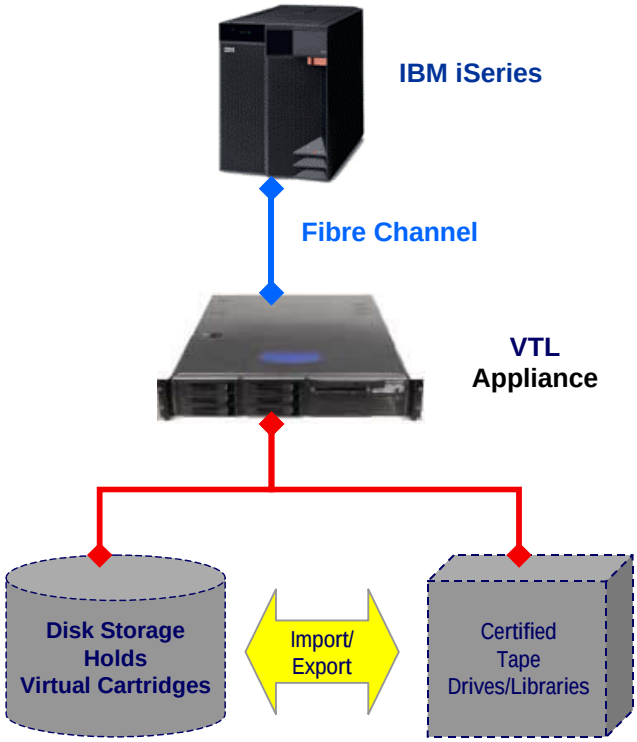
```
cat /proc/scsi/scsi
```

IBM System i Configuration

Overview

IBM System i servers support several types of tape libraries, ranging from relatively simple solutions that can automatically load tapes during operation and maintain a limited cartridge inventory to tape automation systems capable of supporting many systems and managing vast cartridge inventories.

SGI's Virtual Tape Library for IBM System i allows IBM System i systems to connect to a COPAN 400 appliance which emulates IBM 3590 E11 tape library and the IBM 3583 and IBM3584 tape libraries with IBM 3580-TD1, IBM 3580-TD2, and IBM 3580-TD3 tape drives.



Before you begin

Before you can use Virtual Tape Library for IBM System i, your environment must meet the following criteria:

- The System i operating system must be V5R2 or V5R3.
- There must be a Fibre Channel connection between the System i host and the COPAN 400 appliance.
- The AS/400 must use either the IBM 2765 PCI or IBM 5704 PCI-*x* Fibre Channel tape controller or equivalent.
- The COPAN 400 appliance must use a QLogic QLA 234*x* HBA as the Fibre Channel target mode server.

Set up the tape library

With Virtual Tape Library for IBM System i, you use the procedures described earlier in this guide to create a virtual tape library and assign it to an System i host.

Note: When you create a virtual tape library for use with an System i host, you must select IBM3590, IBM3584, or IBM3583 virtual tape library emulation.

In addition, for COPAN 400 import/export, you must use one of the supported tape drives in the physical tape library. This ensures that you have 1:1 data transfer between the virtual volume and the physical tape media.

Once you have created a virtual tape library and assigned it to the host, you should perform the following tasks to ensure that the System i system can see and properly work with the library. (For more information about working with the System i, refer to your System i documentation.)

1. At the System i system, display the library status functions.

   To do this, access the command line and type the following command:

   WRKMLBSTS

2. Make resources available to the tape drive.

   In the option field next to each resource that you want to make available to the tape drive, type 4 (ALLOCATE) and press Enter.

3. Inventory the tape library.

   In the option field next to the tape library, type 9 (INVENTORY) and press Enter.

4. Add a tape to the inventory by typing the following command at the command line:

   ADDTAPCTG DEV(*library device name*) CTG(*cartridge identifier*) CGY(*NOSHARE) CHKVOL(*NO)

   Alternatively, you can use *SHARE400 for the CGY parameter.

After you issue this command, the tape status changes from INSERT to AVAILABLE.

5. Mount a tape onto a drive by typing the following command:

   CHKTAP DEV(*device name*) VOL(*volume identifier*)

   After you issue this command, the tape status changes from AVAILABLE to MOUNTED.

6. Back up a library object by typing the following command:

   SAVLIB LIB(*library name*) DEV(*tape media library device name*) VOL(*volume identifier*)

7. Create a library object by typing the following command:

   CRTLIB LIB(*library name*)

8. Restore a library object by typing the following command:

   RSTLIB SAVLIB(*original library name*) DEV(*tape media library device name*) VOL(*volume identifier*) RSTLIB(*destination library name*)

9. To confirm that the restore worked, display the library object content by typing the following command:

   DSPLIB LIB(*library name*)

10. Delete a library object by typing the following command:

    DLTLIB LIB(*library name*)

11. Unmount a tape by typing the following command:

    CHKTAP DEV(*device name*) VOL(*volume identifier*) ENDOPT(*UNLOAD)

    After you issue this command, the tape status changes from MOUNTED to AVAILABLE.

Import cartridges

The process of adding cartridges to the tape library inventory is called *importing*. Most tape libraries provide an I/O station for adding cartridges without interrupting any automated operation.

To import cartridges:

1. From the console, move the tape from vault to library.
2. At the AS/400, re-inventory the library as described in step 3 in ‘Set up the tape library’.
3. Add the tape into inventory as described in step 4 in ‘Set up the tape library’.

Export cartridges (move to vault)

Cartridges that have been removed from the tape library inventory are referred to as *exported*.

To export a cartridge, type the following command at the command line:

RMVTAPCTG DEV(*library device name*) CTG(*cartridge identifier*)

After you issue this command, if you re-inventory the library from the AS/400, the tape is no longer there. From the console, you can see the tape in the virtual vault.

Hosted Backup

Overview

The Hosted Backup option makes virtual tape libraries and drives available to the local system by allowing certified backup applications to be installed directly onto the COPAN 400 appliance, eliminating the need for a dedicated backup server.

> **Note:** Your backup application should be installed on the /apps partition on your COPAN 400 appliance.

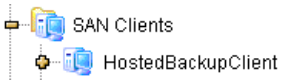
While COPAN 400 natively accelerates backup from the backup server to virtual tape, data transfer between application servers and the backup application is accelerated because the backup application is hosted on the COPAN 400 appliance itself. This shortens the data path between the application server and the backup application/server and therefore enhances backup performance.

Configure Hosted Backup

To configure Hosted Backup:

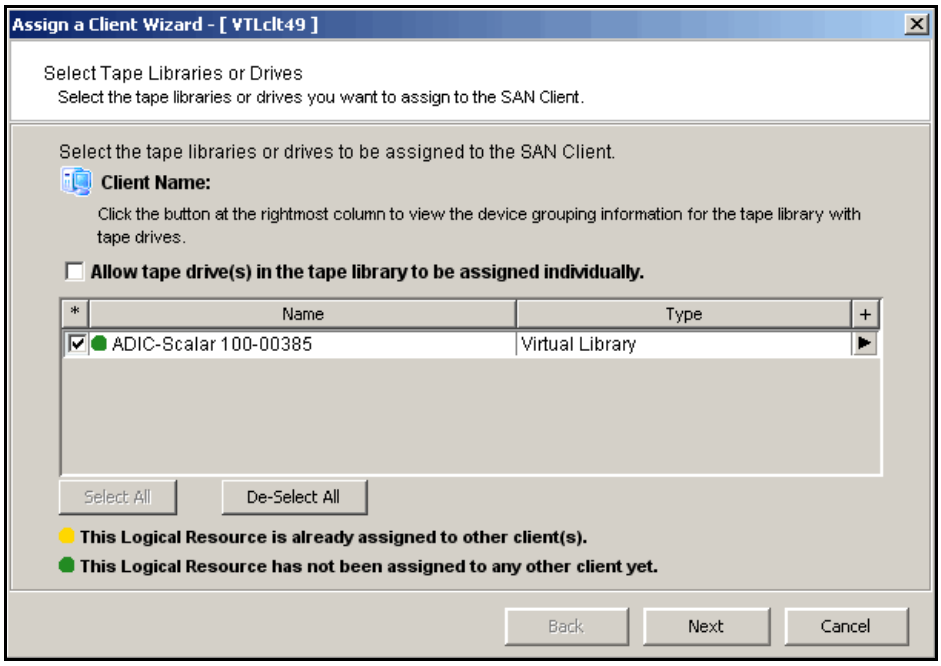
1. Right-click the COPAN 400 server in the console and select *Options* --> *Enable Hosted Backup*.

   After it has been enabled, a new client called *HostedBackupClient* appears under *SAN Clients*.

2. Right-click *HostedBackupClient* and select *Assign* to assign virtual libraries to this client.

3. Select the virtual libraries or drives that this client will use.



Libraries assigned to the *HostedBackupClient* can also be assigned to other clients.

4. Confirm all information and click *Finish*.

If installed, the backup application will now see the devices as local devices. You can use Linux's *cat /proc/scsi/scsi* command on your COPAN 400 appliance to see the library and all of the drives in the library listed as local devices.

```
Host: scsi101 Channel: 00 Id: 02 Lun: 05
  Vendor: STK      Model: T9840B          Rev: 1.33
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 00 Lun: 00
  Vendor: ADIC     Model: Scalar 100      Rev: 2.62
  Type:   Medium Changer                  ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 01 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 02 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 03 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 04 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 05 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 06 Lun: 00
  Vendor: IBM      Model: ULTRIUM-TD1     Rev: 18N2
  Type:   Sequential-Access               ANSI SCSI revision: 03
```

The virtual library and its drives are listed here as local devices.

If the library is not listed in the console, right-click the *Physical Resources* object and select *Discover New Devices* in the dialog.

5. Verify that the following rpm packages are installed on the COPAN 400 server:

   All backup software:

   - audit-libs-1.7.7-6.el5.i386.rpm
   - cracklib-2.8.9-3.3.i386.rpm
   - glibc-2.5-34.i686.rpm
   - glibc-2.5-34.x86_64.rpm
   - glibc-common-2.5-34.x86_64.rpm
   - libacl-2.2.39-3.el5.i386.rpm
   - libattr-2.4.32-1.1.i386.rpm
   - libICE-1.0.1-2.1.i386.rpm
   - libselinux-1.33.4-5.1.el5.i386.rpm
   - libsepol-1.15.2-1.el5.i386.rpm
   - libSM-1.0.1-3.1.i386.rpm
   - libXp-1.0.0-8.1.el5.i386.rpm
   - libXt-1.0.2-3.1.fc6.i386.rpm
   - libXtst-1.0.1-3.1.i386.rpm
   - ncurses-5.5-24.20060715.i386.rpm
   - pam-0.99.6.2-4.el5.i386.rpm
   - pam-0.99.6.2-4.el5.x86_64.rpm
   - xinetd-2.3.14-10.el5.x86_64.rpm

   Veritas NetBackup 6.5.4:

   - libattr-2.4.32-1.1.i386.rpm
   - libacl-2.2.39-3.el5.i386.rpm

   EMC Networker 7.5:

   - xorg-x11-filesystem-7.1-2.fc6.noarch.rpm
   - libXau-1.0.1-3.1.x86_64.rpm
   - libXdmcp-1.0.1-2.1.x86_64.rpm
   - libXp-1.0.0-8.x86_64.rpm
   - libXrender-0.9.1-3.1.x86_64.rpm
   - libSM-1.0.1-3.1.x86_64.rpm
   - libXext-1.0.1-2.1.x86_64.rpm
   - libXpm-3.5.5-3.x86_64.rpm
   - libXft-2.1.10-1.1.x86_64.rpm
   - libICE-1.0.1-2.1.x86_64.rpm
   - libXmu-1.0.2-5.x86_64.rpm
   - libjpeg-6b-37.x86_64.rpm
   - fontconfig-2.4.1-6.el5.x86_64.rpm
   - libXt-1.0.2-3.1.fc6.x86_64.rpm
   - libpng-1.2.10-7.x86_64.rpm
   - libX11-1.0.3-8.el5.x86_64.rpm
   - openmotif-2.3.0-0.3.el5.x86_64.rpm

IBM Tivoli Storage Manager 6.1:

- libaio-0.3.96-3.i386.rpm
- libaio-0.3.96-3.x86_64.rpm
- compat-libstdc++-33-3.2.3-61.i386.rpm
- compat-libstdc++-33-3.2.3-61.x86_64.rpm
- xorg-x11-filesystem-7.1-2.fc6.noarch.rpm
- libXau-1.0.1-3.1.x86_64.rpm
- libXdmcp-1.0.1-2.1.x86_64.rpm
- libXp-1.0.0-8.x86_64.rpm
- libXrender-0.9.1-3.1.x86_64.rpm
- libSM-1.0.1-3.1.x86_64.rpm
- libXext-1.0.1-2.1.x86_64.rpm
- libXpm-3.5.5-3.x86_64.rpm
- libXft-2.1.10-1.1.x86_64.rpm
- libICE-1.0.1-2.1.x86_64.rpm
- libXmu-1.0.2-5.x86_64.rpm
- libjpeg-6b-37.x86_64.rpm
- fontconfig-2.4.1-6.el5.x86_64.rpm
- libXt-1.0.2-3.1.fc6.x86_64.rpm
- libpng-1.2.10-7.x86_64.rpm
- libX11-1.0.3-8.el5.x86_64.rpm
- openmotif-2.3.0-0.3.el5.x86_64.rpm

If they are not installed, Oracle Linux RPMs can be downloaded from http://public-yum.oracle.com/repo/EnterpriseLinux/EL5/.

Refer to your backup application's own documentation to determine if there are any additional packages that may be needed.

6. If not yet installed, install your backup application and configure it.

   Your backup application should be installed on the /apps partition on your COPAN 400 appliance.

   If the operating system sees the hosted backup devices but the backup application does not, you may need to rescan devices from the backup application or restart the backup application services in order to see the devices.

Important note about tape and library devices: Any time you add or remove physical or virtual devices on the COPAN 400 server and then reboot the server, you will need to check that the paths of the assigned tape and library devices are in the correct sequence in your backup software. If they are not in the correct sequence, you will need to reconfigure the paths.

Stopping COPAN 400 processes with Hosted Backup

If you are using the Hosted Backup option, you must make sure to stop the backup application before stopping COPAN 400.

NDMP Backup Support

Overview

The *NDMP Backup Support* option allows certified backup applications and industry standard NAS devices (i.e. NetApp filers) to perform backup and restore using the NDMP protocol over an IP network.

With the *NDMP Backup Support* option, the COPAN 400 appliance acts as an NDMP server, centralizing management by eliminating locally attached tape devices from each NAS device. When a backup occurs, data is moved from the NAS device directly to the virtual library.

The *NDMP Backup Support* option supports the following:

- NDMP v2, 3, 4
- The following data transfer models:
  - Filer to direct-attach tape drive (local filer)
  - Filer to another filer attached tape drive (filer-to-filer)
  - Filer to *NetVault* Client/Server attached tape drive (filer-to-server)
  - *NetVault* Client/Server to filer attached tape drive (server/client-to-filer)
- Library and tape sharing
- Direct Access Restores (DAR)

Notes:

- The NDMP Backup Support option is not needed when presenting a virtual tape library over FC to a NAS filer as a replacement for a physical library.
- Before you begin configuration, you must define the hostname of the COPAN 400 server in the /etc/hosts file in the format "IPAddress Hostname".
  For example: 10.7.2.41 Server41
- Because some backup applications use NDMP, if you are running backup software on the COPAN 400 server, it should be started after COPAN 400 has started and should be stopped before COPAN 400 is stopped. Otherwise, the NDMP service that is loaded by the backup software may interfere with COPAN 400's NDMP service.

Configure NDMP support

To configure NDMP support:

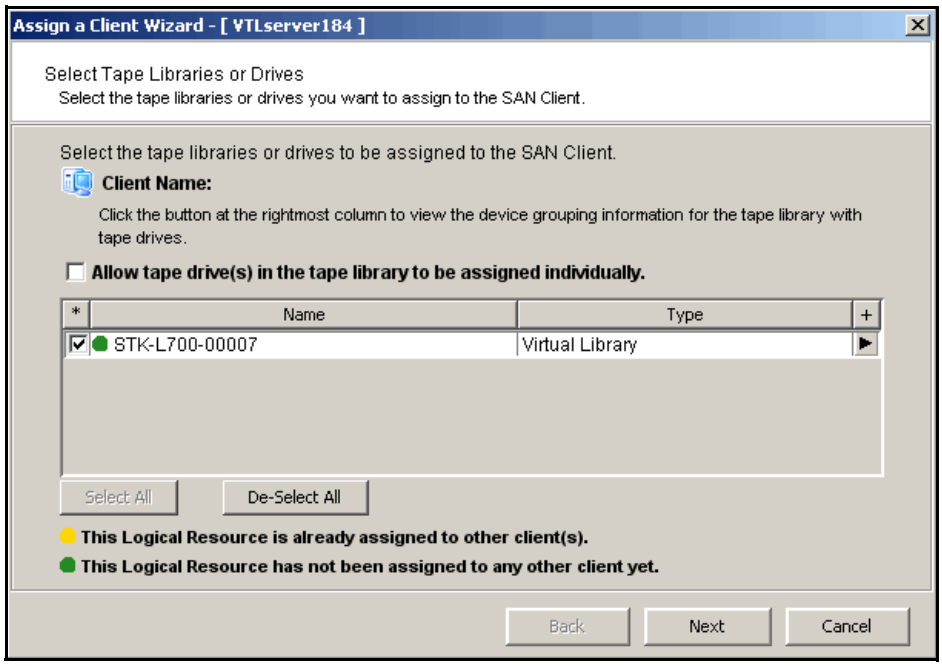
1. Right-click your COPAN 400 server and select *Options* --> *NDMP* --> *Enable NDMP*.

2. Enter the user name and password the backup server will use to talk to NDMP.

   You must enter the same user name/password into the NDMP module in your backup application.

3. Right-click *HostedBackupClient* and select *Assign* to assign virtual libraries to this client.

4. Select the virtual libraries or drives that this client will use.



   HostedBackupClient can have any number of virtual libraries assigned to it. Conversely, libraries assigned to the *HostedBackupClient* can also be assigned to other clients.

5. Confirm all information and click *Finish*.

The backup application will now see the devices as local devices. You can use Linux's *cat /proc/scsi/scsi* command on your COPAN 400 appliance to see the library and all of the drives in the library listed as local devices.

```
[root@VTLserver184 bin]# cat /proc/scsi/scsi
Attached devices:
Host: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA      Model: ST3808110AS      Rev: J
  Type:   Direct-Access                    ANSI SCSI revision: 05
Host: scsi0 Channel: 00 Id: 08 Lun: 00
  Vendor: DP       Model: BACKPLANE        Rev: 1.00
  Type:   Enclosure                        ANSI SCSI revision: 05
Host: scsi101 Channel: 00 Id: 00 Lun: 00
  Vendor: FALCON   Model: IPSTOR DISK      Rev: v1.0
  Type:   Direct-Access                    ANSI SCSI revision: 04
Host: scsi101 Channel: 00 Id: 03 Lun: 00
  Vendor: FALCON   Model: IPSTOR DISK      Rev: v1.0
  Type:   Direct-Access                    ANSI SCSI revision: 03
Host: scsi101 Channel: 00 Id: 03 Lun: 01
  Vendor: STK      Model: L700             Rev: 3.05
  Type:   Medium Changer                   ANSI SCSI revision: 03
Host: scsi101 Channel: 00 Id: 03 Lun: 02
  Vendor: STK      Model: T9840B           Rev: 1.30
  Type:   Sequential-Access                ANSI SCSI revision: 03
Host: scsi101 Channel: 00 Id: 03 Lun: 03
  Vendor: STK      Model: T9840B           Rev: 1.30
  Type:   Sequential-Access                ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 00 Lun: 00
  Vendor: STK      Model: L700             Rev: 3.05
  Type:   Medium Changer                   ANSI SCSI revision: 03
Host: scsi32 Channel: 00 Id: 01 Lun: 00
  Vendor: STK      Model: T9840B           Rev: 1.33
```

The virtual library and its drives are listed here as local devices.

Important notes about NDMP devices:

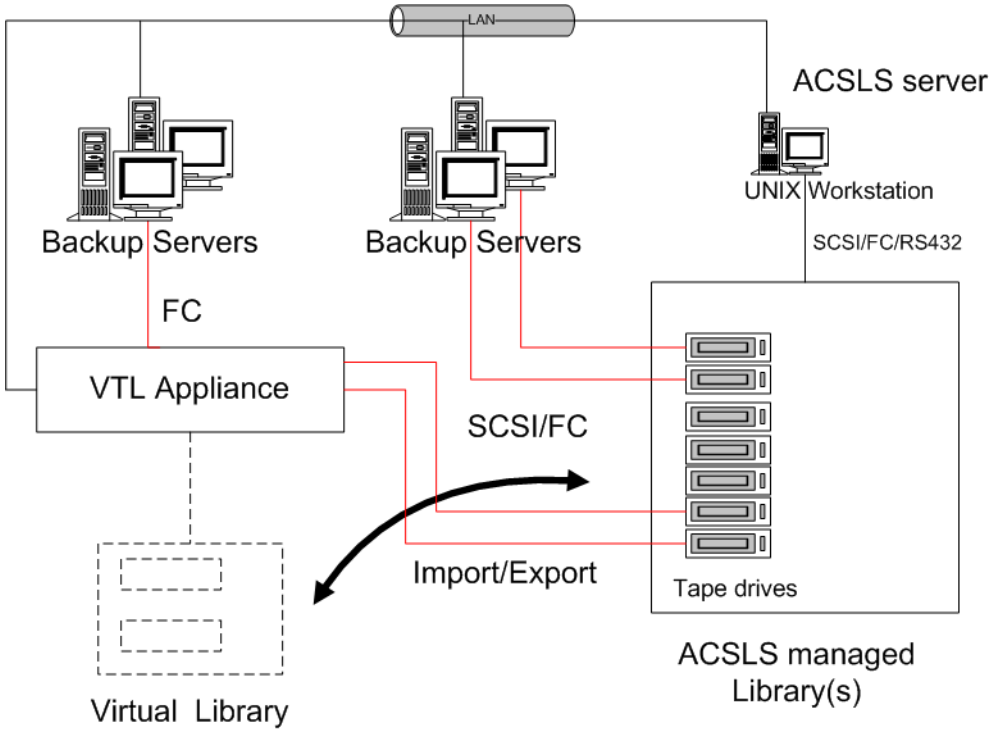
- Any time you add or remove physical or virtual devices on the COPAN 400 server and then reboot the server, you will need to check that the paths of the assigned NDMP devices are in the correct sequence in Veritas NetBackup. If they are not in the correct sequence, you will need to reconfigure the paths.
- If you are using a physical library assigned as an NDMP device to your client, make sure that this library is not assigned for any other COPAN 400 functions.

ACSLS and Library Station Configuration

Overview

ACSLS Manager™ and Library Station software manage heterogeneous StorageTek tape libraries.

The ACSLS/Library Station option works with ACSLS/Library Station-managed tape libraries, allowing the system to share ACSLS/Library Station-managed libraries among the COPAN 400 server and your backup servers. This makes it possible to import data from physical tapes and export data on virtual tapes to physical tapes.



Hardware configuration

1. Physically connect the tape drives that will be assigned to the COPAN 400 appliance.

   Note: Physical tape drives cannot be shared with COPAN 400 appliances or other applications.

2. (ACSLS only) Create at least one storage pool on the ACSLS server for COPAN 400 and assign tapes to it.

   If you have already created a pool, you can use that one.

3. Make a note of the following:
   - ACS IDs, LSM IDs, Panel IDs, and Device IDs of the libraries that hold the tape drives connected to COPAN 400. You can run the cmd.proc utility on your ACSL server to determine the IDs. For Library Station users, check with your Library Station administrator to determine the IDs.
   - IP address of the ACSLS/Library Station server.
   - (ACSLS only) IDs of the storage pools to be assigned to the COPAN 400 appliance.

4. Make sure that the COPAN 400 server and the ACSLS/Library Station server can communicate with each other.

Configure COPAN 400 to work with ACSLS

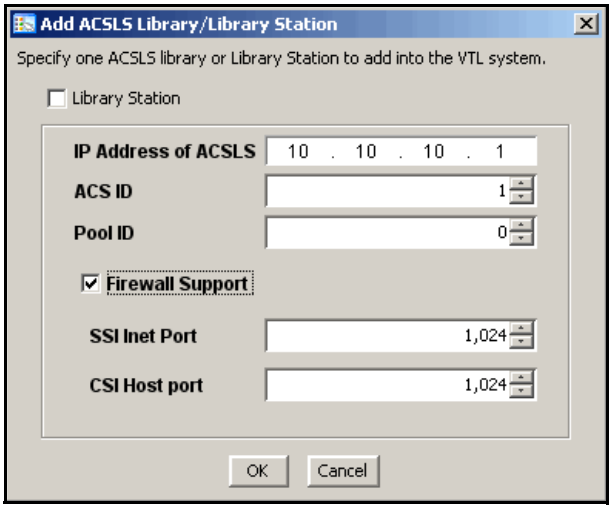
The following instructions give you an overview of the steps you must follow to configure your ACSLS/Library Station option. Refer to the appropriate sections in this User Guide for more detailed information.

1. Launch the console and connect to the COPAN 400 appliance.

2. Right-click your COPAN 400 server and select *System Maintenance --> Network Configuration* to make sure DNS is configured properly.

   Enter the *Domain Name*, select *Append suffix to DNS lookup* and enter the DNS server IP address.

3. Right-click the *Physical Tape Libraries* object and select *Add ACSLS/Library Station.*



4. Enter the IP address of the ACSLS/Library Station server; the ACS ID and the Pool ID of the ACSLS/Library Station library.

   Once completed, the server automatically does an inventory to obtain a list of physical tapes.

5. If applicable, enter your firewall information.

   If you select the *Firewall Support* option, you need to edit the /usr/local/sgi/vtl/etc/acsls_ls_cdk.conf file and add the following lines:

   ```
   CSI_HOSTPORT=[ACSLS assigned port number]
   SSI_INET_PORT=[ACSLS assigned port number]
   ```

   If you **do not** select the *Firewall Support* option, the *portmap* process needs to be running. Otherwise, the system will fail to assign or retrieve the library's status after restarting COPAN 400 services or rebooting. To enable *portmap* on RedHat/CentOS, run the following command: chkconfig --add portmap

6. Assign your physical tape drives to your ACSLS/Library Station tape library.

   You will have to enter the *Drive ID* for each. The *Drive ID* is comprised of the drive's ACS ID, LSM ID, Panel ID, and Device ID in the format n,n,n,n

   You can run the cmd.proc utility on your ACSL server to determine the IDs. For Library Station users, check with your Library Station administrator to determine the IDs. You may want to supply the administrator with the drive's SCSI address to help him determine the IDs.

Set eject policy

You need to edit the /usr/local/sgi/vtl/etc/acsls_ls_cdk.conf file to set how many tapes will be ejected after each backup.

Enter your policy information in the following format:

```
RepositoryID:ACSLS/LS IP:acsid:poolid:eject
```

In the following example:

```
4:10.6.2.62:1:2:5
```

- 4 is the Repository/Database ID. (This can be found in the COPAN 400 console by clicking on the *Database* object.)
- 10.6.2.62 is the IP address of the ACSLS/Library Station.
- 1 is the ACS ID.
- 2 is the Pool ID.
- 5 is the eject value. In this example, after each backup, the system will eject five tapes at a time. This is usually set to the same value as the *CAP size*.

Filter tapes displayed in the COPAN 400 console

If you pool physical tapes in Library Station and you *only* want to display a range of Library Station barcodes in the console, you will need to edit the /usr/local/sgi/vtl/etc/acsls_ls_cdk.conf file.

Locate the following sections:

```
#Library Station barcode filters...
#end Library Station barcode filters
```

Enter your range information **between** these sections (before the `#end` line) in the following format:

```
RepositoryID:ACSLS/LS IP:acsid:startrange-endrange:startrange-endrange
```

The barcode length should be six characters and spaces should not be used. Any number of barcode ranges can be specified. In the following example:

```
4:10.6.2.62:6:000000-004444:AA0000-AA8888
```

- 4 is the Repository ID. (This can be found in the COPAN 400 console by clicking on the *Database* object.)
- 10.6.2.62 is the IP address of the ACSLS/Library Station.
- 6 is the ACS ID.
- 000000-004444 is the first range to display.
- AA0000-AA8888 is the next range to display.

Configure ACSLS to work with Failover

When Failover is enabled and ACSLS is configured, you must make the following modification to the /etc/hosts file so that ACSLS will continue to function after a takeover (when the secondary server takes over for the primary).

1. Change the virtual IP to the heartbeat IP of both servers in the set.
2. Run the following command on both servers:

```
revolution restart tleupcall
```

Add/remove tapes

Whenever you add or remove tapes from an ACSLS/Library Station pool, you must inventory the tapes through the COPAN 400 console (right-click the physical library and select *Inventory)*.

Email Alerts

COPAN 400 includes a unique customer support utility that proactively identifies and diagnoses potential system or component failures and automatically notifies system administrators via email.

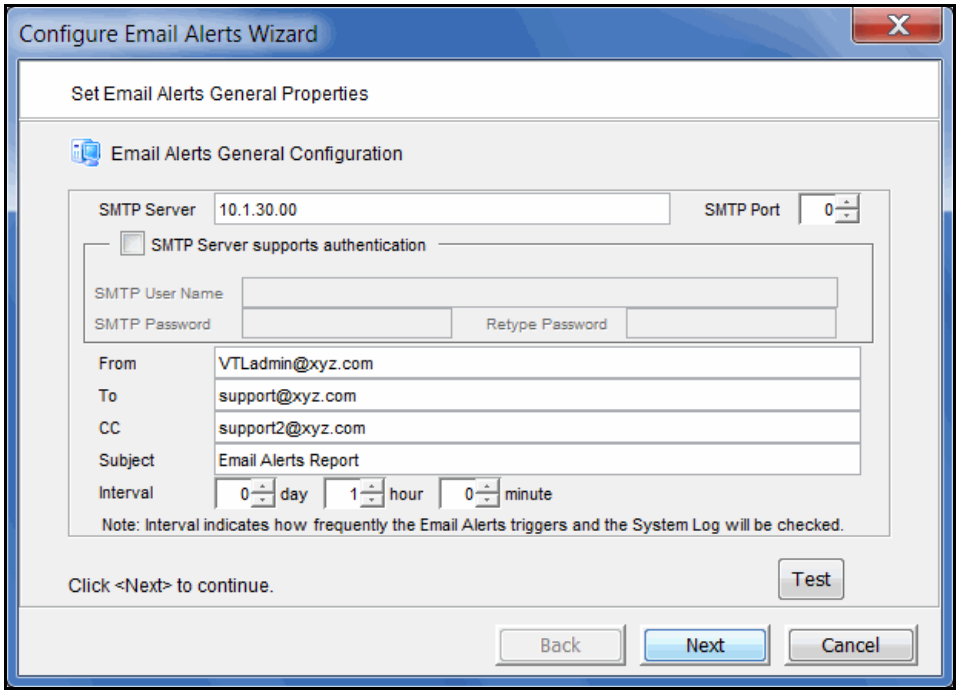
Using pre-configured scripts (called *triggers*), Email Alerts monitors a set of pre-defined, critical system components (memory, disk, SCSI drive errors, offline device, etc.) and system log messages. With its open architecture, administrators can easily register new elements to be monitored by these 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 server and select *Options* --> *Enable Email Alerts*.
2. Enter general information for your Email Alerts configuration.



SMTP Server - Specify the mail server that Email Alerts should use to send out notification emails. You can enter an IP address or hostname consisting of alphabet letters, numbers, "_", "-", or ".". The maximum length is 255 characters.

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 - If you enabled the authentication option on the SMTP server, specify the user account that will be used by Email Alerts to log into the mail server. Email Alerts may not work if the SMTP username and password are set without authentication.

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.

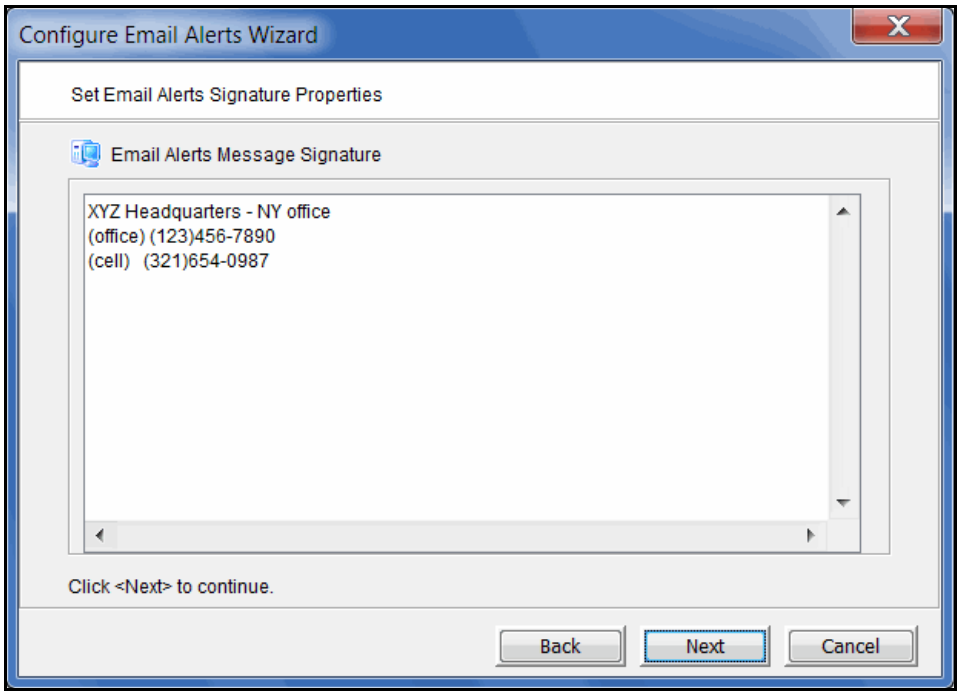
CC - Specify any other email accounts that should receive emails from Email Alerts.

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

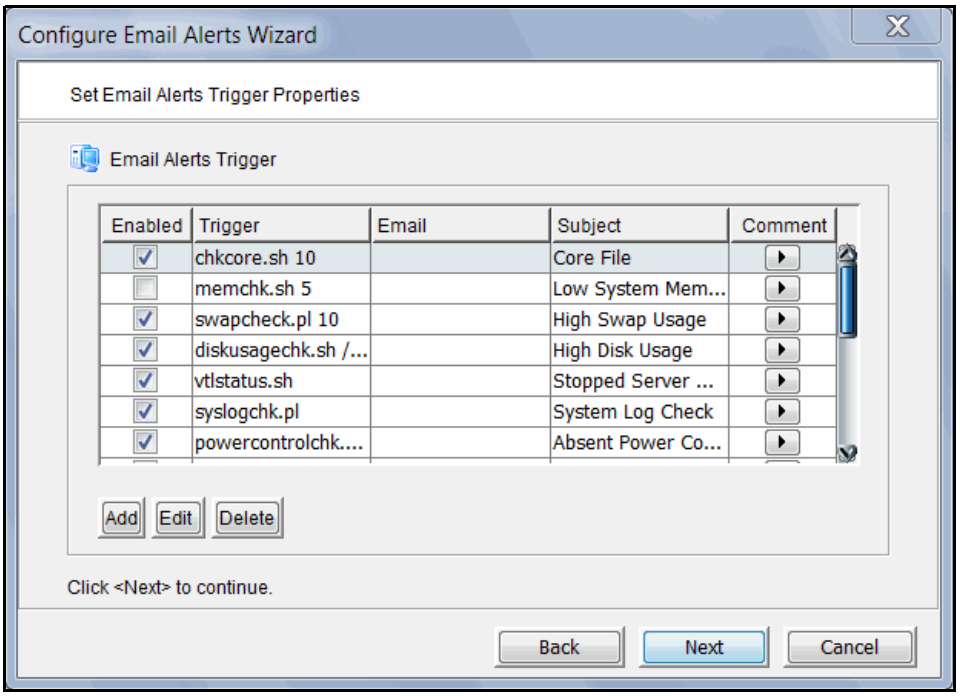
Interval - Specify how frequently the Email Alerts triggers and the System Log should be checked. This interval works in conjunction with the “-memorize” argument for the “syslogchk.pl” trigger to limit the number of alerts that will be sent for the same event.

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.



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



Triggers are the scripts/programs that perform various types of error checking. By default, SGI includes scripts/programs that check for low system memory, low disk space, and relevant new entries in the system log.

The following scripts are pre-defined:

chkcore.sh 10 (Core file check) - This script checks to see if a memory core file has been created by the operating system in the bin directory of the server. If a core file is found, Email Alerts compresses it, deletes the original, and sends an email alert but does not send the compressed core file (which can still be large). If there are more than 10 (default) compressed core files, the oldest ones will be deleted.

memchk.sh 5 (Memory check) - This script checks available system memory. If the percentage is below the specified value (default 5%), an email alert is sent.

swapcheck.pl 10 (Memory swap usage check) - This script checks available swap memory. If the percentage is below the specified value (default 80), an email alert is sent with the total swap space and the swap usage.

diskusagechk.sh / 95 (Disk usage check) - This script checks disk space usage of the specified device(s). If the current percentage is over the specified percentage (default is 95), an email alert is sent. To check usage for multiple disks, append multiple “mount point/threshold” parameters. For example, “diskusagechk.sh / 95 /usr 80” will check “/” and “/usr” with thresholds of 95 and 80, respectively.

vtlstatus.sh (COPAN 400 status check) - This script checks server module status. If any module has stopped, an email alert is sent.

syslogchk.pl (System log check) - This script looks at the last 20 MB of messages in the system log. If any message matches what was defined on the *System Log Check* dialog and does not match what was defined on the *System Log Ignore* dialog, an email alert is sent with an attachment that includes all files in $ISHOME/etc and $ISHOME/log.

If you want to limit the number of email alerts for the same System log event or category of events, set the –memorize parameter to the number of minutes to remember each event. If the same event is detected in the previous Email Alerts interval, no email alert is sent for that event. If an event is detected several times during the current interval, the first occurrence is reported in the email that is sent for that interval and the number of repetitions is indicated at the end of the email body with the last occurrence of the message. The default value is the same as the Email Alerts interval that was set on the first dialog (or the *General* tab if Email Alerts is already configured).

powercontrolchk.pl -interval 1440 (Power control check) - This script checks the server configuration file once a day (by default) and sends an email alert if the power control option is missing in a failover configuration.

processchk.pl -interval 60 (System process check) - This script checks system processes and sends an email alert if there are processes using more than 1 GB of non-swapped physical memory. This script also sends an email alert if there are processes using more than 90% of CPU usage.

zombiechk.pl 10 -interval 1440 (Defunct process check) - This script checks system processes once a day (by default) and sends an email alert if there are 10 (default) or more defunct processes.

neterrorchk.pl -interval 60 (Network configuration check) - This script uses the 'ifconfig' command to check network configuration and sends an email alert if there are any network errors, overruns, dropped events, or network collisions.

netconfchk.pl -interval 1440 (Inactive network interfaces/invalid broadcasts check) - This script uses the 'ifconfig' command to check network configuration once a day (by default) and sends an email alert if there are any network devices set to '_tmp' or any broadcast addresses that do not match the IP and netmask rules.

fcchk.pl -interval 60 (QLogic HBA check) - This script checks each QLogic adapter initiator port and sends an email alert if there is a status change from *Online* to *Not Online*. The script also checks QLogic link status and sends an email alert if the status of FC Link Down changes from *OK* to *Not OK*.

promisecheck.pl 10.x.x.x administrator password -interval 10 (Promise storage check) - This script checks events reported by Promise storage hardware every 10 minutes (by default) and sends an email alert if there is an event with a category other than *Info*. This trigger needs to be enabled on-site and requires the IP address and user/password account needed to access the storage via *ssh*. The *ssh* service must be enabled and started on the Promise storage.

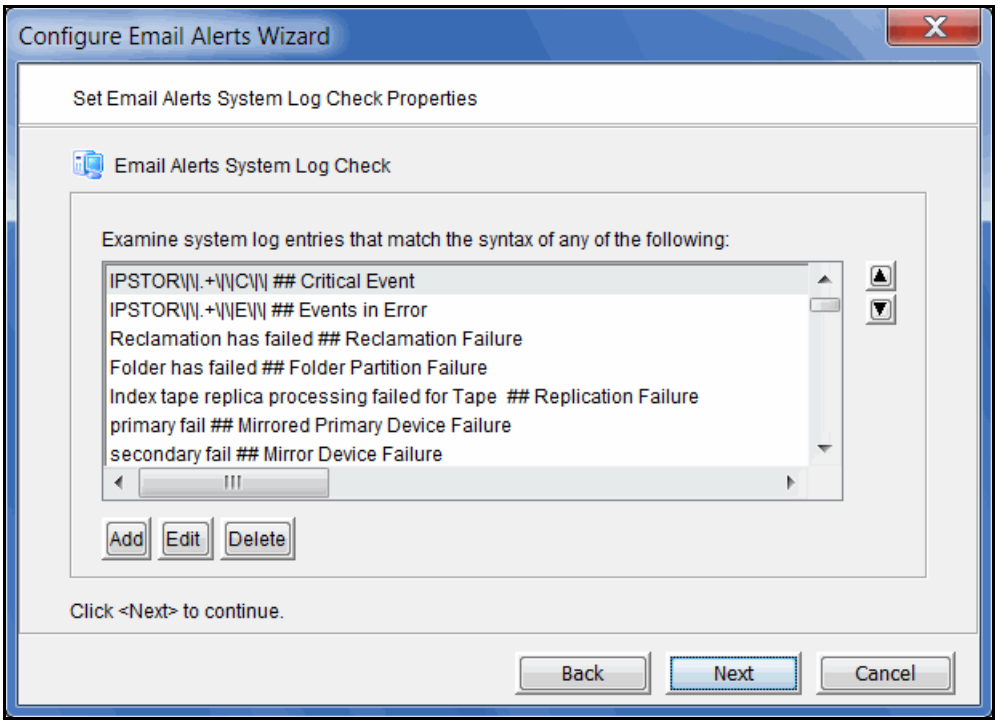
scsitimeoutchk.pl -interval 60 (Storage connection check) - This script checks if a SCSI connection has timed out.

activity.pl (Activity check) - This script checks to see if an *fsstats* activity statistics file exists. If it does, an email alert is sent with the activity file attached.

reportheartbeat.pl (Heartbeat check) - This script checks to see if the server is active. If it is, Email Alerts sends an email every 24 hours, by default, to report that the server is alive. You can change the default interval with the parameter '*-interval <value in minutes>*'.

If you need to modify an existing script or create a new script/program, refer to 'Script/program trigger information' for more information. You cannot delete the predefined triggers.

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



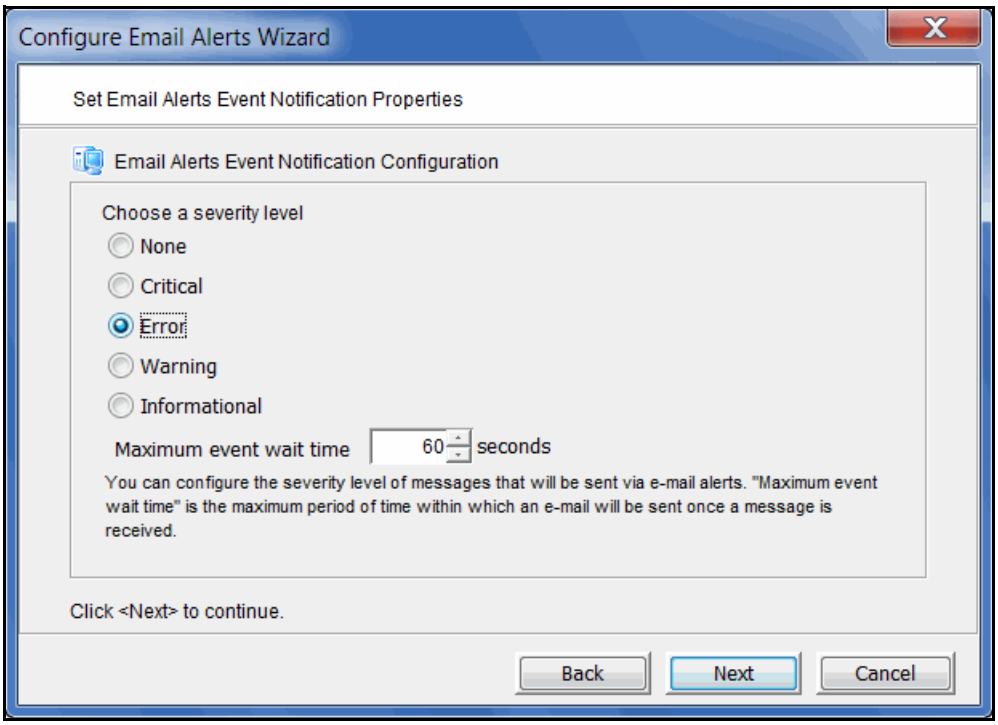
The system log records important events or errors that occur in the system, including those generated by the server.

This dialog allows you to rule out entries in the system log that have nothing to do with the server, and to list the types of log entries generated by the server 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 the server.

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 system log messages that should be sent as email alerts.



   If you selected the syslogchk.sh trigger on the *Email Alerts Trigger* tab, you can select *None* here. You will still get alerts for critical events and errors because they are listed as *included* on the *Email Alerts System Log Check* tab.

   If you want to include warnings or informational messages, you can select them here or you can go back to the *Email Alerts System Log Check* tab and add them there.

   If you select them here, critical and error alerts will be sent based on the interval set on the *Email Alerts General Configuration* tab and on the *Maximum event wait time* set below. Warnings/informational messages will only be sent based on the *Maximum event wait time*.

   If you add warnings and/or informational messages on the *Email Alerts System Log Check* tab and select *None* here, alerts will only be sent based on the interval set on the *Email Alerts General Configuration* tab.

   Maximum event wait time is the maximum period of time within which an email will be sent once a system log 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 on your 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, SGI includes several scripts/programs that check for low system memory, changes to the server 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 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 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 COPAN 400 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 COPAN 400 module has stopped, this trigger generates a return code of 1 and sends an email.

COPAN 400 Server

COPAN 400 servers are designed to require little or no maintenance.

All day-to-day administrative functions can be performed through the 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.

The following commands are available:

- revolution start - Starts the COPAN 400 server processes. When you start the server, you will see the processes start.
- revolution restart - Stops and then starts the COPAN 400 server processes
- revolution status - Checks the status of the COPAN 400 server processes. You will see a list of processes that are currently running.
- revolution stop - Stops the COPAN 400 server processes. You will see each process stop.

Important notes about stopping COPAN 400

Warning: Stopping the COPAN 400 Server processes will detach all virtual devices. To prevent data loss, we recommend stopping all COPAN 400 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 COPAN 400.

Server processes

When you run a server command, you will see a list of processes. Your list will look similar to the following, depending upon which COPAN 400 options you are using:

Status of COPAN 400 Configuration Module	[RUNNING]
Status of COPAN 400 Base Module	[RUNNING]
Status of COPAN 400 HBA Module	[RUNNING]
Status of COPAN 400 Authentication Module	[RUNNING]
Status of COPAN 400 Server (Compression) Module	[RUNNING]
Status of COPAN 400 Server (HiFn HW Compression) Module	[RUNNING]
Status of COPAN 400 Server (FSNBase) Module	[RUNNING]
Status of COPAN 400 Server (Upcall) Module	[RUNNING]
Status of COPAN 400 Server (Transport)	[RUNNING]
Status of COPAN 400 Server (Event) Module	[RUNNING]
Status of COPAN 400 Server (Path Manager) Module	[RUNNING]
Status of COPAN 400 Server (Application)	[RUNNING]
Status of COPAN 400 Server VTL Upcall Module	[RUNNING]
Status of COPAN 400 Server VTL Upcall Daemon	[RUNNING]
Status of COPAN 400 Server VTL Module	[RUNNING]
Status of COPAN 400 Memory Map Module	[RUNNING]
Status of COPAN 400 Target Module	[RUNNING]
Status of COPAN 400 iSCSI Target Module	[RUNNING]
Status of COPAN 400 iSCSI (Daemon)	[RUNNING]
Status of COPAN 400 Communication Module	[RUNNING]
Status of COPAN 400 CLI Proxy Module	[RUNNING]
Status of COPAN 400 Logger Module	[RUNNING]
Status of COPAN 400 Email Alerts Module	[RUNNING]
Status of COPAN 400 Self Monitor Module	[RUNNING]
Status of COPAN 400 SNMPD Module	[RUNNING]

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

Process	Description
COPAN 400 Configuration	QLogic FC initiator module provides configuration and interaction between the COPAN 400 server and the FC environment/storage.
COPAN 400 Base	QLogic FC initiator module provides configuration and interaction between the COPAN 400 server and the FC environment/storage.
COPAN 400 HBA	QLogic FC initiator module provides configuration and interaction between the COPAN 400 server and the FC environment/storage.
COPAN 400 Authentication	Security authentication module for connections.
COPAN 400 Server (Compression)	Provides software compression engines for COPAN 400.
COPAN 400 Server (HiFn HW Compression)	Provides hardware compression engines for COPAN 400.
COPAN 400 Server (FSNBase)	Provides basic IO services to the kernel modules.
COPAN 400 Server (Upcall)	Handles interactions between kernel and user mode components.
COPAN 400 Server (Transport)	Provides support for replication.
COPAN 400 Server (Event)	Provides message logging interface to the syslog.
COPAN 400 Server (Path Manager)	Manages the IO paths to the storage.
COPAN 400 Server (Application)	Provides core IO services to the rest of the application.
COPAN 400 Server VTL Upcall	Provides a kernel-to-user mode interface for communication with the ACSLS server.
COPAN 400 Server VTL Upcall Daemon	Provides a kernel-to-user mode interface for communication with the ACSLS server.
COPAN 400 Server VTL	Provides the tape drive/library emulation and interaction to physical tape libraries.
COPAN 400 Server Memory Map	Allows mapping of physical memory (not managed by Linux memory manager).
COPAN 400 Server Hosted Backup	Provides virtual libraries and drives to a local Linux system.
COPAN 400 Target Module	Provides Fibre Channel target functionality.
COPAN 400 iSCSI Target	Provide iSCSI target functionality.

Process	Description
COPAN 400 iSCSI (Daemon)	Handles the login process from an iSCSI initiator.
COPAN 400 Communication	Handles console-to-server communication and manages overall system configuration information.
COPAN 400 CLI Proxy	Facilitates communication between the CLI utility and a COPAN 400 server.
COPAN 400 Logger	Provides the logging function for COPAN 400 reports.
COPAN 400 Email Alerts	Provides Email Alerts functionality.
COPAN 400 Self Monitor	Self-monitor process that checks the server's own health.
COPAN 400 Failover Module	Provides failover functionality.
COPAN 400 SNMPD	An agent that processes SNMP requests and returns the information to the sender/requester i.e. SNMP management software.

Command Line

(COPAN 400) provides a simple utility that allows you to perform some of the more common COPAN 400 functions at a command line instead of through the console. You can use this command line utility to automate many tasks, as well as integrate COPAN 400 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 COPAN 400 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	COPAN 400 server name (hostname or IP address)
-u	--server-username	COPAN 400 server username
-p	--server-password	COPAN 400 server user password
-c	--client-name	COPAN 400 client name
-v	--vdevid	COPAN 400 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 COPAN 400 Server

Log in to the COPAN 400 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 COPAN 400 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 1,800 seconds.

Log out from the COPAN 400 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 COPAN 400 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> | -B <barcode>] [-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> | --barcode=<barcode>]
[--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.

-v (--vdevid) or -n (--vdevname) are options to query and report a single device. Cannot be combined with -B (--barcode).

-B (--barcode) is an option to query and report virtual tapes by barcode. The format for this argument is a list of barcodes separated by commas.

-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 1,800 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.

-c (--client-name) is required 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 1,800 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 Fibre Channel 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 an 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 1,800 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 1,800 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 1,800 seconds.

Assign virtual device

```
iscon assignvdev -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> -a <access-mode> [-y]
[-I <initiatorWWPN|*>] [-T <targetWWPN|*> [-l <lun>]
[-X <rpc-timeout>]

iscon assignvdev --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --vdevid=<vdevid>
--client-name=<client-name> --access-mode=<access-mode> [--vlib-only]
[--initiatorWWPN=<initiatorWWPN|*>] [--targetWWPN=<targetWWPN|*> [--lun=<lun>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command 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.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Add iSCSI client

```
iscon addiscsiclient -s <server-name> [-u <username> -p <password>]
-c <client-name> -I <initiator-name-list>
[-a <user-name-list>] [-X <rpc-timeout>]

iscon addiscsiclient --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--client-name=<client-name> --initiator-name-list=<initiator-name-list>
[--user-name-list=<user-name-list>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command allows you to add an ISCSI 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 the client name: <>"&$/\'

-I (--initiator-name-list) is required to provide at least one valid initiator name. Multiple names must be separated with commas.

-a (--user-name-list) is an option to limit client access to specified iSCSI users. There must be an existing iSCSI user account for each name specified. Multiple names must be separated with commas. By default, the client will allow unauthenticated access.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Assign virtual library or drive to an iSCSI client target

```
iscon assignvdevtoiscsiclient -s <server-name> [-u <username> -p <password>]
-v <vdevid> -c <client-name> -r <iscsi-target-id> [-y] [-l <lun>] [-X <rpc-timeout>]

iscon assignvdevtoiscsiclient --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --client-name=<client-name> --iscsi-target-id=<iscsi-target-id>
[--vlib-only] [--lun=<lun>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command attaches a virtual library or drive to an iSCSI client target.

-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 name to assign the virtual tape library or drive to.

-r (--iscsi-target-id) is required to provide the iSCSI target ID.

-y (--vlib-only) is an option for virtual tape library assignment. The default is to assign all of the virtual tape drives in the library. This option allows you to assign the virtual tape library to the client without assigning all of the virtual tape drives in the library.

-l (--lun) is an option to specify LUN 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 1,800 seconds.

Create an iSCSI target

```
iscon createiscsiclienttarget -s <server-name> [-u <username> -p <password>]
-c <client-name> -I <ip-address> [-R <iscsi-target-name>] [-l <lun>] [-X <rpc-timeout>]

iscon createiscsiclienttarget --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--ip-address=<ip-address> --iscsi-target-name=<iscsi-target-name>
[--lun=<lun>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates an iSCSI target for the specified client.

-c (--client-name) is required to specify the client name. The client type must be iSCSI.

-I (--ip-address) is required to specify the IP address of the target.

-R (--iscsi-target-name) is an option to specify the target name. Valid characters are: a to z, 0 to 9, and .

-l (--lun) is an option to specify the starting LUN 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 1,800 seconds.

Delete an iSCSI target

```
iscon deleteiscsiclienttarget -s <server-name> [-u <username> -p <password>]
-c <client-name> -r <iscsi-target-id> [-X <rpc-timeout>]

iscon deleteiscsiclienttarget --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--iscsi-target-id=<iscsi-target-id> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command deletes the specified iSCSI target. All virtual devices must be unassigned from the target prior to running the command.

-c (--client-name) is required to specify the client name.

-r (--iscsi-target-id) is required to specify the target 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 1,800 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 1,800 seconds.

Delete virtual device

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

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

Description:

This command allows you to delete a virtual tape library, virtual tape drive, standalone virtual tape drive, or virtual tape.

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

A virtual device cannot be deleted if any of the following conditions apply:

- The specified virtual device is a virtual tape library or a virtual tape drive and there are clients currently connected to the library or drive.
- The specified virtual device is a virtual tape configured for replication, unless the -f (--force) option is used.
- The specified virtual device is the only existing virtual tape drive in the parent virtual tape library.

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

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

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

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

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

-d (--delete-virtual-tapes) is an option to delete all of the existing virtual tapes from a virtual tape library, a loaded virtual tape drive, or a standalone virtual tape drive selected for deletion. If not specified, the virtual tapes are moved to the vault, or, if a loaded virtual tape drive is selected, back to the library.

-f (--force) is an option to force the deletion of a virtual tape configured for replication. The corresponding virtual tape replica will not be deleted or promoted.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Shred virtual tape

```
iscon shredvirtualtape -s <server-name> [-u <username> -p <password>]
-B <barcode> | -v <vid> [-d] [-X <rpc-timeout>]

iscon shredvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--barcode=<barcode> | --vdevid=<vid> [--delete-virtual-tapes]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command deletes the data stored on the specified virtual tapes located in the vault. Either the barcode or the virtual tape ID can be used in order to identify the tapes. When barcode identification is used, the command will shred all of the virtual tapes that share the same barcode. The format for the identification arguments is a list of items separated by commas.

-B (--barcode) can be used to specify the virtual tapes by barcode.

-v (--vdevid) can be used to specify the virtual tapes by ID.

-d (--delete-virtual-tapes) is an option to delete the virtual tapes after the shredding operation is executed.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 1,800 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 1,800 seconds.

Create virtual tape library

```
iscon createvirtuallibrary -s <server-name> [-u <username> -p <password>]
-t <vlib-type> [-n <vlib-name>] -d <vdrive-type> [-r <vdrive-name-prefix>]
[-R <num-of-drives>] [-A <auto-archive-mode> [-Y <days>] [-J] | -N <auto-repl-mode>
-S <target-name> [-M <#[D|H|M]>] ] [-B <barcode-range>] [-T <num-of-slots>]
[-E <import-export-slots>] [-D -I <initial-size> -C <increment-size>]
[-m <max-capacity>] [-L <on|off>] [-f] [-k <key-name> -W <key-password>]
[-X <rpc-timeout>]

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

Description:

This command creates a virtual tape library.

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

-n (--vlib-name) is optional. A default name will be provided in the format of <vendorID>-<productID>-<vid> if it is not specified.

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

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

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

-A (--auto-archive-mode) is an option with one of the following values: *copy* or *move*.

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

-J (--auto-eject-to-ie) is an option to be specified with -A (--auto-archive-mode) to eject the tape to the import/export (IE) slot after the export job.

-N (--auto-replication) is an option with one of the following values: *replication* or *remotemove*.

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

-M (--delay-delete-time) is an option for *remotemove* mode to specify a time to wait before deletion. It can be specified in days(D), hours(H) or minutes(M). For example, 2D, 10H, 150M

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

Barcode is an alpha-numeric value with a length of 4 to 12. <barcodeB> and <barcodeE> have to be the same length.

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

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

The (--import-export-slots) cannot exceed the maximum number of IE slots supported by the specified library type. The default is to use the maximum number of slots supported by the specified library type.

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

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

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

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

-L (--auto-loader) is an option to set the auto-loader for those libraries that support the feature. The default value is *off*.

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

-k (--key-name) and -W (--key-password) are options for tape encryption support to be set in conjunction with Auto-Archive Mode. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 specific 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 1,800 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 1,800 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 preferred physical devices for creating 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 1,800 seconds.

Get virtual tape information

```
iscon getvirtualtapeinfo -s <server-name> [-u <username> -p <password>]
[-L <parent-library-id] [-B <barcode>] [-X <rpc-timeout>]

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

Description:

This command displays information about the specified virtual tapes, in CSV format. By default, the command reports all virtual tapes found in the COPAN 400 system that are located in virtual libraries.

-L (--tape-library-vid) is an option to choose a single virtual library to be queried and report on only those virtual tapes that are located in this library.

-B (--barcode) is an option to only display information about the virtual tape that is specified by this barcode. The tape must be in a virtual tape library.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Move virtual tape

```
iscon movevirtualtape -s <server-name> [-u <username> -p <password>]
-v <vdevid> | -B <barcode> [-i]
[-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> | --barcode=<barcode> [--include-filter]
[--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) or -B (--barcode) is required to identify the virtual tape to be moved to a different location.

-i (--include-filter) is an optional filter that can be used to uniquely identify a virtual tape when multiple tapes have the same barcode and -B (--barcode) is used. This option can be one of the following values:

- TapeName="*"
- Location=*
- ParentID=#

"Location" is the current location: the library ID if the tape is in a slot, the drive ID, or Vault. "ParentID" is the ID of the last library that hosted the tape and it is preserved when the tape is moved to the vault. If the tape cannot be uniquely identified, the command will fail.

-L (--tape-library-vid) is the virtual library to move to. It is not required if the virtual tape is moved within the same library.

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

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

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

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

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

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

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

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

- Standalone Tape Drive -> Vault

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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>] | [-h]
[-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>] | [--local]
[--tape-library-vid=<tape-library-vid> | --tape-drive-vid=<tape-drive-vid>]
[--vdevname=<vdevname>] [--force] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a copy of the specified virtual tape. The data is transferred through a replication job.

-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. If the replication is local, use the -h (--local) option.

-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.

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

-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 1,800 seconds.

Set virtual tape library duplication

```
iscon setvirtuallibrarytapeduplication -s <server-name> [-u <username> -p <password>]
-v <vdevid> -Z <on|off> -Q <num-of-copies> [-X <rpc-timeout>]

iscon setvirtuallibrarytapeduplication --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-duplication=<on|off> --num-of-copies=<num-of-copies>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command sets the Tape Duplication property for a virtual tape library.

-v (--vdevid) is required in order to identify the virtual library.

-Z (--tape-duplication) is required in order to enable or disable the Tape Duplication property: *on* (enable) or *off* (disable).

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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]
[--tape-duplication=<on|off> --num-of-copies=<num-of-copies>]
[--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 an 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.

-Z (--tape-duplication) is an option to set the Tape Duplication property with one of the following values: *on* (enable), *off* (disable), or *inherited*.

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

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 1,800 seconds.

Automated tape caching

Set tape caching

```
iscon settapecaching -s <server-name> [-u <username> -p <password>]
-L <library-vid> -t <tape-caching-enable> -m <delete-cache>
[-H <hours>] [-S <start-time>]
[-W <day-of-the-week>][-b <and-or>] [-d <# of hours>][-c][[-e][-f]]
[[-I | -M | -R <# of days> | -N] [-X <rpc-timeout>]

iscon settapecaching --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<library-vid> --tape-caching-enable=<tape-caching-enable>
[--reclamation-method=<delete-cache]
[--hourly <hours>] [--start-time=<start-time>] [--day-of-the-week=<day-of-the-week>]
[--trigger-combine=<and-or>] [--retention-hours=<# of hours>]
[--migration-threshold] [[--tape-ejected-to-slot] [--tape-full]]
[--immediately | --reclamation-threshold | --retention-days=<# of days> | --never]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command can be used in order to enable, disable, or change the Automated Tape Caching policy for a virtual tape library. The reclamation method used is "delete cache".

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

Set -t (--tape-caching-enable) to 1 for enable or 0 to disable. If the *disable* option is used, all other arguments will be ignored. The *enable* option must be used in order to set or change the tape caching policy.

-m (--reclamation-method) is an option to select the following reclamation method: delete-cache.

Time-based data migration triggers: Time Based

-H (--hourly) is an option to start migration every specified number of hours, up to 23. This option cannot be combined with any other migration trigger.

-S (--start-time) alone can be used to start daily migrations at the time specified. When combined with other data migration triggers, the *-S* option will delay the migration execution to the specified time.

-W (--day-of-the-week) is the default time based trigger that can be used to start weekly migrations on the specified day at 00:00(am): Sunday: 0, Monday: 1, ..., Saturday: 6. This option is ignored if Policy Based triggers are used.

Policy-based data migration triggers:

-b (--trigger-combine) tells how trigger policies are combined (specified by -d, -c, -e). 1 -- and; 0 -- or. The default value is 1 (and).

-d (--retention-hours) triggers the data migration after the data was retained on the disk for the specified number of hours, up to a year.

-c (--migration-threshold) triggers the data migration when the disk usage percentage is above the global disk space threshold.

-e (--tape-ejected-to-slot) triggers the data migration when unloading a virtual tape from a drive that had data written to it.

-f (--tape-full) applies to the --tape-ejected-to-slot trigger. The data is migrated only if the tape becomes full.

Reclamation triggers:

-I (--immediately) triggers the data reclamation immediately after the data migration completes.

-M (--reclamation-threshold) triggers the data reclamation when the disk usage percentage is above the global disk space threshold.

-R (--retention-days) triggers the data reclamation after the specified number of days, up to 2000.

-N (--never) means that virtual tapes will never be reclaimed.

The reclamation triggers are mutually exclusive.

The command always overwrites the current policy. Therefore, all of the desired properties must be provided each time the command is executed. The following properties are set by default if no triggers are provided:

- Migration trigger: daily at 00:00(am)
- Reclamation trigger: immediately

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Sync physical tapes

```
iscon syncphysicaltape -s <server-name> [-u <username> -p <password>]
-l <plib-vid> -b <physical-tape-barcode> -L <virtual-tape-library-id>
-t <virtual-tape-slot-no> [-M <sync-mode>] [-k <key-name> -W <key-password>]
[-I <ACSL list>] [-n <vdevname>] [-g <#(GB)>] [-X <rpc-timeout>]

iscon syncphysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-vid=<physical-tape-library-vid> --physical-tape-barcode=<physical-tape-barcode>
--tape-library-vid=<virtual-tape-library-id>
--virtual-tape-slot-no=<virtual-tape-slot-no> [--sync-mode=<sync-mode>]
[--key-name=<key-name> --key-password=<key-password>] [--scsiaddress=<ACSL list>]
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a synchronized virtual tape for each physical tape provided. The physical tapes must be from the specified physical tape library and the virtual tape will be created in the specified virtual tape library. The virtual tape library must have the tape caching feature enabled.

-l <--plib-vid> is the virtual ID of the physical tape library where the physical tapes are located.

-b (--physical-tape-barcode) is the barcode of the physical tape. If the barcode contains leading or trailing spaces, it must be enclosed in double quotes. For batch mode, the argument can be a list of barcodes separated by commas or a file name enclosed in "< >" (i.e., "<file>") containing a barcode on each line. Do not use quotes inside the file. The file must be located in the same folder as the command line utility or a full path is required. The virtual tape(s) will be created with the same barcode as the physical tape(s). The barcode(s) must not be in use by any other virtual tape in the system.-L <--tape-library-vid> is the ID of the virtual tape library where the virtual tapes will be created.

-t <--virtual-tape-slot-no> is an option to provide an empty destination slot for the virtual tape. Not for "-M cache" mode. For batch mode, virtual tapes will be created starting with the specified slot number.

[-M <--sync-mode>] is an option to select the synchronization mode from one of the following values (default is “cache"):

- cache (create cache)
- metadata (create cache and copy meta data)
- directlink (create direct link)

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be synchronized was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data.

The following three options can be selected for create cache mode only:

[-I <--scsiaddress>] is an option to specify preferred physical devices for creating the virtual device. It can be a list of ACSLs separated with commas. ACSL=#:#:#:# (adapter:channel:id:lun)

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

-g (--size-gb) is an option to specify the initial size, in GB, of the virtual tapes, if the capacity-on-demand property for the virtual tape library is enabled. The default is 1 GB.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Migrate virtual tapes

```
iscon migratevirtualtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-f] [-X <rpc-timeout>]

iscon migratevirtualtapes --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-vid-list=<tape-vid-list> [--tape-full] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command migrates the specified virtual tapes to the physical libraries they are synchronized with.

-T (--tape-vid-list) is a list of virtual tape ID(s) separated with commas.

-F (--tape-full) is an option to force full tape migration. By default, the migration operation is incremental.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Reclaim disk space

```
iscon reclaimtapes -s <server-name> [-u <username> -p <password>]
-T <tape-vid-list> [-X <rpc-timeout>]

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

Description:

This command reclaims the disk space occupied by the specified migrated virtual tapes.

-T (--tape-vid-list) is required to specify the ID of the virtual tapes to be reclaimed, separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Renew cache

```
iscon renewcache -s <server-name> [-u <username> -p <password>]
-v <vdevid> [-M <metadata>] [-k <key-name> -W <key-password>] [-I <ACSL>] [-n <vdevname>]
[-g <#(GB)>] [-X <rpc-timeout>]

iscon renewcache --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--import-mode=<metadata>]
[--key-name=<key-name> --key-password=<key-password>] [--scsiaddress=<ACSL>]
[--vdevname=<vdevname>] [--size-gb=<#(GB)>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command converts a virtual direct access tape into a virtual cache tape.

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

-M (--import-mode) is an option to specify that the header area should be copied from the physical tape to the new virtual tape cache. The value of this option must be: *metadata*.

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be renewed was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data.

The following properties of the virtual cache tape can be set if the "-M" option is not specified:

-I (--scsiaddress) is an option to specify preferred physical devices for creating the virtual device. It can be a list of ACSLs separated with commas or a file enclosed in <> containing an ACSL on each line.
ACSL=#:#:#:# (adapter:channel:id:lun)

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

-g (--size-gb) is an option to specify the size in GB. The size of the virtual tape will be the size configured in the properties of the virtual tape library or virtual tape drive if it is not specified. This option cannot be specified if the capacity-on-demand option is not enabled at library level.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Get tape caching info

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

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

Description:

This command reports a list of virtual tapes that are candidates for tape migration and summarizes the information about the space used by those tapes.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 1,800 seconds.

Get license keycode information

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

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

Description:

This command gets a list of licenses for the specified server.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Register a license keycode

```
iscon registerlicense -s <server-name> [-u <username> -p <password>] -k <license-keycode>
[-X <rpc-timeout>]

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

Description:

This command registers a specific license key code license.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 1,800 seconds.

Get COPAN 400 info

```
iscon getvtlinfo -s <server-name> [-u <username> -p <password>]
[-T <vtl-info_type> [-L <tape-library-vid>]] [-F <vtl-info-filter>] [-l [-A] [-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 [--long-physical-layout] [--output-delimiter=<output-delimiter>] ]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command lists all the virtual tape libraries, drives, and tapes on the specified server.

-T (--vtl-info-type) is the COPAN 400 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 detailed information.

-A (--long-physical-layout) is an option to display the physical layout associated with the device, if applicable. The argument is ignored if -l (--long-list) 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 1,800 seconds.

Get COPAN 400 server info

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

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

Description:

This command queries information about the specified server and returns server version, operating system version, kernel version, and installed patches.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Enable Hosted Backup

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

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

Description:

This command enables the Hosted Backup 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 1,800 seconds.

Disable Hosted Backup

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

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

Description:

This command disables the Hosted Backup 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 1,800 seconds.

Import/Export

Import tape

```
iscon importtape -s <server-name> [-u <username> -p <password>]
[-M <import-mode>] -v <plib-or-pdrive-vid> [-B <barcode> | -l <slot-no>]
-L <tape-library-vid> [-b <virtual-tape-barcode>] -t <virtual-tape-slot-no>
[-j <job-description>] [-k <key-name> -W <key-password>] [-X <rpc-timeout>]

iscon importtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--import-mode=<import-mode>] --plib-or-pdrive-vid=<plib-or-pdrive-vid>
[--barcode=<barcode> | --slot-no=<slot-no>] --tape-library-vid=<tape-library-vid>
--virtual-tape-slot-no=<virtual-tape-slot-no>
[--virtual-tape-barcode=<virtual-tape-barcode>] [--job-description=<job-description>]
[--key-name=<key-name> --key-password=<key-password>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command imports the data from a tape into the COPAN 400.

-M (--import-mode) is an option in one of the following values: *copy* (default) or *direct-access* or *recycle*.

-v (--pdrive-or-pdrive-vid) is required to specify the virtual device ID of the physical tape library or physical tape drive from which the physical tape is to be imported.

If the physical tape is from a physical tape library, either <barcode> or <slot-no> of the physical tape must be specified with -B (--barcode) or -l (--slot-no) to identify the physical tape. If the barcode contains leading or trailing spaces, it must be enclosed in double quotes. Physical tape information is not required if the physical tape is imported from a standalone physical tape drive.

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

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

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

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

-k (--key-name) and -W (--key-password) are options for tape encryption support. If the tape to be imported was encrypted through the system, you need to specify the key name and the key password of the encryption key to decrypt the data.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Export virtual tape

```
iscon exportvirtualtape -s <server-name> [-u <username> -p <password>]
-v <vdevid> -L <tape-library-vid> -b | -B <barcode> | -l <slot-no>
[-M <export-mode> [-Y <days>] ] [-j <job-description>] [-f] [-J]
[-k <key-name> -W <key-password>] [-Z <on> -Q <num-of-copies>] [-X <rpc-timeout>]

iscon exportvirtualtape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--vdevid=<vdevid> --tape-library-vid=<tape-library-vid>
--same-barcode | --barcode=<barcode> | --slot-no=<slot-no>
[--export-mode=<export-mode> [--delay-delete-days=<days>]]
[--job-description=<job-description>] [--force] [--auto-eject-to-ie]
[--key-name=<key-name> --key-password=<key-password>]
[--tape-duplication=<on> --num-of-copies=<num-of-copies>] [--rpc-timeout=<rpc-timeout>]
```

Description:

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

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

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

You must include one of the following arguments to select the physical tape:

- -b (--same-barcode) lets you select a physical tape with the same barcode of the virtual tape if a physical tape with the same barcode exists.
- -B (--barcode) lets you specify the barcode of an available physical tape in the physical tape library. If the barcode contains leading or trailing spaces, it must be enclosed in double quotes.
- -l (--slot-no) lets you specify the slot number of an available physical tape in the physical tape library.

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

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

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

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

-J (--auto-eject-to-ie) is an option to eject the tape to the IE slot after the export job.

-k (--key-name) and -W (--key-password) are options for tape encryption support. Specify the key name and key password of the encryption key if you wish to encrypt the data when exporting the virtual tape to the physical tape.

-Z (--tape-duplication) is an option to enable Tape Duplication for this export job: *on* (enable); Default is *off* (disabled).

-Q (--num-of-copies) is an option to specify the number of copies to be made using the same barcode if the tape duplication option is enabled. The maximum value is 5. The default value is 1.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Get import/export job status

```
iscon getimportexportjobstatus -s <server-name> [-u <username> -p <password>]
[-j <job-id-list>] [-T <job-type> -S <job_status> -D <date-range|date> -l]
[-X <rpc-timeout>]

iscon getimportexportjobstatus --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--job-id-list=<job-id-list>] | [--job-type=<job_type> --job_status=<job_status>]
--date-range=<date-range|date> --longlist] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command displays the status of the import/export jobs present in the queue. If no filters are specified, the command displays all the jobs that are in the queue.

-j <--job-id-list> is an optional list of job IDs separated with commas. The command displays the status of specified jobs only. All other filters are ignored.

-T <--job-type> is an optional job type based filter. The command displays those jobs matching the provided type. The accepted job type values are: IMPORT, EXPORT, or OTHER (such as scan).

-S <--job_status> is an optional job status based filter. The command displays those jobs matching the provided status. The accepted job status values are: FAILED, HOLD, READY, or OTHER (such as waiting for tape/drive or cancelled).

-D (--date-range) is an option to specify the date range for the report (future dates are ignored): YYYYMMDD-YYYYMMDD or YYYYMMDD.

-l (--longlist) is an option to display detailed information.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Resume import/export jobs

```
iscon resumeimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon resumeimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command resumes the specified import/export jobs. The jobs must be in the budget queue in a suspended state.

-j <--job-id-list> is a list of job IDs separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Restart import/export jobs

```
iscon restartimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon restartimportexportjobs --server-name=<server-name>
```

```
[--server-username=<username> --server-password=<password>]
--job-id-list=<job-id-list> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command restarts the specified import/export jobs. The jobs must be in the budget queue and they must have either been cancelled or failed.

.-j <--job-id-list> is a list of job IDs separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Delete import/export jobs

```
iscon deleteimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon deleteimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command deletes the specified import/export jobs. The jobs must be in the budget queue.

-j <--job-id-list> is a list of job IDs separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Suspend import/export jobs

```
iscon suspendimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon suspendimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command suspends the specified import/export jobs. The jobs must be in the budget queue and must be idle.

-j <--job-id-list> is a list of job IDs separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Cancel import/export jobs

```
iscon cancelimportexportjobs -s <server-name> [-u <username> -p <password>]
-j <job-id-list> [-X <rpc-timeout>]

iscon cancelimportexportjobs --server-name=<server-name>
[--server-username=<username> --server-password=<password>] --job-id-list=<job-id-list>
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command cancels the specified import/export jobs. The jobs must be in the budget queue and must be running.

-j <--job-id-list> is a list of job IDs separated with commas.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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>]
[-L <#:#:#:#>] [-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>] [--preferred-lun=#:#:#:#]
[--vdevname=<replica-name>] [--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 an option to specify the target server name where the tape replica will be created and replicated to. If the replication is local, use -H (--local) option.

-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 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.*

-L (--preferred-lun) is an option to specify preferred physical devices for creating the virtual device. The format for this option is: #:#:#:# (adapter:channel:id:lun)

-n (--vdevname) is an option to specify the replica tape name.The maximum length of the device name is 64. Leading and trailing spaces will be removed. Enclose the name in double quotes to ensure proper parsing. The following characters are invalid for the 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 1,800 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 1,800 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 1,800 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 1,800 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 1,800 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 1,800 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 lists the replication configuration for the specified virtual tape.

-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 1,800 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 1,800 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 1,800 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 1,800 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 1,800 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 1,800 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 an 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 1,800 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 1,800 seconds.

Rename physical device

```
iscon renamephysicaldevice -s <server-name> [-u <username> -p <password>]
-i <guid> | -I <ACSL> -n <new-name> [-X <rpc-timeout>]

iscon renamephysicaldevice --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--scsiaddress=<ACSL> | --guid=<guid> --name=<new-name> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command renames a physical device.

<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 <guid> or <ACSL> can be specified for the physical device.

<new-name> is required for the new physical device name. The maximum length for the name is 64. The following characters are invalid for the 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 1,800 seconds.

Mark physical library or drive enabled/disabled

```
iscon markphysicallibdrvstate -s <server-name> [-u <username> -p <password>]
-v <plib-or-pdrive-vid> [-E <on | off>] [-X <rpc-timeout>]

iscon markphysicallibdrvstate --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-or-pdrive-vid=<plib-or-pdrive-vid> [--state=<on | off>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command marks a physical tape library or drive as enabled or disabled.

-v (--plib-or-pdrive-vid) is required to specify the ID of the device.

-E (--state) is required to specify the new state for the device. If the argument is not specified, the command retrieves the current state for the device.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 1,800 seconds.

Inventory physical tape library

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

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

Description:

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

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

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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Get physical tape list

```
iscon getphysicaltapelist -s <server-name> [-u <username> -p <password>]
-l <physical-tape-library-vid> [-F <filter>] [-X <rpc-timeout>]

iscon getphysicaltapelist --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--plib-vid=<physical-tape-library-vid> [--ptape-filter=<filter>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command displays a list of physical tapes located in the specified physical tape library.

-l (--plib-vid) is the ID of the physical tape library.

-F (--ptape-filter) is an option to show only the physical tapes having the specified property: SYNC (eligible for sync operation) .

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Move physical tape

```
iscon movephysicaltape -s <server-name> [-u <username> -p <password>]
-m <move-operation> -L <physical-tape-library-vid>
-B <physical-tape-barcode> | -l <from-location-id> -t <to-location-id>
[-X <rpc-timeout>]

iscon movephysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--move-operation=<move-operation> --tape-library-vid=<physical-tape-library-vid>
--physical-tape-barcode=<barcode> | --from-location-id=<from-location-id>
--to-location-id=<to-location-id> [--rpc-timeout=<rpc-timeout>]
```

Description:

This command moves a physical tape to a new location.

-l (--plib-vid) is the ID of the physical tape library.

-m(--move-operation) is one of the following operations:

- DriveToSlot
- SlotToSlot
- SlotToDrive
- IESlotToSlot
- SlotToIESlot

-L(--tape-library-vid) is the physical library virtual ID where the tape is located.

-B(--physical-tape-barcode) identifies the physical tape to be moved. If barcode is not provided, the current tape location must be provided accordingly to the requested operation.

-l(--from-location-d) is the current slot or import/export (IE) slot number, or the physical drive virtual ID.

-t(--to-location-id) is the destination slot or IE slot number or the physical drive virtual ID.

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

Eject physical tape

```
iscon ejectphysicaltape -s <server-name> [-u <username> -p <password>]
-L <physical-tape-library-vid> -B <physical-tape-barcode-list>
[-A <acs-lsm-cap>] [-X <rpc-timeout>]

iscon ejectphysicaltape --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
--tape-library-vid=<physical-tape-library-vid>
--tape-barcode-list=<physical-tape-barcode-list> | [--acs-lsm-cap=<acs-lsm-cap>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command ejects physical tapes from the specified library.

-L(--tape-library-vid) is the physical library virtual ID where the tapes are located.

-B(--tape-barcode-list) identifies the physical tapes to be ejected. This argument can be a list of barcodes separated with commas. The list should be enclosed in quotes.

-A <--acs-lsm-cap> is an optional argument representing the Cartridge Access Port for the Automated Cartridge System Library Software libraries. The format of the argument is acs:lsm:cap

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 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 an 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 1,800 seconds.

Reports

Disk space allocation for virtual tapes in libraries report

```
iscon creatediskspaceallocreport -s <server-name> [-u <username> -p <password>]
[-h [-R <resource-list> -z <report period> | -D <date-range> -d <interval>]]
[-o <filename>] [-X <rpc-timeout>]

iscon creatediskspaceallocreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--historical [--resource-list->resource-list>
--report-period=<report-period> | --date-range=<date-range> --data-points=<interval>]]
[--output-file=<filename>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that summarizes the disk space used by the allocated tapes on a specific server.

-h (--historical) is an option to create a historical report. By default, the report presents the current disk allocation.

The following four options can be used when the historical report option is selected. Otherwise they are ignored:

-R <--resource-list> in an option to report the status of the specified libraries only. The argument can be a list of virtual identifiers separated with commas, or the file name, enclosed in "< >", of a text file containing the list in the first line. The file must be located in the same folder as the command line utility or the full path is required. For example: -R 10,17 or -R "<lib_id_file.txt>"

-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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 days): YYYYMMDD-YYYYMMDD or YYYYMMDD

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The default value is: "-z t" (today).

-d (--data-points) is an option to specify the time interval between the data points: "daily", "weekly", "monthly", "quarterly". The default values for the data points interval are:

- hourly - when reporting up to 3 days of data
- daily - when reporting between 4 and 60 days of data
- weekly - when reporting more than 60 days of data

-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: DiskSpaceAllocationVirtualTapes-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 1,800 seconds.

Disk space usage history report

```
iscon createdisk spaceusagehistoryreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-o <filename>] [-X <rpc-timeout>]

iscon createdisk spaceusagehistoryreport --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 time that the report should cover. The accepted values are:

- t - today
- y - yesterday
- 7 - last seven days
- 30 - last thirty days
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 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 local server 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 1,800 seconds.

Fibre Channel adapters 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 World Wide Port Name (WWPN) and port information for all Fibre Channel adapters.

-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 1,800 seconds.

Import export job report

```
iscon createimportexportjobreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-i <filter>] [-o <filename>] [-X <rpc-timeout>]

iscon createimportexportjobreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--include-filter=<filter>] [--output-file=<filename>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays all of the import/export 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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 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 local server time. The default value is: "-z t" (today).

-i (--include-filter) is an optional filter to include only the specified jobs. The following values are accepted. Multiple values must be separated with commas.

Job Type:

- ESD[C | M] - Export to standalone drive, Copy or Move
- EPL[C | M] - Export to physical library, Copy or Move
- ISD[C | R] - Import from standalone drive, Copy or Recycle
- IPL[C | R] - Import from physical library, Copy or Recycle
- CC - Create cache with copy meta data

The default is to include tapes that were exported with either Copy or Move or were imported with either Copy or Recycle.

Job Status:

- WTD - Waiting for tape/drive
- FAIL - Failed
- COMP - Completed
- CANC - Cancelled
- HOLD - On hold
- WIE - Waiting for IE slot
- RUN - Running

For example: -i EPL,COMP,CANC
This command will include only jobs with export to physical library, *copy* and *move*, *completed* and *cancelled*.

By default all jobs are included.

-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 1,800 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 virtual tapes 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 1,800 seconds.

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 all virtual devices that have been allocated from all or selected virtualized LUNs.

-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 1,800 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 lists all physical adapters for a specific server. For each adapter, the report shows all information about each physical device that has been configured to the adapter.

-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 1,800 seconds.

Physical tape usage report

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

iscon createphytapeusagereport --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 information about how each physical tape in the physical tape database is mapped to a virtual tape.

-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: PhysicalTapeUsage-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 1,800 seconds.

Replication status report

```
iscon createreplicationstatusreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-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>]
[--report-period=<report-period>] | [--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 information about virtual tapes enabled for replication and for virtual tape replicas.

-z (--report-period) is an option to specify 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
- 365 - last 365 days

-D (--date-range) is an option to specify a maximum 365 days interval. The date format is YYYYMMDD or YYYYMMDD-YYYYMMDD.

Either -z (--report-period) or -D (--date-range) can be specified, but not both. The default value is: "-z t" (today).

-r (--repl-resource-type) is an option to specify a generic resource type to be queried. It can be one of the following: TAPE or 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 1,800 seconds.

SCSI device throughput report

```
iscon createscsidevicethroughputreport -s <server-name> [-u <username> -p <password>]
-I <ACSL> [-z <report period>] | [-D <date-range>] [-o <filename>]
[-X <rpc-timeout>]

iscon createscsidevicethroughputreport --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 information for the selected physical SCSI storage 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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 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 local server 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 1,800 seconds.

SCSI/Fibre 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 information about data going through the selected SCSI or Fibre Channel adapter.

-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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 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 local server 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 1,800 seconds.

Virtual library and drive assignment report

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

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

Description:

This command creates a report that lists all of the virtual tape libraries and drive assignments for all clients.

-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: LibraryDriveAssignment-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 1,800 seconds.

Virtual library information report

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

iscon createvirtuallibinforeport --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 information about each virtual tape library, including the physical library it emulates, the amount of storage it occupies, and information about its drives, tapes, and slots.

-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 1,800 seconds.

Virtual tape activity report

```
iscon createvirtualtapeactivityreport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-i <filter>] [-o <filename>] [-X <rpc-timeout>]

iscon createvirtualtapeactivityreport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--include-filter=<filter>] [--output-file=<filename>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays all virtual tape activity for all virtual tapes for three types of operations: Backup, Tape Import (*write* operations), and Tape Export (*read* operations).

-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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 days): YYYYMMDDhhmmss-YYYYMMDDhhmmss, 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).

-i (--include-filter) is an optional filter to include only the virtual tapes that match the barcode filter. This option can be one of the following values:

- BARCODEPREFIX=barcodePrefix,
- BARCODECONTAINS=pattern,
- BARCODERANGE=barcodeStart-barcodeEnd,

-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: VirtualTapeActivity-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 1,800 seconds.

Virtual tape information report

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

iscon createvirtualtapeinforeport --server-name=<server-name>
[--server-username=<username> --server-password=<password>] [--output-file=<filename>]
[--include-filter=<filter>] [--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that displays the current status of all virtual tapes.

-i (--include-filter) is an optional filter to include only the specified virtual tapes. This option can be any combination of the following values, separated by commas. Multiple IDs of the same type must be separated by semicolons. The barcode filters are mutually exclusive.

- BARCODEPREFIX=barcodePrefix
- BARCODECONTAINS=pattern
- BARCODERANGE=barcodeStart-barcodeEnd
- LIBRARY=ID1;ID2 (virtual library ID list)

Additionally, the following values can be used to select from different output templates. Multiple views must be separated with semicolons. The default view is overall summary.

- VIEW=OS (overall summary)
- TC (tape caching view)
- RR (replica resources view, includes all replica tapes)
- VV (vault view, includes all tapes from the vault)
- DT (detailed tape view)

The argument must be enclosed in double quotes. For example:
-i "LIBRARY=10;11,BARCODEPREFIX==00,VIEW=OS;DE;TC"

-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

-X (--rpc-timeout) is an option to specify a number between 1 and 30000 seconds for the RPC timeout. The default RPC timeout is 1,800 seconds.

COPAN 400 performance report

```
iscon createvtlperformancereport -s <server-name> [-u <username> -p <password>]
[-z <report period>] | [-D <date-range>] [-d <interval>] [-i] [-o <filename>]
[-X <rpc-timeout>]

iscon createvtlperformancereport --server-name=<server-name>
[--server-username=<username> --server-password=<password>]
[--report-period=<report-period>] | [--date-range=<date-range>]
[--data-points=<interval>] [--include-filter=<filter>] [--output-file=<filename>]
[--rpc-timeout=<rpc-timeout>]
```

Description:

This command creates a report that lists CPU/memory usage and total throughput performance.

-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
- 365 - last 365 days

-D (--date-range) is the starting date and ending date in the following format (maximum 365 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).

-d (--data-points) is an option to choose the time interval between data points when either the report period or date range argument is used. In order to limit the number of data points and prevent reports with a single data point, the accepted values are:

- "hourly" when the report period is less than 4 days
- "daily" when the report period is between 2 and 59 days
- "weekly" when the report period is more than 13 days
- "monthly" when the report period is more than 59 days
- "quarterly" when the report period is more than 121 days

The default values for the data points are:

- "hourly" when the report includes up to 3 days of data
- "daily" when the report includes between 4 and 60 days of data
- "weekly" when the report includes more than 60 days of data

If a report period is not specified, there is no need to use -d (--data-points).

-i (--include-filter) is an optional filter to include only the specified devices. This option can be any combination of the following values, separated by commas. Multiple IDs of the same type must be separated by semicolons. The argument must be enclosed in quotes.

- Storage HBAs - ADAPTER=all or ADAPTER_NO_1;ADAPTER_NO_2
- Storage devices - LUN=all or A:C:S:L(1);A:C:S:L(2)
- Clients - CLIENT=all or CLIENT_ID_1;CLIENT_ID_2
- Virtual libraries - LIBRARY=all or ID_1;ID_2

By default, the report lists the performance for the whole COPAN 400 server and for all devices mentioned above. Use "none" in order to filter out individual devices. For example:

- -i "ADAPTER=all,LUN=100:0:0:1;100:0:0:5,LIBRARY=100"
- -i "none"

-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: VTLPerformance-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 1,800 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 COPAN 400 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 1,800 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 1,800 seconds.

SNMP Integration

COPAN 400 provides Simple Network Management Protocol (SNMP) support to integrate COPAN 400 management into an existing enterprise management solution, such as HP OpenView, CA Unicenter, IBM Tivoli NetView, or BMC Patrol.

COPAN 400 can send different types of information to your SNMP manager:

- **COPAN 400 Event Log messages** - By default, Event Log messages (informational, warnings, errors, and critical errors) are not sent, but you may want to configure COPAN 400 to send certain types of messages. Refer to 'Server properties' for more information.
- **MIBs** - Each MIB (Management Information Base) monitors information and processes in COPAN 400. You will need to compile the COPAN 400 MIBs into your SNMP manager. The procedure to do this will vary by SNMP manager. You will need to compile the following COPAN 400 MIB files which can be found in $ISHOME/etc/snmp/mibs:
  - falc-common.mib
  - falconstor.mib
  - falc-vtl.mib
  - falc-vtl-history.mib
  - falc-vtl-monitor.mib

VTL MIBs

falcVtlMonitorMIB

The falcVtlMonitor MIB has multiple tables that display different capacity, usage, and performance statistics.

falcVTLMonCapacity

Displays COPAN 400 capacity and usage statistics. Includes the following tables:

Table	Description
falcVtlCapCacheGeneralInfo	COPAN 400 capacity statistics, including: • *BackupCacheCapacityAvailable* - Available cache capacity, in GBs • *BackupCacheCapacityTotal* - Total cache capacity, in GBs • *CacheCapacityUsed* - Cache used space, in GBs • *UnassignedVTLCacheCapacity* - Unassigned cache space, in GBs • *CacheCapacityPercentFree* - Free cache space percentage • *CacheCapacityPercentUsed* - Used cache space percentage • *CacheCapacityPercentUnassigned* - Unassigned cache space percentage
LibCacheUsage	Cache usage by all tapes in each individual library, including: • *falcVtlLibID* - Virtual tape library ID assigned by the COPAN 400 server • *falcVtlLibUsedByAllVtapes* - Space used by virtual tapes, in MB
PolicyCacheUsage	Cache usage by all tapes in each policy, including: • *Name* - Policy name • *UsedByAllVtapes* - Space used by virtual tapes, in MB

falcVTLMonPerformance

Displays COPAN 400 performance and statistics. Includes the following tables:

Table	Description
falcVtlPerfOneDayIntervalDataInfo	Note that no data will be available for a failover server that has been taken over. COPAN 400 performance for the past 24 hours, including: • *DataWritten* - Amount of data written, in MB, for all job types (backup, import) • *CacheSpaceUsed* - Amount of space used after compression, in MB • *DataRead* - Amount of total uncompressed data read, in MB • *DataCompressedRead* - Amount of compressed data read, in MB • *ReplRawDataTx* - Raw replication data transferred, in MB • *ReplActualDataTx* - Actual amount of replication data transferred, in MB • *ReplTotalTapesTx* - Number of tapes replicated
falcVtlMonPerformanceInfo	COPAN 400 performance, including: • *CompressRatio* - Average tape compression ratio

falcVtlHistoryMIB

The falcVtlHistoryMIB has multiple tables that display historical information about activity on the server, dashboard, and tape history.

falcVtlActivityTable

Displays tape activity history including operations related to client backup and restore, import, and export:

Table	Description
Activity	• *StartTime* - Start time for the tape operation • *EndTime* - End time for the tape operation • *VlibraryID* - Virtual library in which the tape was present when the operation took place • *VDriveID* - Virtual drive used by the operation • *VTapeID* - Virtual tape used for the operation • *Operation* - Operation performed • *WriteDataMB* - Uncompressed data written, in MB • *WriteCompressDataMB* - Compressed data written, in MB • *ReadDataMB* - Uncompressed data read, in MB • *ReadCompressDataMB* - Compressed data read, in MB • *StartEODMB* - Location on the tape that marks the end of data at the start of the operation (in MB to denote the location as offset from the beginning of the tape) • *EndEODMB* - Location on the tape that marks the end of data at the end of the operation (in MB to denote the location as offset from the beginning of the tape) • *Barcode* - Tape barcode

falcVtlDashStatisticsTable

Displays the following dashboard activity history:

Table	Description
DashStatistics	• *TimeStamp* - Date and time the data was collected • *DiskSpaceTotal* - Total disk space used, in GB • *DiskSpaceAvailable* - Available disk space, in GB • *PerformanceRead* - Read performance, in MB/sec (calculated at the HBA level) • *PerformanceWrite* - Write performance, in MB/sec (calculated at the HBA level)

falcVtlServer

Displays information about the COPAN 400 server and the options configured.

Table	Description
Processor	Displays information about all of the processors in the COPAN 400 server.
NetInterface	Displays information about all of the network interfaces in the COPAN 400 server.
FailoverInfo	Displays failover information for the configured failover mode, including: • Type of failover (active-passive or mutual) • Failover partner • COPAN 400 servers in failover group • Self check interval • Heartbeat interval • Recovery setting • Current failover state
FCInfo	Displays information about all of the Fibre Channel HBAs in the COPAN 400 server. It displays the WWPN (World Wide Port Name) for each HBA and the mode (target or initiator).
falcVTLServerOptionsInfo	Displays which COPAN 400 server options (Fibre Channel, iSCSI, COPAN 400 database, Email Alerts, Hosted Backup, NDMP) are enabled.
falcVTLServerInfo	Displays COPAN 400 server information, including: • Hostname • IP address • COPAN 400 server version • Operating system version • Kernel version • Amount of memory • Amount of swap space

falcVtlLibrarySystem

Displays information about virtual and physical libraries, SAN clients, and physical resources.

falcVtlVirtualLibs

Displays information about the configuration and properties of each virtual tape library.

Table	Description
VirtualLibrary	• *falcVtlVirtLibID* - Virtual tape library ID • *falcVtlVirtLibName* - Virtual tape library name • *falcVtlVirtLibVendorID* - Vendor ID • *falcVtlVirtLibProductID* - Product ID • *falcVtlVirtLibRev* - Firmware version • *falcVtlVirtLibNumSlots* - Number of slots • *falcVtlVirtLibNumDrives* - Number of drives • *falcVtlVirtLibBarcodeBegin* - First barcode in range for library • *falcVtlVirtLibBarcodeEnd* - Last barcode in range for library • *falcVtlVirtLibTapeCapacityOnDemand* - Indicates if tape capacity on demand (COD) is enabled • *falcVtlVirtLibInitAllocSize* - Initial tape size, in MB (if tape COD is enabled) • *falcVtlVirtLibIncrementSize* - Incremental amount, in MB (if tape COD is enabled) • *falcVtlVirtLibMaxCapacity* - Maximum tape capacity, in MB (if tape COD is enabled) • *falcVtlVirtLibAutoArchive* - Indicates if auto archive is enabled • *falcVtlVirtLibMediaType* - Media type • *falcVtlVirtLibNumTapes* - Number of tapes in library • *falcVtlVirtLibSerialNum* - Serial number of library • *falcVtlVirtLibAutoReplication* - Indicates if auto replication is enabled • *falcVtlVirtLibAutoTapeCaching* - Indicates if tape caching is enabled • *falcVtlVirtLibTapeDuplication* - Indicates if tape duplication is enabled
falcVtlVirtualLibsInfo	Total number of virtual tape libraries

falcVtlVirtualDrives

Displays information about the configuration and properties of each virtual tape drive.

Table	Description
VirtualDrive	• *falcVtlVirtDriveID* - Virtual tape drive ID • *falcVtlVirtDriveName* - Virtual tape drive name • *falcVtlVirtDriveVendorID* - Vendor ID • *falcVtlVirtDriveProductID* - Product ID • *falcVtlVirtDriveRevision* - Firmware version • *falcVtlVirtDriveMediaType* - Media type • *falcVtlVirtDriveLocationType* - Virtual tape drive location • *falcVtlVirtDriveLocationID* - ID of the virtual tape library where the virtual tape drive resides • *falcVtlVirtDriveGBRead* - GB read from this virtual drive • *falcVtlVirtDriveGBWritten* - GB written to this virtual drive • *falcVtlVirtDriveCompression* - Indicates if compression is enabled • *falcVtlVirtDriveStatus* - Operational status: unknown, empty, loaded, ejected (but not removed), offline, passthrough (all commands will be sent), becoming ready, unloading, online
falcVtlVirtualDrivesInfo	Total number of virtual tape drives

falcVtlVirtualTapes

Displays information about the configuration and properties of each virtual tape.

Table	Description
VirtualTape	• *falcVtlVirtTapeID* - Virtual tape ID • *falcVtlVirtTapeName* - Virtual tape name • *falcVtlVirtTapeTotalSize* - Size, in MB • *falcVtlVirtTapeStatus* - Status (online, offline) • *falcVtlVirtTapeGUID* - Globally Unique Identifier (GUID) • *falcVtlVirtTapeUsedSize* - Used size, in MB • *falcVtlVirtTapeBarcode* - Barcode • *falcVtlVirtTapeMediaType* - Media type • *falcVtlVirtTapeCapacityOnDemand* - Indicates if tape capacity on demand is enabled • *falcVtlVirtTapeAutoArchive* - Indicates if auto archive is enabled or disabled • *falcVtlVirtTapeWriteProtection* - Indicates if the tape is write protected • *falcVtlVirtTapeLocationType* - Tape location (library slot, drive, or vault) • *falcVtlVirtTapeLocationID* - ID of the virtual device where the tape resides (-1, not applicable, for vault) • *falcVtlVirtTapeLocationSlot* - Slot number of virtual tape library that tape resides in (-1, not applicable, for vault and drive) • *falcVtlVirtTapeInitAllocSize* - Initial tape size, in MB (if tape COD is enabled) • *falcVtlVirtTapeIncrementSize* - Incremental amount, in MB (if tape COD is enabled) • *falcVtlVirtTapeMaxCapacity* - Maximum tape capacity, in MB (if tape COD is enabled) • *falcVtlVirtTapeRdeTapeType* - Type of tape
falcVtlVirtualTapesInfo	Total number of virtual tapes

falcVtlPhysicalLibs

Displays information about the configuration and properties of each physical tape library.

Table	Description
PhysicalLibrary	• *falcVtlPhyLibID* - Physical tape library ID • *falcVtlPhyLibName* - Physical tape library name • *falcVtlPhyLibAllocationType* - Same as *falcVtlPhyLibName* • *falcVtlPhyLibVendorID* - Vendor ID • *falcVtlPhyLibProductID* - Product ID • *falcVtlPhyLibStatus* - Status (online, offline) • *falcVtlPhyLibGUID* - Globally Unique Identifier • *falcVtlPhyLibSerialNumber* - Serial number • *falcVtlPhyLibNumSlots* - Number of slots
falcVtlPhysicalLibsInfo	Total number of physical tape libraries

falcVtlPhysicalDrives

Displays information about the configuration and properties of each physical tape drive.

Table	Description
PhysicalDrive	• *falcVtlPhyDriveID* - Physical tape ID • *falcVtlPhyDriveName* - Physical tape drive name • *falcVtlPhyDriveVendorID* - Vendor ID • *falcVtlPhyDriveProductID* - Product ID • *falcVtlPhyDriveStatus* - Status (online, offline) • *falcVtlPhyDriveGUID* - Globally Unique Identifier • *falcVtlPhyDriveSerialNumber* - Serial number • *falcVtlPhyDriveState* - Operational status: empty, loaded, ejected (but not removed from drive), offline, passthrough (all commands will be sent)
falcVtlPhysicalDrivesInfo	Total number of physical tape drives

falcVtlPhysicalTapes

Displays information about the configuration and properties of each physical tape.

Table	Description
PhysicalTape	• *TapeSlot* - Physical slot the tape is in • *TapeBarcode* - Barcode
falcVtlPhysicalTapesInfo	Total number of physical tapes

falcVtlJobQueue

Displays information about the import/export job queue.

Table	Description

VTLJob	• *falcVTLJobID* - Job ID
	• *falcVTLJobType* - Job type:
	  • exportToSADriveAndCopy - Export with copy on a standalone physical tape drive
	  • exportToSADriveAndMove - Export with move on a standalone physical tape drive
	  • exportToPhyLibAndCopy - Export with copy to a physical tape library
	  • exportToPhyLibAndMove - Export with move to a physical tape library
	  • importFromSADriveAndCopy - Import in copy mode from a standalone physical tape drive
	  • importFromSADriveAndRecycle - Import in recycle mode from a standalone physical tape drive
	  • importFromPhyLibAndCopy - Import in copy mode from a physical library
	  • importFromPhyLibAndRecycle - Import in recycle mode from a physical library
	  • createFromCacheMetaDataModeAndCopy - Create cache in copy meta data mode
	  • moveTapeIESlot - Moving tape to an IE slot
	• *falcVTLJobPhysicalLibName* - Physical library used for import/export
	• *falcVTLJobPhysicalTapeBarcode* - Physical tape barcode used for import/export
	• *falcVTLJobPhysicalSlot* - Physical slot number used for import/export
	• *falcVTLJobVirtualLibName* - Virtual library used for import/export
	• *falcVTLJobTapeName* - Virtual tape used for import/export
	• *falcVTLJobTapeBarcode* - Virtual tape barcode used for import/export
	• *falcVTLJobVirtualSlot* - Library virtual slot number used for import/export
	• *falcVTLJobStatus* - Job status: ready, running, completed, cancelled, or failed
	• *falcVTLJobDescription* - Job description

falcVtlJobQueueInfo	• Total number of import/export drives

falcVtlReplicaResources

Displays information about replica resources.

Table	Description
ReplicaResource	• *VirtualID* - Replica resource ID • *VirtualName* - Resource name • *AllocationType* - Resource type (virtual device) • *TotalSize* - Size, in MB • *ConfigurationStatus* - Status - (online or offline) • *GUID* - Globally Unique Identifier • *PrimaryVirtualID* - Source replication server and device in the format <hostname of source>:<virtual device ID>. • *ReplicationStatus* - Current status of the replication schedule - Replication failed, new, idle, merging, unknown (stopped) • *LastStartTime* - Last replication start time
ReplicaPhyAllocationLayout	Displays information about the physical devices which were used to create active replica resources, including: • *VirtualID* - Replica resource ID • *VirtualName* - Resource name • *Name* - Physical device name • *Type* - Type (primary or mirror) of the physical layout • *SCSIAddress* - SCSI address of the replica resource in the format <Adapter:Channel:SCSI:LUN> • *FirstSector* - First sector of the physical device used for this resource • *LastSector* - Last sector of the physical device used for this resource • *Size* - Size allocated for the replica resource, in MB
ReplicationPolicy	Displays information about tapes with replication policies, including: • *ResourceID* - Virtual tape ID • *ResourceName* - Virtual tape name • *Option* - Replication status (enabled or disabled) • *ReplicaServer* - Target replica server name • *ReplicaDeviceID* - Target replica device ID • *Schedule* - Current status of the schedule: On Schedule, Suspended, or N/A • *Watermark* - Watermark set to trigger replication • *WatermarkRetry* - Retry interval if replication fails • *Time* - Time when replication is scheduled to occur • *Interval* - Time interval between replication jobs
falcVtlReplicaResourcesInfo	Total number of replica resources

falcVtlPhysicalResources

Displays information about physical resources.

Table	Description
falcVtlScsiAdapterTable/ StorageHBAs	Information about each storage HBA, including: • *Number* - SCSI Adapter number • *Info* - Model/type • *WWPN* - World wide port name • *Mode* - Mode: Target or initiator • *AliasWWPN* - Alias WWPN, if dual mode • *AliasMode* - Mode of alias: Target or initiator • *GBRead* - Amount of data read, in GB, for target ports • *GBWrite* - Amount of data written, in GB, for target ports
falcVtlScsiDeviceTable/ StorageDevices	Information about the hardware specifications and characteristics of each SCSI device (physical tape library, physical tape drive, and storage device), including: • *DeviceType* - Access type for the attached device (Direct-Access, Sequential-Access, Medium Changer) • *VendorID* - Product vendor • *ProductID* - Product model • *FirmwareRev* - Firmware version • *AdapterNo* - SCSI adapter number • *ChannelNo* - SCSI channel • *ScsiID* - SCSI ID • *LUN* - SCSI LUN • *TotalSectors* - Number of sectors or blocks • *SectorSize* - Number of bytes in each sector or block • *TotalSize* - Total size of the device, in MB • *ConfigStatus* - Status (online or offline) • *UsedSize* - Space used, in MB • *FreeSize* - Free space, in MB • *StorageOwner* - Owner of the device. Storage devices will show the server name. Media changers and drives will be displayed as local owner.
falcVtlPhysicalResourcesInfo	Total number of adapters and devices.

falcVtlLogicalResources

These MIBs are obsolete and are no longer included. The information that was previously included here can be found under falcVtlLibrarySystem, in the falcVtlPhysicalLibs, falcVtlPhysicalDrives, and falcVtlPhysicalTapes tables.

falcVtlSanClients

Displays information about SAN clients (backup servers).

Table	Description
SanClient	Information about each backup server, including: • *falcVtlSanClientID* - SAN client ID • *falcVtlSanClientName* - SAN client name • *falcVtlSanClientType* - SAN client type: Fibre Channel, iSCSI, HostedBackup
FCClientResource	Information about virtual resources assigned to each FC client, including: • *ResourceID* - SAN Resource ID • *ResourceName* - SAN Resource name • *ClientID* - Client ID • *ClientName* - Client name • *ResourceAllocType* - Resource type (direct device virtual library, direct device virtual drive) • *LUN* - SCSI LUN of client • *InitatorWWPN* - WWPN of the client's initator HBA • *TargetWWPN* - WWPN of the client's target HBA • *Access* - Read/write access mode
ISCSIClientResource	Information about virtual resources assigned to each iSCSI client, including: • *ResourceID* - SAN Resource ID • *ResourceName* - SAN Resource name • *ClientID* - Client ID • *ClientName* - Client name • *ResourceAllocType* - Resource type • *LUN* - SCSI LUN of client • *IPAddress* - Client IP address • *TargetID* - Client target ID • *TargetName* - Client target name
falcVtlSanClientsInfo	Total number of backup servers.

Common MIBs

These MIBs monitor COPAN 400.

falcServer

The falcServer MIB has the following tables:

Table	Description
falcServiceTable	Current state (service-up/service-down) of each COPAN 400 server process and module.
falcServerInfo	Provides general system status, including capacity watermarks and any monitored triggers. • Green - No further attention is needed. • Yellow - A watermark or non-critical alert has been triggered. • Red - The system is at risk of failing or filling up within the next 48 hours.

falcEvents

The falcEvents MIB displays the same errors, warnings, informational messages, and attention required information displayed in the console.

The falcEvents MIB has the following tables:

Table	Description
falcErrorEventTable	Displays error events logged in the Event Log.
falcWarningEventTable	Displays warning events logged in the Event Log.
falcInformationalEventTable	Displays informational events logged in the Event Log.
falcAttentionRequiredTable	Displays attention required events logged on the *Attention Required* tab.
falcCriticalEventTable	Displays critical error events logged in the Event Log.

Troubleshooting

This chapter contains general troubleshooting information and a list of error codes generated by COPAN 400 servers.

General Console operations

The console is unable to connect to a COPAN 400 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 COPAN 400 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 COPAN 400 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 the console is installed open a SSH session to the COPAN 400 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 COPAN 400 server is running, go to the system console and type:
  revolution status.

  If a module has stopped, restart it with the command:
  revolution 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 COPAN 400 license** - Contact technical support.

- **Expanding the COPAN 400 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 COPAN 400 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/log/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 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 COPAN 400 server is very busy performing heavy processing. You can check the Event Log or syslog (/var/log/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 console does not show physical storage devices correctly

There are several steps to try when physical storage devices have been connected/ assigned to the COPAN 400 server yet they are not showing in the console.

Rescan devices

Perform a rescan from the 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/log/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 COPAN 400 initiator driver and use persistent binding. Otherwise, COPAN 400 cannot manage the storage.

An HBA port is missing after rebooting and restarting COPAN 400

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" in 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 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 COPAN 400 to make sure that each physical resource is accessible.

Disks are displayed as "offline" in the console

All storage devices must be powered on before the appliance is started. If storage is not available when the appliances are up, reboot all appliances for the system to come up properly.

Client cannot see tape library/drive as provisioned by COPAN 400

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" in 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 COPAN 400 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 COPAN 400 target driver. Otherwise some clients cannot detect more than eight LUNs on COPAN 400 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. COPAN 400 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/log/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 COPAN 400.

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 (tape library or drive)

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 COPAN 400 server 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 COPAN 400 services or rebooting. To enable *portmap*, you will have to run the following command: chkconfig --add portmap

Export to direct link tape fails

Writing data to a direct link tape will fail if the media types are not the same between your physical and virtual tapes. When you create a cache for your physical tapes, you must make sure that your physical tapes use the same media type as your virtual tapes.

NDMP

NDMP backup jobs are failing

If you are using NDMP, you must define the hostname of the COPAN 400 server in the
/etc/hosts file in the format "IPAddress Hostname".
For example: 10.7.2.41 Server41

The COPAN 400 server NDMP daemon fails to start

Because some backup applications use NDMP, if you are running backup software on the COPAN 400 server, it should be started after COPAN 400 has started and should be stopped before COPAN 400 is stopped. Otherwise, the NDMP service that is loaded by the backup software may interfere with COPAN 400's NDMP service.

Replication

There are several aspects to replication: replication configuration, replication process, replica resource promotion, replication configuration removal. If a problem occurs and you get a message on the *Attention Required* tab, check the Event Log or syslog (/var/log/messages). Look for error messages relating to replication. Some common problems are described below.

Replication configuration

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 process

Replication fails

When replication finishes successfully, you will see "`replica_fin 10000342 0`". If you see a number other than zero, there was a problem. In the message below, replication was manually stopped from the primary server or it was stopped because the primary tape was moved into a drive.

```
Jan 13 15:52:54 VTL89-115 kernel: IOCORE1 [iocore|29557]
OnSANREPRequest, SANREP_STOP_REPLICATION
Jan 13 15:52:54 VTL89-115 ipstorcomm
[mgtpipe_exec.c:pipe_thread:3109][29861]:
Rcv'd mgtpipe cmd: 'replica_fin 10000342 1'
```

In the following message, you see `Failed to get virtual tape`. This indicates that the replica tape has been deleted but a request to the tape was delayed and is still trying to get its information. In this case, no action is required.

```
Jan 13 16:18:43 VTL89-115 ipstorcomm
[SANConsoleRPC_proc.c:sanconsolerpcgetvdevinfo2_1_svc:16499][29861]:
Failed to get virtual tape 10000219
```

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.

Replica resource promotion

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.

Replication configuration removal

You try to remove a replication configuration for a tape but it fails. Search for a message that contains `[crres.c:ReplicationRemoval:6469]`. A return code of `ret=-2146631164` means that the tape that has no data on it (size is zero).

Import/Export

Import/Export does not work as expected

Check tape capacity mismatch

When you Import/export data between a physical tape device and a virtual device, you must make sure the tape devices are of the same type and the same capacity. If they do not have the same capacity, an end-of-media-hit condition occurs and import/export fails.

If data compression is used, make sure the *actual* capacity matches, not just the *compressed* capacity. Import/export will fail when the destination does not have enough space to hold uncompressed data coming from source.

Check job status

Highlight the *Budget Queue* and search for a job related to this operation. If the job is in progress, wait until it is completed. If the job is not there and the import/export operation is not done, look at console Event Log to see if there are any job failure messages.

Check barcodes of virtual tapes

When you import data from a physical tape, make sure the virtual tapes have different barcodes. Otherwise, the import operation fails. Use the *Inventory* feature in the console to get the updated bar codes and status from the physical library.

Check physical tape library and device status

Make sure the physical tape library does not show any abnormal situation. For example, the tape drives may require cleaning or tapes may need to be moved to the proper location.

Check element address on the physical library

When you import data, make sure the assignment of drive in COPAN 400 follows the element address of the drives in the physical library. Assign the tape drive in the order of their element address.

For example, an import job cannot be executed and the physical library has two DLT 8000 drives with the following configuration:

```
Library SCSI ID: 1
Drive at element address 1200: SCSI ID 10
Drive at element address 1201: SCSI ID 09
```

```
COPAN 400 Resources:
ABC-00003
DLT8000-0008: SCSI ID 09
DLT8000-0009: SCSI ID 10
```

In this case you need to unassign tape drives, select first DLT8000-0009, assign it, then select DLT8000-0008, and assign it to the physical library ABC-00003.

Check system log for errors

Check the Event Log or syslog (/var/log/messages). Look for error messages relating to the physical tape library or drive. If you find error messages but cannot find the cause, contact technical support.

System event messages

Information from the /var/log/messages file on the COPAN 400 server can be viewed via the Event Log in the console. A maximum of 10,000 records will be displayed in the Event Log.

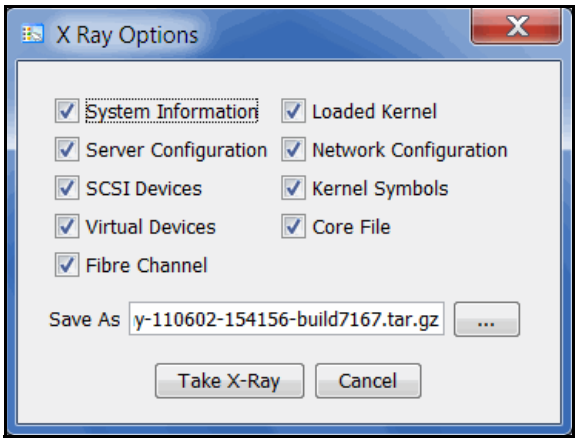
For troubleshooting purposes, /var/log/messages keeps track of the last 20 MB of system events. When the file reaches 20 MB, it is renamed to messages.*n*, where *n* is a sequential number between 1 and 30. When it is renamed, it is also compressed to save space.

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 COPAN 400 server and select *X-Ray*.



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

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

Error codes

This section contains error messages generated by COPAN 400 servers.

Number	Type	Text	Probable Cause	Suggested Action
1005	Error	Out of kernel resources. Failed to get major number for COPAN 400 SCSI device.	Too many Linux device drivers are installed.	Type cat /proc/devices for a list to see if any can be removed.
1006	Error	Failed to allocate memory.	Memory leak from various modules in the Linux OS, most likely from network adapter or other third-party interface drivers.	Check the Knowledge Base for known memory leak problems in various drivers.
1008	Error	Failed to set up the network connection due to an error in SANRPCListen -- [Error].	Another application is using UDP port 11577.	Confirm using *netstat -a,* then remove or reconfigure the offending application.
1023	Error	Failed to connect to physical device [Device number]. Switching to alias to [ACSL].	Adapter/cable problem.	Check for a loose or damaged cable on the affected drive.
1030	Error	Failed to start replication -- replication is already in progress for virtual tape.	Replication is still in progress when a new replication is manually triggered by a user or started by the scheduler based on the replication policy.	If replication is manually triggered by the user, check the replication status in the right panel before starting another replication. If replication is triggered by the scheduler, adjust the schedule in the replication policy to avoid replicating too often.
1043	Error	A SCSI command terminated with a non-recoverable error condition that was most likely caused by a flaw in the medium or an error in the recorded data.	Most likely caused by a flaw in the medium or an error in the recorded data.	Check the system log for additional information. Contact the hardware manufacturer for a diagnostic procedure.

Number	Type	Text	Probable Cause	Suggested Action
1044	Error	A SCSI command terminated with a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.). Check the system log for additional information.	General I/O error that is not medium related. This can be caused by a number of potential failures, including controller failure, device failure, parity error, etc.	Check the system log for additional information. Contact the hardware manufacturer for a diagnostic procedure.
1061	Warning	I/O path failure detected. Alternate path will be used. Failed path (A.C.S.L): [ACSL]; New path (A.C.S.L): [ACSL].	An alias is in use due to primary path failure.	Check primary path from COPAN 400 appliance to physical device.
1067	Error	Replication cannot proceed -- unable to connect to replica server.	The primary server cannot connect to the target server. Either there is a problem with the network or the target server is busy.	Check if the network is working properly and check server activity. If replication is triggered by the user, wait until the network is working properly or until the server is not as busy. If replication is triggered by the scheduler, next replication will be started at the next scheduled time.
1069	Error	Replication cannot proceed -- virtual tape [VT#] no longer has a replica or the virtual tape replica does not exist.	The replica of the virtual tape no longer exists on the target server. It might have been removed from the target server while the primary server was not available.	Remove replication setup from the virtual tape console since it no longer has a valid replica.
1084	Error	A SCSI command terminated with a recovered error condition. This may indicate that the device is becoming less reliable. Check the system log for additional information.	The physical devices, i.e., the SCSI disks or the RAID, returned an error code reporting that the I/O operation initially encountered an error, but was successful after a retry. This may indicate the reliability of the storage device is questionable.	If possible, determine the true cause of the problem by contacting the hardware manufacturer. If the drive is reaching MTBF*, it may be prudent to replace the drive.
1087	Warning	Replication cannot proceed -- virtual tape %1 is in the drive.	The tape is in the drive when replication was triggered.	None.

Number	Type	Text	Probable Cause	Suggested Action
7001	Error	Patch %1 failed -- environment profile is missing in /etc.	Unexpected loss of environment variables defined in /etc/.is.sh on the server.	Check server package installation.
7002	Error	Patch %1 failed -- it applies only to build %2.	The server is running a different build than the one for which the patch is made.	Get the patch, if any, for your build number or apply the patch on another server that has the expected build number.
7003	Error	Patch %1 failed -- you must be the root user to apply the patch.	The user account running the patch is not the root user.	Run the patch with root account.
7004	Warning	Patch %1 installation failed -- it has already been applied.	You tried to apply the patch again.	None.
7005	Error	Patch %1 installation failed -- prerequisite patch %2 has not been applied.	A required previous patch has not been applied.	Apply the required patch before applying this one.
7006	Error	Patch %1 installation failed -- cannot copy new binaries.	Unexpected error on the binary file name or path in the patch.	Contact Technical Support.
7008	Warning	Patch %1 rollback failed -- there is no original file to restore.	Patch has not been applied or was already rolled back.	None.
7009	Error	Patch %1 rollback failed -- cannot copy back previous binaries.	Unexpected error on the binary file name or path in the patch.	Contact Technical Support.
7010	Error	Patch %1 failed -- the file %2 has the patch level %3, higher than this patch. You must rollback first %4.	A patch with a higher level, and conflicting with the current patch, has been applied.	Roll back the high-level patch, apply this patch, and then apply the high-level patch.
7011	Error	Patch %1 failed -- it applies only to kernel %2.	A patch was applied to a server running an unexpected OS.	Apply the patch on a server that has the expected kernel.
10001	Error	Insufficient privilege (uid: [UID]).	COPAN 400 software is not running with root privilege.	Login as root to the Linux server where COPAN 400 will be running before starting COPAN 400.

Number	Type	Text	Probable Cause	Suggested Action
10002	Error	COPAN 400 Server environment is corrupt.	The configuration file in the /etc directory, which provides the COPAN 400 home directory and other environmental information, is either corrupted or deleted.	Determine the cause of the corruption and correct the situation. Perform regular backups of COPAN 400 configuration data so it can be restored if corrupted by known elements.
10003	Error	Failed to initialize configuration [File name].	During the initialization process, one or more critical processes experienced a problem. This may be due to system drive failure, storage hardware failure, or system configuration corruption.	Check storage device connectivity, check the system drive for errors (use OS provided utilities), and check for COPAN 400 environment corruption as described in 10002.
10004	Error	Failed to get SCSI device information.	An error occurred when adding newly discovered SCSI devices to the system. This is most likely due to unreliable storage connectivity, hardware failure, or low system resources.	Check the storage devices for power status, controller status, etc. Check for proper connectivity. Fibre Channel switch connection status lights do not guarantee a solid connection. Disconnect/reconnect the Fibre Channel connector for verification. Check the specific storage device using OS provided utilities such as *hdparm*.
10006	Error	Failed to write configuration [File name].	An error was encountered when writing the COPAN 400 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or encountered a hardware failure.	Check the system drive using OS provided utilities. Free up space if necessary. If the drive is unreliable or reaching MTBF*, it may be prudent to replace the drive.

Number	Type	Text	Probable Cause	Suggested Action
10100	Error	Failed to scan new SCSI devices.	An error occurred when adding newly discovered SCSI devices to the system. This is most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004 for information about checking storage devices. If system resources are low, use *top* to check the process that is using the most memory. If physical memory is below the recommendation, install more memory. If the OS is suspected to be in a bad state due to unexpected failure in either hardware or software components, restart the server machine to make sure the OS is in a healthy state before trying again.
10101	Error	Failed to update configuration [File name].	An error was encountered when updating the COPAN 400 configuration file on the system drive. This can only happen if the system drive is corrupted or has failed.	Check the system drive using OS provided utilities.
10102	Error	Failed to add new SCSI devices.	An error occurred when adding newly discovered SCSI devices to the system. This is most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10004.
10200	Warning	Configuration [File name] exists.	A COPAN 400 configuration file already exists when installing the COPAN 400 software, possibly from a previous installation. The configuration file will be reused.	If there is reason to believe the existing configuration should not be used (i.e., the file is suspected of being corrupted), remove the COPAN 400 directory before reinstallation.
10210	Warning	Marked virtualized PDev [GUID] OFFLINE, guid does not match SCSI guid [GUID].	A physical device has a different GUID written on the device header than the record in the configuration file. This is most likely caused by old drives being imported without proper initialization, or more unlikely, due to corruption of the configuration or the device header.	Check the physical connection of the storage and the storage system. If problem persists, call Technical Support.

Number	Type	Text	Probable Cause	Suggested Action
10212	Warning	Marked PDev [GUID] OFFLINE because scsi status indicate OFFLINE.	The physical storage system response indicates the specific device is off-line. It may have been removed, turned off, or malfunctioning.	Check the storage system, including all cabling. Once the problem is corrected, rescan the adapter with the connected drive. Limit the scope of the scan to that SCSI address.
10213	Warning	Marked PDev [GUID] OFFLINE because it was not detected.	The physical device that exists in the configuration is not responding to commands. Its status is now set to OFF-LINE. All virtual drives affected will also be set to OFF-LINE. Most likely the drive or storage system is turned off, or the cable is disconnected, etc.	Check the storage system, including all cabling. Once the problem is corrected, rescan the adapter with the connected drive. Limit the scope of the scan to that SCSI address.
10214	Warning	Marked PDev [GUID] OFFLINE because its GUID is an invalid FSID.	The GUID in the header of the drive does not match the unique ID, called the FSID, which is based on the external properties of the physical drive. It may be caused by drives being changed while COPAN 400 is down.	Make sure drives are not changed without using the console to eliminate them from the virtual resource list first. Also never allow other applications to directly access the physical drives without going through COPAN 400.
10215	Warning	Marked PDev [GUID] OFFLINE because its storage capacity has changed.	The physical drive geometry, including the number of sectors, is different from the original record.	Rescan the drive to re-establish its properties.
10240	Error	Missing SCSI Alias [A,C,S,L].	One of the existing SCSI paths for the device is not accessible. This is most likely caused by a storage cable being disconnected or by Fibre Channel switch re-zoning. This can also be caused by failure of one of the storage ports.	Check cabling and the storage system. After the situation is corrected, rescan the adapter connected to the drive, and limit the scope to that path.
10241	Error	Physical Adapter [Adapter number] could not be located in /proc/scsi/.	The adapter driver could be unloaded.	Check the loaded drivers.

Number	Type	Text	Probable Cause	Suggested Action
10244	Error	Invalid FSID, device [Device ID] LUN in FSID [FSID] does not match actual LUN.	The FSID is generated with the LUN of the device. Once a device is used by COPAN 400, it is not allowed to have the LUN changed.	Do not change the LUN of a virtualized drive. Revert back to the original LUN.
10246	Error	Fail to generate FSID for device acsl:[A C S L], can't validate FSID.	The physical drive does not present valid data for unique ID generation, even if the inquiry pages exist.	Only use this type of drive as a virtual drive and not a SED.
10247	Error	Device (acsl:[A C S L]) GUID is blank, can't validate FSID.	Some process may have erased the disk header. This can be due to an accidental erase by *fdisk*.	Never bypass COPAN 400 to access the virtual drives.
11000	Error	Failed to create socket.	This kind of problem should rarely happen. If it does, it may indicate a network configuration error, possibly due to system environment corruption. It is also possible that the network adapter failed or is mis-configured. It is also possible that the network adapter driver is the problem.	Restart the network. If the problem persists, restart the OS or restart the machine (hard/cold reset). If the problem still persists, you may need to reinstall the OS. If that is the case, make sure you properly save all COPAN 400 configuration information before proceeding.
11001	Error	Failed to set socket to re-use address.	System network configuration error, possibly due to system environment corruption.	See 11000.
11002	Error	Failed to bind socket to port [Port number].	System network configuration error, possibly due to system environment corruption.	See 11000.
11003	Error	Failed to create TCP service.	System network configuration error, possibly due to system environment corruption.	See 11000.
11004	Error	Failed to register TCP service (program: [Program name], version: [Version number]).	System network configuration error, possibly due to system environment corruption.	See 11000.

Number	Type	Text	Probable Cause	Suggested Action
11006	Error	COPAN 400 communication module Failed to start.	This is most likely due to the port for the COPAN 400 communication module is being occupied by a previous unexpected failure of the communication module, or by another application.	Restart the OS and try again. If the problem persists, use the OS provided utilities, such as *netstat*, to check the port used.
11032	Error	Auto save configuration: cannot connect to FTP server port.	The FTP sever is not accessible.	Make sure that the FTP server is running and accessible from the COPAN 400 system.
11033	Error	Auto save configuration: cannot login user.	Incorrect user name or password.	Double check the user name and password specified in the auto save configuration settings.
11034	Error	Auto save configuration: directory doesn't exist.	The target directory specified in the auto save configuration setting doesn't exist on the FTP server.	Create the specified directory or use an existing directory.
11035	Error	Auto save configuration: failed to copy to FTP server.	The specified FTP user may not have write access to copy files. It can also happen if the FTP server doesn't have enough space.	Check the user access rights for the FTP user specified in the auto save configuration setting. Also check the free space available on the FTP server.
11036	Error	Auto save configuration: failed to delete old file from FTP server.	The specified user doesn't have rights to delete files on the FTP server.	Check the access rights of the specified user.
11050	Warning	Cannot start replication for virtual device [VD#] because it's on LUN [L#], which is being migrated.	A replication operation was triggered for a tape that has segments on a LUN that is being migrated.	No specific user action required. Replication will continue at the next scheduled time, after the LUN migration is completed.
11101	Error	SAN Client ([host name]): Failed to add SAN Client.	This error is most likely due to system configuration error, or system resources running low.	Check OS resources using provided utilities such as *top*.
11104	Error	There are too many SAN Client connections.	The number of simultaneous connections exceeded the supported limit the current system resource can handle.	This is an unlikely condition as long as the recommended memory is available to the server.

Number	Type	Text	Probable Cause	Suggested Action
11112	Error	SAN Client ([host name]): Failed to parse configuration file [File name].	The configuration file is corrupted or manually tempered so that it is no longer recognizable by COPAN 400. If corruption is the cause, then it is most likely due to a system drive hardware error.	If there is a valid configuration file saved, it can be restored to the system. Make sure to use reliable storage devices for any critical system functions.
11114	Error	SAN Client ([host name]): Failed to allocate memory.	System resources are running low. This may be due to too little memory installed in the system or a runaway process that is consuming too much memory.	Use *top* to check the process that is using the most memory. If physical memory is below the recommendation, install more memory.
11170	Error	Failed to virtualize LUN [L#] because of a mismatched size between the configuration file and disk. Rescan and try it again.	Attempting to virtualize a LUN that has a different capacity than what was previously seen.	Rescan for new devices and try again.
11201	Error	There are too manyconsole connections.	Too many console processes are connected to the particular COPAN 400 server. This is a highly unlikely condition.	None.
11202	Error	Console ([host name]): Illegal access.	The console host attempted to perform an operation outside of its privilege level. This rarely happens. If it does, it is either due to a retry operation from an unexpectedly terminated connection that was assigned a different privilege level or it is a deliberate break-in attempt to reverse engineer the COPAN 400 console software, which is not feasible.	See 11107.

Number	Type	Text	Probable Cause	Suggested Action
11203	Error	Console ([host name]): SCSI device re-scanning has failed.	An error occurred when adding newly discovered SCSI devices to the system. This is most likely due to unreliable storage connectivity, hardware failure, or low system resources.	See 10100.
11204	Error	Console ([host name]): SCSI device checking has failed.	An error occurred when accessing SCSI devices when the console requests the server to check the known storage devices. This is most likely due to a storage connectivity failure or hardware failure.	Check the storage devices, e.g., power status; controller status, etc. Check the connectivity, e.g., cable connectors. In Fibre Channel switches, even the connection status light indicates the connection is good, it is still not a guarantee. Disconnect/reconnect the connector to make sure. Check the specific storage device using OS provided utilities such as *hdparm*.
11209	Error	Console ([host name]): Insufficient privilege access.	A 'read only' user attempted to do an operation that requires configuration change.	Log in as an administrator user if configuration changes need to be made.
11211	Error	Console ([host name]): Failed to save file [filename].	An error was encountered when writing the COPAN 400 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or if there is a hardware failure in the system drive.	See 10006.
11212	Error	Console ([host name]): Failed to create index file [file name] for Event Log.	Failed to create an index file for the event log retrieval. This is most likely due to insufficient system disk space.	Free up disk space, or add additional disk space to system drive.
11216	Error	Console ([host name]): Out of system resources. Failed to fork process.	The COPAN 400 server is low in memory resources for normal operation.	See 11114.

Number	Type	Text	Probable Cause	Suggested Action
11219	Error	Console ([host name]): Failed to add virtual device [Device number].	Failed to create a virtual drive due to a system configuration error, storage hardware failure, or system resource access failure.	Check system resources, such as memory, system disk space, and storage device connectivity (cable connections).
11233	Error	Console ([host name]): Failed to map the SCSI device name for [A C S L].	The mapping of the SCSI address, namely the adapter, channel, SCSI ID, and LUN, (ACSL) is no longer valid. This is due to sudden failure, improper removal, or change of storage devices in the COPAN 400 server.	See 11204. Check and restore the physical configuration to a proper state if changed improperly.
11234	Error	Console ([host name]): Failed to execute hdparm for [Device number].	Failed to perform the device throughput test for the given device. This can be due to an OS in a bad state such that the program cannot be run or the storage device failed.	Test run the *hdparm* program from the COPAN 400 server console directly. Check storage devices as described in 11204.
11240	Error	Console ([host name]): Failed to start the COPAN 400 server module.	When a COPAN 400 process cannot be started, it is most likely due to insufficient system resources, an invalid state left by COPAN 400 processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this occurs frequently, there are external factors that contributed to the behavior and these must be investigated and removed before running the COPAN 400 server.	If system resources are low, use *top* to check the process that is using the most memory. If physical memory is below the recommendation, install more memory. If the OS is suspected of being in a bad state due to an unexpected failure in either hardware or software components, restart the server machine to make sure the OS is in a healthy state before trying again.

Number	Type	Text	Probable Cause	Suggested Action
11242	Error	Console ([host name]): Failed to stop the COPAN 400 server module.	When any COPAN 400 process cannot be started, it is most likely due to insufficient system resources, an invalid state left by COPAN 400 processes that may not have been stopped properly, or an unexpected OS process failure that left the system in an unstable state. This should happen very rarely. If this occurs frequently, there are external factors that contributed to the behavior and these must be investigated and removed before running the COPAN 400 server.	If system resources are low, use *top* to check the process that is using the most memory. If physical memory is below the recommendation, install more memory. If the OS is suspected of being in a bad state due to unexpected failure in either hardware or software components, restart the server machine to make sure the OS is in a healthy state before trying again.
11257	Error	Console ([host name]): Failed to add SAN Client ([Host name]).	See 11101.	See 11101.
11261	Error	Console ([Host name]): Failed to get SAN Client connection status for virtual device [Device ID].	Failed to get a SAN Client connection status due to a system configuration error, storage hardware failure, or system resource access failure. This should rarely happen.	Check system resources, such as memory and system disk space. Check the syslog for a specific reason for the failure.
11262	Error	Console ([host name]): Failed to parse configuration file [File name].	See 11112.	See 11112.
11263	Error	Console ([host name]): Failed to restore configuration file [File name].	See 10006.	See 10006.
11266	Error	Console ([host name]): Failed to erase partition of virtual device [Device number].	Storage hardware failure.	See 10004.

Number	Type	Text	Probable Cause	Suggested Action
11291	Error	Console ([host name]): Failed to update meta information of physical device [Device number].	Storage hardware failure.	See 10004.
11292	Error	Console ([host name]): Failed to swap IP address from [IP address] to [IP address].	See 11000.	See 11000.
11295	Error	Console ([host name]): Invalid configuration format.	See 11112.	See 11112.
11315	Error	You have no license for %1 protocol.	An attempt was made to enable a protocol such as Fibre Channel without the appropriate license key.	Install the appropriate license key that includes support for the needed protocol.
11316	Error	You have exceeded the storage capacity allowed by your license, used space=%1MB, needed space=%2MB, licensed capacity=%3MB.	Physical capacity usage has exceeded the capacity allowed by the license.	Contact SGI to purchase an additional capacity license.
11406	Error	Failed to prepare the failover configuration package.	Suspend failover was initiated while packaging failover configuration information.	No action required. The operation will be retried automatically.
11407	Error	Failed to extract the failover configuration package.	Same as 11406	No action required. The operation will be retried automatically.
11500	Error	Out of disk space to expand virtual tape.	There is no storage space available to expand a virtual tape.	Add more storage to the COPAN 400 system.

Number	Type	Text	Probable Cause	Suggested Action
11512	Error	Console: Failed to add a replica for virtual tape to the server (watermark: MB, time: , interval: , watermark retry: , suspended:).	There may have been a connection error while the primary server was synchronizing the initial status of the virtual tape to the replica on the target server or the virtual tape is loaded in the drive at the moment by backup software or a console on a different machine.	Check that the network is working properly and correct any problems. If the virtual tape is moved to the drive, reconfigure replication later.
11514	Error	Console: Failed to remove the replica for virtual tape from the Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	An error was encountered when writing the COPAN 400 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or if there is hardware failure in the system drive.	Check to make sure there is enough free space on the system disk. (This should never happen since the COPAN 400 system has a mechanism to automatically prune the syslog periodically to prevent the syslog from using up all system disk free space). If enough space is available on system disk, check the integrity of the system disk file system using the *fsck* utility.
11516	Error	Console: Failed to create the virtual tape replica.	Could not update the virtual tape partition information on disk.	Check the storage system and make sure that storage is working properly.
11518	Error	Console: Failed to start replication for virtual tape.	Replication triggered manually by the user failed. It can be due to one of the following reasons: network problems, the virtual tape is loaded in a drive, replication is in progress, or the replica no longer exists.	See actions for corresponding events: 1067, 1030 and 1069.
11522	Error	Console: Failed to promote virtual tape replica to a virtual tape.	Failed to update the virtual tape partition information.	Check if the physical disk is working properly or the server is busy. Retry the operation when the physical disk is working properly or when the server is not busy.
11524	Error	Console ([host name]): Failed to run COPAN 400 Server X-Ray.	See 11240.	See 11240.

Number	Type	Text	Probable Cause	Suggested Action
11534	Error	Console ([host name]): Failed to reset the umap for virtual device [Device number].	Storage hardware failure.	See 10004.
11535	Error	Console: Failed to update the replication parameters for virtual tape to The Server (watermark: MB, time: , interval: , watermark retry: , suspended:).	An error was encountered when writing the COPAN 400 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or if there is a hardware failure in the system drive.	Check if the system drive is out of space or has any corruption.
11537	Error	Console ([host name]): Failed to claim physical device [Device number].	This may due a specific version of the COPAN 400 server limiting the support of the storage.	Check the license agreement for the version of COPAN 400 server.
11539	Error	Console ([host name]): Failed to import physical device [Device number].	Storage hardware failure.	See 10004.
11542	Error	Console: Failed to remove virtual tape replica.	An error was encountered when writing the COPAN 400 configuration file to the system drive. This can only happen if the system drive ran out of space, is corrupted, or if there is a hardware failure in the system drive.	Check if the system drive is out of space or has any corruption.
11554	Error	Console ([host name]): Failed to set failover option <selfCheckInterval:>	IP network communication failure.	Check network connectivity.
11569	Error	Console ([host name]): Failed to set [Device number] to Fibre Channel mode [Mode].	This is possibly due to the Fibre Channel driver being improperly loaded or the wrong version of the driver is loaded. COPAN 400 FC target mode requires the COPAN 400 version of the driver to be used.	Use *lsmod* to check that the proper COPAN 400 driver is loaded. If it is, check to make sure it is the correct revision. The correct revision should be located in the COPAN 400/lib directory.

Number	Type	Text	Probable Cause	Suggested Action
11578	Error	Console ([host name]): Failed to get Fibre Channel initiator information.	See 11569.	See 11569.
11632	Error	Console: Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: sec>.	IP network communication failure.	Check network connectivity.
11633	Error	Console : Failed to set failover option on secondary server <heartbeatInterval: sec, autoRecoveryInterval: disabled>.	Same as 11632	Check Network connectivity.
11648	Error	Failed to get inquiry string on SCSI device [Device ID].	Hardware problem with a SCSI device.	Check hardware.
11651	Error	Medium test failed for SCSI device [Device name].	Hardware problem with a SCSI device.	Check hardware.
11652	Error	Could not get type for SCSI device [Device ID] because of inquiry string failure.	Hardware problem with a SCSI device.	Check hardware.
11655	Error	Discarded scsi device [Device ID], bad capacity size.	Hardware problem with a SCSI device.	Check hardware.
11741	Error	Console: Failed to create virtual library with [#of Slots] slots due to only [#of Slots] slots available.	The specified slot count for the virtual library exceeds the total slot count supported by the system.	Specify the appropriate slot count.
11742	Error	Console: Create only [count] out of [count] virtual drives requested due to memory allocation failure.	The system is out of memory, which prevents the creation of the specified number of virtual tape drives.	Increase system memory.

Number	Type	Text	Probable Cause	Suggested Action
11744	Error	Console: The configuration file update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write to the COPAN 400 configuration file.	Check /usr partition for free space. If the partition is out of space, delete unwanted files to create space.
11745	Error	Console: The disk partition update for testmode promoting [#of tapes] tapes was rolled back.	Failed to write update partition information to disks.	Check physical connectivity to the storage system/LUN.
11746	Error	Console: The testmode promotion of [# of tapes] tapes was rolled back.	Cannot add the device to IOCore module.	Call Technical Support.
11782	Error	Barcode of the source tape already exist on target server. Auto-replication cannot be configured.	A tape with the same barcode exists on the remote sever.	Remove the tape with same barcode from the remote server or change its barcode.
11788	Error	Appliance Hardware Problem:	Detected an error on the COPAN 400 appliance.	Check the error message for information on the error to determine the solution.
11791	Error	Failed to re-size virtual tape to MB. Error:	Virtual tape partition information couldn't be updated. This could happen in rare cases when the system is extremely busy and updates to disks take too long.	No user action required since it doesn't cause any problem for backup/restore. If this error happens, the tape will not be resized.
11793	Warning	Appliance Hardware Problem: message	Detected a hardware problem with the appliance.	Check the error message and take appropriate hardware maintenance.
12509	Error	Failed to inventory physical library VID.	The physical library inventory process failed.	Check the server log for more information on the cause of the hardware failure.
12511	Error	Failed to move tape in library VID from slot %2 to drive VID.	The physical tape move from slot to drive failed.	Check the server log for more information on the cause of the hardware failure.
12514	Error	Failed to restart job <Job ID, (cmd <IOCTL Call number>, rc <IOCTL Return Code>).	An import/export tape job failed probably due to the tape not being present or the tape drive not being available.	Check that the tape exists and the tape drive is available for the job to continue and then restart the job.

Number	Type	Text	Probable Cause	Suggested Action
12521	Error	Failed to move tape in library VID from drive VID to slot VID.	The physical library may have hardware issues.	Check the server log for more information on the cause of the hardware failure.
12611	Error	Failed to add ACSLS lib to physical library %1, tleioctl failed, errno = %2.	The ACSLS server cannot be added into the list of physical libraries due to connection problems or initialization issues.	Check the ACSLS library to make sure it is running properly and is connected correctly to the COPAN 400 server.
13309	Error	Failed to communicate with the primary server.	The secondary server failed to talk to the primary server.	Check network connectivity.
13704	Warning	COPAN 400 failure detected.	The secondary server detected a software/ hardware failure on the primary server. This will trigger a takeover operation.	Once the primary server is brought back up, manually initiate a failback operation.
13710	Warning	The Live Trial period has expired for COPAN 400 Server [Server name]. Contact SGI or its representative to purchase a license.	The 30-day live trial grace period has been exceeded.	Contact SGI or its representative to obtain a proper license.
13711	Warning	The following options are not licensed: [COPAN 400 option]. Contact SGI or its representative to purchase a license.	The specific option is not licensed properly.	Contact SGI or its representative to obtain a proper license.
13800	Critical	Primary server failure detected. Failure condition:	The primary server detected a software/hardware failure on itself. This will trigger a failover operation to the secondary server.	Once the primary server is brought back up, manually failback operations to the primary server.
13804	Error	Quorum disk failed to release to secondary.	Negotiations through the Quorum disk failed.	Check storage or connectivity to storage.
13817	Critical	Primary server failback operation failed.	The primary server had a software/hardware failure condition during failback.	Check hardware (such as FC ports), storage, and connectivity to storage.
13820	Warning	Primary server heartbeat not detected. Testing network connectivity.	Network communication failure.	Check network connectivity.

Number	Type	Text	Probable Cause	Suggested Action
13821	Error	Failed to contact other entities in network. Assume failure in secondary side. Failover not initiated.	There was a network connectivity failure and there is no connectivity to the outside network.	Check network connectivity and the secondary server's health.
13822	Warning	Secondary will not take over because storage connectivity is not 100%.	There was a storage or storage connectivity failure on the secondary server.	Check storage or connectivity to storage.
13828	Warning	Almost running out of file handler (current [Number of handles], max [Number of handles]).	The Linux system is running out of resources for file handles.	Determine the appropriate amount of memory required for the current configuration and applications. Determine if there are processes that are leaking memory.
13829	Warning	Almost running out of memory (current [Number of KB] K, max [Number of KB]).	The Linux system is running out of memory.	See 13828.
13856	Error	Secondary server ServerName failed to communicate with primary server ServerName through IP IPAddress.	A network connectivity failure occurred between the primary and secondary servers.	Check network connectivity between the primary and secondary servers.
14005	Error	Cannot update partition information.	Storage is offline.	Check connectivity to storage.
15055	Error	Server ioctl call [Device ID] failed on vdev id [Device ID]: Device or resource is busy (EBUSY).	The virtual drive is busy with I/O and is not responsive to the upper layer calls.	Try again when the system is less busy or determine the cause of the extensive I/O and correct the situation if necessary.
16100	Warning	Email Alerts failed to connect to SMTP server ServerIP on port PortID.	There are connectivity problems with the SMTP server due to IP address or PortID. Login credentials for the SMTP server are incorrect when *authentication mode* is on.	Check network connectivity, SMTP server IP address, and PortID. If the SMTP server requires *authentication mode* to be set, check that the user ID and password are correct.
16101	Warning	Email Alerts failed to send email to SMTP server ServerIP on port PortID.	See 16100.	See 16100.

Number	Type	Text	Probable Cause	Suggested Action
17001	Error	Rescan replica cannot proceed due to replication already in progress.	A rescan cannot be performed when replication is in progress.	Wait for the process to complete before trying again or change the replication schedule.
17002	Error	Rescan replica cannot proceed due to replication control area missing.	There may be a storage problem.	Check the virtual device layout and storage devices for missing segments.
17003	Error	Rescan replica cannot proceed due to replication control area failure.	There may be a storage problem.	Check the virtual device layout and storage devices for missing segments.
17004	Error	Replication cannot proceed due to replication control area failure.	There may be a storage problem.	Check the virtual device layout and storage devices for missing segments.
17005	Error	Replication cannot proceed due to replication control area failure.	There may be a storage problem.	Check the virtual device layout and storage devices for missing segments.
17006	Error	Rescan replica cannot proceed due to replication control area failure.	There may be a storage problem.	Check the virtual device layout and storage devices for missing segments.
17011	Error	Rescan replica failed due to network transport error.	Rescan requires a connection to the replica server. A network problem will cause rescan to fail.	Check network conditions between the servers.
17012	Error	Replicating replica failed due to network transport error.	Replication failed due to a network condition.	Check network conditions between the servers.
17013	Error	Rescan replica failed due to local disk error.	Rescan encountered a disk I/O error from the source disk.	Check the storage device or system in the source server.
17014	Error	Replication failed due to local disk error.	Replication encountered a disk I/O error from the source disk.	Check the storage device or system in the source server.
17015	Error	Replication failed because local snapshot used up all of the reserved area.	Replication failed because the snapshot from the source drive could not be maintained due to low snapshot resources.	Expand the snapshot resource for the source device.

Number	Type	Text	Probable Cause	Suggested Action
17016	Error	Replication failed because the replica snapshot used up all of the reserved area.	Replication failed because the snapshot from the replica drive could not be maintained due to low snapshot resource space.	Expand the snapshot resource for the replica device.
19004	Warning	Allocate space at MB has reached the threshold of the total capacity.	Storage utilization has reached the limit specified by the user.	Check storage utilization and delete unused virtual tapes to free up space or add more storage.
19057	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- unable to connect to remote server.	Replication configured using remote copy failed due to network problem.	See 1067.
19065	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- virtual tape is in the drive.	The virtual tape was moved to the tape drive when the remote copy processing started.	Remove the replication setup configured through remote copy. Reconfigure remote copy when the virtual tape is moved to the vault or slot.
19073	Error	[Remote Copy] The copying of the virtual tape to the remote server cannot proceed -- the remote server %1 is busy.	The target server is busy and the source server cannot get the target server transaction lock. The remote copy cannot proceed.	Remove the tape's remote copy configuration; try the remote copy job at a later time.
19074	Error	Replication cannot proceed -- the replica server %1 is busy.	The target server is busy and the source server cannot get the target server transaction lock. Replication cannot proceed.	Set a replication retry count and retry interval so that replication will retry if there is a failure.
19077	Error	[Remote Copy] Copying of the virtual tape to the remote server cannot proceed -- the remote server %1 does not enough space.	The target VTL server does not have enough space.	Add additional storage on the VTL target server.
19078	Error	Replication cannot proceed -- the remote server %1 does not have enough space.	The target VTL server does not have enough space.	Add additional storage on the VTL target server.

Number	Type	Text	Probable Cause	Suggested Action
19202	Error	Console (User Name): Failed to create key KEYNAME	The key name already exists. Another user using a different console may have created a key with the same name.	Retry the operation.
19204	Error	Console (User Name): Failed to delete Key KEYNAME	The key may have been deleted or renamed by somebody else in a different console.	Retry the operation. The console will be automatically updated if another user had deleted the key from another console.
19206	Error	Console (User Name): Failed to update information for key KEYNAME	The key name may have been deleted or changed or the new key name may already exist.	Retry the operation. The console will be automatically updated if another user had deleted/created the key from another console.
19208	Error	Console (User Name): Failed to create key package PACKAGENAME.	The keys to be exported may be modified or deleted.	Retry the operation.
19210	Error	Console (User Name): Failed to get key package information.	The key package format/ content may be invalid.	Recreate the key package.
40002	Error	Block list full on tape.	Too many very small sized blocks (< 512 bytes) have been written to tape.	Increase the block size used by the backup application.
40009	Error	Error with Move Medium command, Lib VID##, SrcEle ### DestEle ###	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40010	Error	Attach to tape failed.	A physical device is not available.	Check storage device connectivity and make sure that the software can access the devices.
40011	Error	Failed to read from Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40013	Error	Export Tape failed, not enough memory.	The system is running low on memory. This may be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory on the system may also resolve the problem.

Number	Type	Text	Probable Cause	Suggested Action
40014	Error	Read tape info failed.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40015	Error	Export tape failed, unsupported block size.	The backup application has used an unsupported block size on the virtual tape. 1 MB is currently the maximum block size supported.	Change the backup application configuration to use a smaller block size.
40017	Error	Failed to write to Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40018	Error	Failed to load Physical Tape.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40019	Error	Failed to write to Virtual Tape.	The storage LUN where the virtual tape is stored cannot be accessed.	Check the storage LUN where the virtual tape is located.
40022	Error	Failed to get Physical Tape block size.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40023	Error	Import failed, not enough memory.	The system is running low on memory. This may be because too many concurrent operations are in process.	If too many operations are in progress, wait till some operations are completed. Increasing the physical memory on the system may also resolve the problem.
40032	Warning	Physical Tape not available to start export job in lib.	There is an import/export job in the queue waiting for a physical tape.	Insert tapes with appropriate barcodes in the physical library and perform an inventory operation.
40039	Error	Read Element command to Physical Library failed.	There is a hardware problem with the physical tape library.	Check with the tape library vendor.
40043	Error	Move Medium command failed in Physical Library.	There is a hardware problem with the physical tape library.	Check with the tape library vendor.
40044	Error	Unload command failed on Physical Tape Drive.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40045	Error	Read from Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40046	Error	Write to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.

Number	Type	Text	Probable Cause	Suggested Action
40047	Error	Write File Mark to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40048	Error	Mode sense command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40049	Error	Mode select command to physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40050	Error	Rewind command to Physical Tape Drive failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40051	Error	Inquiry command to Physical device failed.	There is a hardware problem with the physical tape drive.	Check with the tape drive vendor.
40065	Error	Read data from Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located.
40066	Error	Write data to Virtual Tape failed.	The storage LUN where the virtual tape is located cannot be accessed.	Check the LUN where the virtual tape is located.
40069	Error	Cannot expand Tape.	There is not enough storage space available to expand a virtual tape.	Add more storage space to the system or free up space by deleting virtual tapes that are no longer required.
40074	Error	Export to Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40076	Error	Import Physical Tape failed.	Check the event log messages prior to this message for the exact reason for the failure.	Check suggested action for the error message prior to this message.
40077	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	COPAN 400 doesn't allow duplicate barcodes in a system. Delete the existing tape or use a different barcode while importing.
40078	Error	Import Physical Tape failed. Duplicate Virtual Tape Barcode.	A virtual tape with the same barcode already exists in the virtual library.	COPAN 400 doesn't allow duplicate barcodes in a system. Delete the existing tape or use a different barcode while importing.

Number	Type	Text	Probable Cause	Suggested Action
40085	Error	Init Element Status command failed on Physical Library, Error.	There is a physical library hardware problem.	Check physical library hardware.
40086	Error	Write command to Configuration Repository Failed. Check repository LUNs.	Storage or storage connectivity problems.	Check storage and storage connectivity.
40090	Error	Failed to load tape because it is a cleaning tape. Lib VID ##, Drive VID ##, BC ###	A cleaning tape was manually moved into a drive from the console or a cleaning tape is being used for import/export jobs.	Check and make sure that cleaning tapes are not used for import/export jobs.
40092	Error	Error in retrieving the hostname of this CDL server.	Cannot get the system's hostname.	Verify that 'uname -a' returns the hostname.
40093	Error	Failure in looking up the IP address of the server (ServerName). Verify that DNS is configured correctly for both ACSLS and COPAN 400 server.	Couldn't find the IP address of the server from DNS or the /etc/hosts file.	If DNS is configured, verify that the DNS server is running and is configured correctly for COPAN 400 and ACSLS. If DNS is not configured, verify that the /etc/hosts file contains the public IP of the appliance.
40096	Error	Failed to open [AAA].	Could not open the ACSLS configuration file.	Verify that the ACSLS configuration file exists at /usr/local/sgi/VTL/etc/acsls_ls_cdk.conf
40097	Error	DNS configuration for COPAN 400 server is incorrect. DNS or /etc/hosts is returning x.x.x.x as the IP of COPAN 400 server ServerName	Couldn't find the IP of the server from DNS nor the /etc/hosts file.	If DNS is configured, verify that the DNS server is running and is configured correctly for COPAN 400 and ACSLS. If DNS is not configured, verify that the /etc/hosts file contains the public IP of the appliance.
40098	Error	Failed to successfully query ACSLS server with IP x.x.x.x Error from ACSLS: EC	Failed to contact the ACSLS server with the entered IP address.	Verify that the IP is valid and that users can ping the ACSLS server from the server.
40099	Error	Waited N seconds to get a response from ACSLS x.x.x.x. Timing out...	Failed to contact the ACSLS server with the entered IP address.	Verify that the IP is valid and that users can ping the ACSLS server from the server.

Number	Type	Text	Probable Cause	Suggested Action
40100	Error	Failed to mount BARCODE on drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS]	Mount operation failed.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the mount failed.
40101	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to mount BARCODE on drive x.x.x.x. Timing out...	Mount operation failed, timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the mount failed.
40102	Error	Failed to dismount BARCODE from drive x.x.x.x. Error from ACSLS x.x.x.x: [Error message from ACSLS server].	Dismount operation failed.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the dismount failed.
40103	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to dismount BARCODE from drive x.x.x.x. Timing out…	Dismount operation failed, timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the dismount failed.
40104	Error	Failed to retrieve drive information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get the drives list from the ACSLS server.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40105	Error	|Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve drive information in ACS ##. Timing out...	Failed to get the drives list from the ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40106	Error	Failed to retrieve volume information in ACS ## and Pool ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get the volume list from the ACSLS server.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.

Number	Type	Text	Probable Cause	Suggested Action
40107	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve volume information in ACS ## and Pool ##. Timing out.	Failed to get the volume list from the ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40108	Error	Failed to retrieve LSM information in ACS ##. Error from ACSLS x.x.x.x: [Error message from ACSLS server]	Failed to get the LSM list from the ACSLS server.	Check the ACSLS manager server's event log to see why the 'display' command failed.
40109	Error	Waited ## seconds to get a response from ACSLS x.x.x.x after trying to retrieve LSM information in ACS ##. Timing out...	Failed to get the LSM list from the ACSLS server. Timing out.	Check the ACSLS manager server's event log ($ACSLSHOME/log/ acsss_event.log) to see why the 'display' command failed.
40191	Error	Hardware compression card failed - EC [%1], complete code [%2], hardware complete code [%3] while accessing tape [%4] VID [%5].	The compression card reported a failure.	Contact the compression card vendor.
40193	Error	ACSLS/LS: Failed to query %1 server with IP %2 and ACS %3 due to wrong ACS ID %4.	The ACS ID specified in the ACSLS configuration is incorrect.	Use the correct ACS ID in the ACSLS configuration.
40194	Error	ACSLS/LS: portmap daemon is required for ACSLS libraries. Start the portmap daemon using "portmap" command and do a rescan on the physical devices.	The portmap daemon is not running.	Check and make sure portmap daemon is running.

Number	Type	Text	Probable Cause	Suggested Action
40197	Warning	Repository consistency check detected non critical inconsistencies. Check syslog for more information.	Possible non-critical information/structure inconsistencies detected in the COPAN 400 database (repository). Integrity of the disk LUN that stores the COPAN 400 database may be compromised.	Check syslog for details of inconsistencies. Check the storage for possible errors/ issues.
40198	Error	Repository consistency check detected critical errors. Check syslog for more information.	Critical information/structure inconsistencies detected in the COPAN 400 database (repository). Integrity of the disk LUN that stores the COPAN 400 database may be compromised.	Check syslog for details of inconsistencies. Check the storage for possible errors/ issues.
40199	Error	Compression data consistency check: Invalid data signature found on tape [%1] VID %2	Data integrity signature in compressed blocks does not match the original signature. Data received from the storage is corrupted.	Check storage for possible corruption and take appropriate actions to correct it.
40200	Error	Write Filemark Table failed. BC [%1], VID %2, EC %3	Write operations on a Filemark Table (part of virtual tape meta data) failed, possibly due to issues with storage.	Check storage and make sure that storage is accessible.
40201	Error	Tape can not be created - Duplicate VID found %1	A tape is being created with a VID that already exists, possibly due to inconsistencies in internal information.	Contact Technical Support.
40202	Warning	TapeProperty: COPAN 400 management did not find the tape [%1], VID=%2	This is possibly due to inconsistencies in internal information.	Contact Technical Support.
40203	Warning	TapeProperty: Found tape maximum capacity mismatch on tape [%1], VID=%2 - Mark the tape as READ ONLY	A mismatch in the maximum capacity of a tape was detected by consistency checks.	Contact Technical Support.
40204	Warning	TapeProperty: Found tape allocated size mismatch on tape [%1], VID=%2 - Mark the tape as READ ONLY	A mismatch in allocation size of a tape was detected by consistency checks.	Contact Technical Support.

Number	Type	Text	Probable Cause	Suggested Action
40205	Warning	TapeProperty: Found stub tape property mismatch on tape [%1], VID=%2, stubtape=%3 - Mark the tape as READ ONLY	A mismatch in stub tape property was detected by consistency checks	Contact Technical Support.
40206	Warning	TapePropertyCheckUpCall: Found tape capacity on demand property mismatch on tape [%1], VID=%2, COD=%3	A mismatch in COD property was detected by consistency checks.	Contact Technical Support.
40213	Error	Data block size %1 on tape [%2] VID %3 can not be decompressed through hardware compression driver - error %4	The compression card reported a failure.	Contact the compression card vendor.
40215	Error	Export Job %1 - The current physical tape position %2 mismatch with the number of blocks %3 transferred to the physical tape [%4] in physical tape drive VID [%5]. The start position on the physical tape is %6, the expected current position on the physical tape should be %7	The current physical tape position got changed by a third-party application during a tape export job.	Make sure physical drives are not shared with other applications.

For any error not listed in this table, Contact SGI Technical Support.

Appendix

This appendix contains information about ports used by COPAN 400 and LUN migration.

Port usage

COPAN 400 servers use the ports listed in the following tables for incoming requests. 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 ports are not used unless the associated option is enabled in COPAN 400. For SGI appliances, the ports marked ● are enabled by default.

Protocol	Port	Usage
TCP	20	Standard FTP data port
UDP	20	Standard FTP data port
TCP	21	Standard FTP port
UDP	21	Standard FTP port
TCP	22 ●	Standard Secure Shell (SSH) port for remote connection to the server
TCP	23	Standard Telnet port for remote connection to the server
UDP	23	Standard Telnet port for remote connection to the server
TCP	25	Standard SMTP port for Email Alerts
UDP	25	Standard SMTP port for Email Alerts
HTTP	80 ●	Standard HTTP port to access SGI Web Setup and also used for online registration of license key codes. Note: Port 80 is used to send license material to the SGI license server for registration. The registration reply is then sent back using HTTP protocol, where a local random port number is used on the server in the same way as Web-based pages. The firewall does not block the reply if the 'established bit' is set to let established traffic in.
HTTP	81 ●	Standard HTTP port to access SGI Management Console via Web Start
TCP	111	PortMapper for ACSLS*

Protocol	Port	Usage
UDP	111	PortMapper for ACSLS*
UDP	123	Standard Network Time Protocol (NTP) transport layer to access external time servers
UDP	161	SNMP port for SNMP queries
HTTPS	443 ●	Standard secure HTTP port to access SGI Web Setup
UDP	623 ●	Failover IPMI power control port
HTTPS	1311	Management port for DELL servers for hardware configuration
TCP	3260	Communication port between iSCSI clients and the server
TCP	5001	isttcp port to test network connection
TCP	8009	Standard Apache AJP port to access SGI Web Setup
NDMP	10000	Communication port between Symantec NetBackup and COPAN 400 for NDMP backup/restore
TCP	11576 ●	Secure RPC communication port between SGI Management Console and the server
TCP	11577 ●	Communication port between servers for data replication
UDP	11577 ●	Communication port between servers for data replication
TCP	11578 ●	Communication port between replication servers for 56-bit authentication
UDP	11578 ●	Communication port between replication servers for 56-bit authentication
TCP	11579 ●	Communication port between replication servers for 128-bit authentication
UDP	11579 ●	Communication port between replication servers for 128-bit authentication
TCP	11580 ●	Communication port between failover pair
TCP	11582 ●	Communication port for Command Line Interface (CLI)

* 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 COPAN 400 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

COPAN 400 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 COPAN 400 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
```

Index