VERITAS NetBackup™ ServerFree Agent 4.5

System Administrator's Guide

for UNIX

March 2002
30-000510-011

VERITAS

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000
Fax 650-527-8050
www.veritas.com

Contents

About This Guide

This guide explains how to install, configure, and use VERITAS NetBackup ServerFree Agent.

Audience

This guide is intended for the NetBackup system administrator and assumes a thorough working knowledge of both UNIX and NetBackup administration.

Organization

- The “Introduction” is an overview of the product’s capabilities, with background information on frozen images and offhost backup.
- “Configuration Checklist” reviews the basic steps for configuring ServerFree Agent.
- “Installation” explains how to install and de-install NetBackup ServerFree Agent.
- “SAN Configuration for ServerFree Agent” provides assistance in setting up the hardware.
- “NetBackup Configuration” explains how to configure NetBackup policies / clients for frozen images and offhost backup.
- “Core Frozen Image Services” provides additional information about the nbu_snap, fsclone, and vxvm frozen image methods.
- “Extended Frozen Image Services (Array Integration Option)” provides basic configuration guidance and vendor-specific details for using the TimeFinder, ShadowImage, and BusinessCopy frozen image methods with disk arrays.
- “Notes on Offhost Backup” provides notes and restrictions on offhost (server-free) backup.
- “Using NetBackup” briefly explains how to back up and restore files.
- “Troubleshooting” helps in resolving problems when using NetBackup ServerFree Agent. See also the *NetBackup Troubleshooting Guide for UNIX*.

- "ServerFree Agent Commands" provides information about several commands.

Related Manuals

- *NetBackup Release Notes for UNIX and Windows*

  Describes supported platforms and provides operating notes not found in the manuals or in the online help.

- *NetBackup DataCenter Installation Guide for UNIX*

  Explains how to install NetBackup DataCenter for UNIX.

- *NetBackup for Oracle Advanced ServerFree Agent System Administrator's Guide for Solaris and HP*

  Explains how to install, configure, and use NetBackup for Oracle ServerFree Agent to back up and restore Oracle databases that are on a UNIX NetBackup client.

  For this NetBackup Oracle product, you may also need the following manuals from Oracle Corporation:

  Oracle Enterprise Manager Administrator's Guide

  Oracle8i Backup and Recovery Guide

  Oracle8i Server Administrator's Guide

  Oracle8i Recovery Manager User's Guide and Reference

- *NetBackup DataCenter System Administrator's Guide for UNIX*

  Explains how to configure and manage NetBackup DataCenter on a UNIX platform.

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*

  Explains how to configure and manage the storage devices and media that UNIX NetBackup servers use for backups.

- *NetBackup Media Manager Device Configuration Guide*

  Provides information about configuring storage devices on UNIX systems.

- *NetBackup Troubleshooting Guide for UNIX*

  Explains NetBackup ServerFree Agent error codes.

- *NetBackup User's Guide for UNIX*

  Explains how to perform user-directed backups, restores, and archives on a UNIX NetBackup client.

Accessibility

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the NetBackup system administrator's guide.

Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: *Do not* ignore cautions.
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the **Password** field.

Notes and Cautions

Note This is a Note. Notes are used to call attention to information that makes using the product easier or helps in avoiding problems.

Caution This is a Caution. Cautions are used to warn about situations that could cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, holding down the **Ctrl** key while pressing another key. Keyboard command sequences are indicated by connecting the keys with a plus sign. For example:

Press Ctrl+t

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

`command` *arg1*|*arg2*

the user can use either the *arg1* or *arg2* variable.

Terms

The terms listed in the table below are used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

Term	Definition
Microsoft Windows, Windows	Terms used as nouns to describe a line of operating systems developed by Microsoft, Inc. A term used as an adjective to describe a specific product or noun. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI. Where a specific Windows product is identified, then only that particular product is valid with regards to the instance in which it is being used. For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.
Windows servers	A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and Windows 2000.
Windows clients	A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

`http://www.support.veritas.com/`

VERITAS Customer Support has an extensive technical support structure that enables you to contact technical support teams that are trained to answer questions to specific products. You can contact Customer Support by sending an e-mail to support@veritas.com, or by finding a product-specific phone number from the VERITAS support web site. The following steps describe how to locate the proper phone number.

1. Open `http://www.support.veritas.com/` in your web browser.
2. Click **Contact Support**. The *Contacting Support Product List* page appears.
3. Select a product line and then a product from the lists that appear. The page will refresh with a list of technical support phone numbers that are specific to the product you just selected.

ServerFree Agent Information on the Web

The VERITAS support web site includes a variety of articles and notes on ServerFree Agent. These provide up-to-date lists of supported operating systems, peripherals, and assistance for some of the configuration procedures found in this manual. To locate this information, do the following:

1. Go to `www.support.veritas.com` on the web.
2. In the left margin, click **Patches and Updates**.
3. Select **NetBackup Products** from the Product List. Then select **NetBackup DataCenter**.
4. In the filter wizard, enter the following:
   - **Keyword**: ServerFree
   - **File type**: PDF (or ALL)
   - **Language**: English
   - **Version**: 4.5
   - **Platform**: All
5. Click **Find Files**.

   The files relating to NetBackup ServerFree Agent 4.5 will be listed along with their descriptions. Do the following to download a file:

   a. Click on the file-name link for more information about the file.

   b. Right-click on the file's download link to download and save the file.

Introduction 1

This chapter describes NetBackup ServerFree Agent and contains the following topics.

- Overview
- Terminology
- Features
- Requirements
- Restrictions
- Frozen Image Overview
- Local Backup of Frozen Image (Local Host)
- Offhost Backup Overview
- Tables of Features and Required Software

Overview

NetBackup ServerFree Agent provides data protection services for frozen image data, and supports offhost backup over Fibre Channel networks (in addition to conventional backups to locally attached devices).

Frozen Image Services

A frozen image is a stable disk copy of the client's data made prior to backup. Such a copy is important on active file systems and Oracle databases, where updates to files or tables can occur at any time. In such cases, making a stable, consistent copy (frozen image) is a prerequisite to making a correct backup.

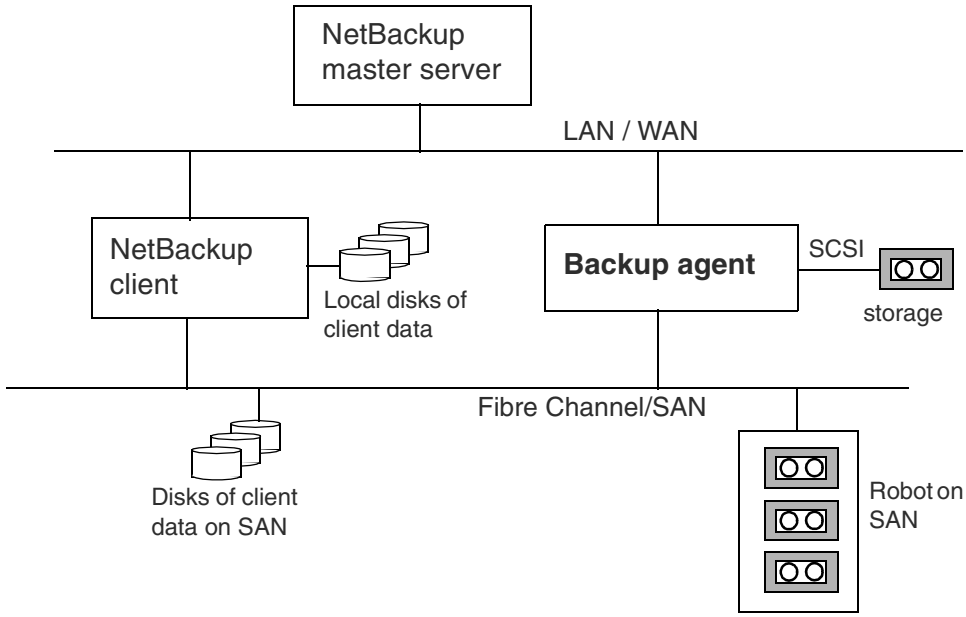
NetBackup supports two different product sets for creating frozen images: Core Frozen Image Services, and Extended Frozen Image Services (also known as the Array Integration option). Refer to "Frozen Image Services" on page 8 for further description of these products, and to "Frozen Image Overview" on page 12 for background on frozen image technology.

Offhost Backups

The other major component of NetBackup 4.5 ServerFree Agent is support for offhost backup. Offhost backup shifts the burden of backup processing onto a separate *backup agent* (NetBackup media server or third-party copy device), greatly reducing the impact on the client's computing resources ordinarily caused by a local backup. A backup agent executing on a separate host reads the data from the client disk and writes it to storage.

See the following network diagram showing a backup agent.

Backup Agent for Offhost Backup



The backup agent can be either a NetBackup media server or a third-party copy device that implements the SCSI Extended Copy command. Note that many types of devices are designed to act as backup agents, such as routers, bridges, robotic libraries, and disk arrays. The backup agent can direct the data to SCSI-attached storage or to storage on the SAN.

Terminology

This section introduces terms used with NetBackup 4.5 ServerFree Agent.

Backup agent (see also Third-Party Copy Device)

A general term for the host that manages the backup on behalf of the NetBackup client. In NetBackup 4.5, this is either the NetBackup media server or a third-party copy device.

BCV

The mirror disk in an EMC primary-mirror array configuration (see *mirror*). BCV stands for "Business Continuance Volume."

Bridge

In a SAN network, a *bridge* connects SCSI devices to Fibre Channel. A *third-party copy device* can be implemented as part of a bridge or as part of other devices. Note that not all bridges function as third-party copy devices.

BusinessCopy

One of three frozen image methods included in the Extended Frozen Image Services (Array Integration) option. BusinessCopy is for making frozen images of client data on HP disk arrays.

Copy manager (see Third-Party Copy Device)

Data movement

A copy operation as performed by a third-party copy device or NetBackup media server.

Disk group

A configuration of disks to create a primary-mirror association, using commands unique to the disks' vendor. See *mirror* and *volume group*.

Extent

A contiguous set of disk blocks allocated for a file and represented by three values: device identifier, starting block address (offset in the device) and length (number of contiguous blocks). The *mapping methods* in ServerFree Agent determine the list of extents and send the list to the backup agent.

Fibre channel

A type of high-speed network composed of either optical or copper cable and employing the Fibre Channel protocol. NetBackup 4.5 ServerFree Agent supports both arbitrated loop and switched fabric (switched fibre channel) environments.

File list

The list of files to be backed up for a NetBackup policy. For ServerFree Agent, the files in a file list must be part of a file system or raw device that was designated as a frozen image source.

File system

Has two different meanings.

- When referring to a product, such as the ufs (Sun Solaris) or VxFS (VERITAS) *file system*, it refers to the management and allocation schemes on which the entire file tree is structured.
- When referring to a particular component in a file tree, *file system* means a directory (with any subdirectories and files) that is attached to the UNIX file tree by means of the `mount` command. When a file system is selected as either a frozen image source or as an entry in the NetBackup file list, this definition applies.

Frozen image

A stable disk copy of the data prior to backup. A *frozen image* is created very rapidly, causing minimal impact on other applications. There are two basic types: *copy-on-write snapshot* and *mirror*.

Frozen image method

A set of routines for creating a frozen image.

Frozen image source

This designates the entity (file system, raw partition, or logical volume) to which a frozen image method is applied. Note that the frozen image source does not identify the files to be backed up (see *file list*).

Mapping

The process of converting a file or raw device (in the file system or Volume Manager) to absolute physical disk addresses or extents for use by backup agents on the network. NetBackup ServerFree Agent uses the *VxMS* library to perform file mapping.

Mapping methods

A set of routines for converting logical file addresses to absolute physical disk addresses or extents. NetBackup ServerFree Agent includes support for file-mapping and volume-mapping methods.

Mirror

- A disk that maintains an exact copy or duplicate of another disk. A mirror disk is often called a *secondary*, and the disk that it copies is called the *primary*. All writes to the primary disk are also made to the *mirror* (or secondary) disk.

- A type of frozen image made on a mirror disk (see also *snapshot*). At an appropriate moment, all further writes to the primary disk are held back from the mirror, thus causing the mirror to be “split” from the primary. As a result of the split, the mirror becomes a “frozen” image of the primary. The frozen image can then be backed up.

NetBackup Media Server (offhost backup method)

One of two offhost backup methods provided by NetBackup ServerFree Agent, in which data movement is performed by a NetBackup media server.

Offhost backup

The off-loading of backup processing to a separate backup agent executing on another host. NetBackup ServerFree Agent contains two offhost backup options: NetBackup Media Server and Third-Party Copy Device.

Primary disk

In a primary-mirror array configuration, the primary is the disk on which client data is stored, and which is directly accessed by client applications. An exact duplicate of the primary disk is the mirror (see *mirror*).

Raw partition

A single section of a raw physical disk device occupying a range of disk sectors, without a file system or other hierarchical organization scheme (thus, a “raw” stream of disk sectors). This is different from a block device, over which the file system is mounted.

SAN (Storage Area Network)

A Fibre Channel-based network connecting servers and storage devices. The storage devices are not attached to servers but to the network itself, and are visible to all servers on the network.

Secondary disk

See *mirror.*

ShadowImage

One of three frozen image methods included in the Extended Frozen Image Services (Array Integration) option. ShadowImage is for making frozen images of client data on Hitachi disk arrays.

Snapshot (copy-on-write)

In NetBackup ServerFree Agent, one of two types of supported frozen images (see also *mirror*). Unlike a mirror, a copy-on-write snapshot does not create a separate copy of the primary data (frozen image source). It creates a block-by-block “account” that describes which blocks in the frozen image source have changed and which have not, from the instant the snapshot was activated. This account is used by the backup application to create the backup copy.

Snapshot mirror

An exact copy of a primary volume at a particular moment, reproduced on a physically separate device. Snapshot mirrors are created by the VERITAS Volume Manager (VxVM).

Standard device

Refers to the primary disk in an EMC primary-mirror disk array (see *primary disk*).

Third-Party Copy Device

This term has two meanings:

- A backup agent on the SAN that operates on behalf of backup applications. The *third-party copy device* receives backup data from a disk attached to Fibre Channel and sends it to a storage device, using the SCSI Extended Copy command. The third-party copy device is sometimes called a copy manager, third-party copy engine, or data mover. In SAN hardware configurations, a third-party copy device can be implemented as part of a bridge, router, or storage device. The third-party copy device may or may not be the device to which the storage units are connected.
- An offhost backup method in NetBackup ServerFree Agent that allows backups to be made by means of a backup agent on the SAN.

TimeFinder

One of three frozen image methods included in the Extended Frozen Image Services (Array Integration) option. TimeFinder is for making frozen images of client data on EMC Symmetrix disk arrays.

ufs file system

This is the UNIX File System (ufs), which is the default file system type on Sun Solaris. The ufs file system was formerly the Berkeley Fast File System.

VxMS (VERITAS Federated Mapping Services)

A library of routines (methods) used by NetBackup ServerFree Agent to obtain the physical addresses of logical disk objects such as files and volumes.

Volume

A virtual device configured over raw physical disk devices (not to be confused with a NetBackup *Media Manager* volume). Consists of a block and character device.

If a frozen image source exists over a volume, NetBackup 4.5 automatically uses a volume *mapping* method to map the volume to physical device addresses. Any of the ServerFree Agent *frozen image methods* can be used when backing up client data configured over volumes.

For NetBackup 4.5, volumes must be created by means of the VERITAS Volume Manager (VxVM).

Volume group

A logical grouping of disks, created with the VERITAS Volume Manager, to allow more efficient use of disk space.

VxFS

This is the VERITAS extent-based File System (VxFS), designed for high performance and large volumes of data.

VxVM

This is the VERITAS Volume Manager (VxVM), which provides logical volume management that can be used in SAN environments.

Features

NetBackup 4.5 ServerFree Agent provides the following services and features.

General capabilities

- Supports heterogeneous server-client environments (HP and Solaris): the media server and client need not be installed on the same platform.
- Backs up the following file systems: ufs (Solaris), VxFS (Solaris and HP-UX), and Online JFS (HP-UX).
- Backs up VxVM volumes on both Solaris and HP-UX.
- Supports NetBackup **Standard**, **FlashBackup**, and **Oracle** policy types.
- Supports multiple data streams.

Frozen Image Services

Core Frozen Image Services and Extended Frozen Image Services (also known as the Array Integration option) each contain three methods for making frozen images:

The Core Frozen Image Services

- **nbu_snap** (Solaris only), for copy-on-write snapshot frozen images of client data.
- **fsclone** (Solaris only), for copy-on-write snapshot frozen images of client data, using VERITAS File System 3.4 clones.

Note VERITAS File System 3.4 is included in the Database Edition for Oracle 2.2.

- **vxvm** (Solaris and HP-UX), for frozen images of client data configured over VERITAS Volume Manager volumes, using VERITAS Volume Manager 3.1 or later snapshot mirrors.

Extended Frozen Image Services (Array Integration Option)

- **TimeFinder** (Solaris and HP-UX), for frozen images with EMC Symmetrix Disk Arrays (with TimeFinder SYMAPI).
- **ShadowImage** (Solaris and HP-UX), for frozen images with Hitachi Data Systems disk arrays with ShadowImage (HOMRCF).
- **BusinessCopy** (Solaris and HP-UX), for frozen images with Hewlett Packard XP series disk arrays with BusinessCopy Services.

Offhost Backup

NetBackup ServerFree Agent provides two offhost backup services: *NetBackup Media Server* and *Third-Party Copy Device*. Both of these services eliminate backup overhead on the application host (NetBackup client), by off-loading backup processing to a NetBackup media server or third-party copy device on the network.

- **NetBackup Media Server**: the backup is performed by a NetBackup media server.
- **Third-Party Copy Device**: the backup is performed by an independent backup agent that uses the Extended Copy command. For a list of supported third-party copy devices and other peripherals, refer to “ServerFree Agent Information on the Web” on page xiv, or to the *NetBackup 4.5 Release Notes*.

Requirements

NetBackup 4.5 ServerFree Agent requires the following components:

- A master server with NetBackup ServerFree Agent server software installed.
- Clients running either Solaris 2.6, 7, 8, or 9, or HP-UX 11.00 or 11i, with NetBackup ServerFree Agent client software installed.

Note Certain operating system and device patches (such as for the host bus adapter) may be required for both servers and clients. To obtain the latest information, refer to "ServerFree Agent Information on the Web" on page xiv.

Please note the following additional requirements:

- To use the **fsclone** frozen image method, all clients must have the Database Edition for Oracle 2.2 or later installed with valid licenses, including support for VxFS 3.4.
- To use the **vxvm** frozen image method, all clients must have VxVM 3.1 or later.
- For the **TimeFinder**, **ShadowImage**, or **BusinessCopy** frozen image methods, assistance may be required from the disk array vendor. Refer to the chapter titled "Extended Frozen Image Services (Array Integration Option)."
- To use the frozen image and offhost backup features of NetBackup ServerFree Agent with a NetBackup Oracle policy, UNIX clients must have Oracle8i installed.
- To use the frozen image and offhost backup feature of NetBackup ServerFree Agent for HP clients, the HP client must be using the Online JFS file system, not the default JFS.

Restrictions

For a complete list of supported peripherals, and for other operational notes, refer to the *NetBackup 4.5 Release Notes,* or to "ServerFree Agent Information on the Web" on page xiv.

Please note the following restrictions:

- If you are using offhost backup (**NetBackup Media Server** or **Third-Party Copy Device**), the disk containing the client's data (the files to back up) must be either a SCSI or Fibre Channel device.
- For offhost backup using the Core Frozen Image Services option (nbu_snap, fsclone, or vxvm), the NetBackup media server must be able to access all the disks that make up the frozen image. The disk(s) can be connected to a SAN. For each of these frozen image methods, note the following:
  - **nbu_snap**: media server requires access to the active disk and the cache disk.

  - **fsclone**: media server requires access to the primary or active disk.
  - **vxvm**: access requirements depend on layout of the volume group. Media server must be able to access all disks that make up the snap mirror volume.

- If you are using the Extended Frozen Image Services (Array Integration) option, the NetBackup clients must be able to access the mirror (secondary) disk containing the frozen image of the client's data. The NetBackup clients must also be able to access the primary disk. The NetBackup media server only needs access to the mirror (secondary) disk.
- If you are using the Extended Frozen Image Services option, a Volume Manager disk group must consist of disks that are all made by the same vendor.
- To be used for offhost backup, the disk must be able to return its SCSI serial number in response to a serial-number inquiry (serialization), or the disk must support SCSI Inquiry Page Code 83.
- Multiplexing is not supported for **Third-Party Copy Device** offhost backups.
- Inline Tape Copies (called Multiple Copies in Vault) is not supported for **Third-Party Copy Device** offhost backups.
- On Windows, the NetBackup Administration Console and the Remote Administration Console are not supported for configuring ServerFree Agent features or for running backups that were configured with ServerFree Agent.

Frozen Image Overview

Large active databases or file systems that must be available around-the-clock are difficult to back up without incurring a penalty. Often, the penalty takes one of two forms:

- The entire database is taken offline or the file system is unmounted, to allow time for the backup, resulting in suspension of service and inconvenience to users.
- The copy is made very quickly but produces an incomplete version of the data, some transactions having failed to complete.

A solution to this problem is to create a *frozen image* of the data. This means "capturing" the data at a particular instant and making a copy of it, without causing significant downtime. The resulting copy or *image* can then be backed up without affecting the performance or availability of the file system or database application data. Without a complete, up-to-date image of the data, a correct backup cannot be obtained.

When a backup is managed by a backup agent on a Fibre Channel network, the data to back up must be contained in a frozen image. The backup agent can only access the data by means of the raw physical disk. Once the data is captured as a frozen image, the NetBackup client "maps" the logical representation of the data to its absolute physical disk address. These disk addresses are sent to the backup agent over the LAN and the data is then read from the appropriate disk by the backup agent. (This process is explained in greater detail under "Offhost Backup Overview" later in this chapter.)

Two types of frozen image methods are available, both supported by NetBackup:

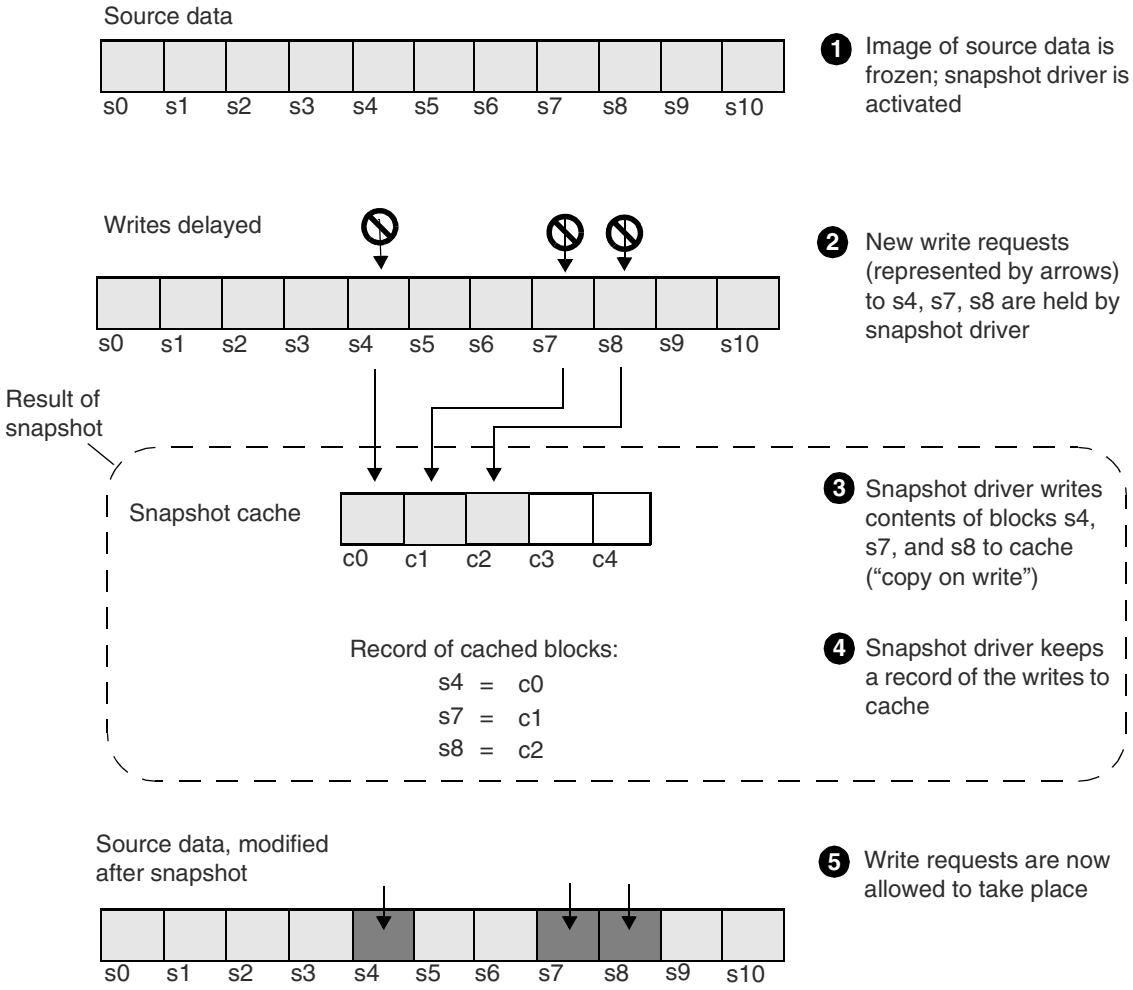
- copy-on-write snapshots
- mirrors

Copy-on-Write Snapshot

A copy-on-write snapshot is a detailed account of data as it existed at a certain moment. Unlike a mirror, explained in the next section, a copy-on-write snapshot is not really a *copy* of the data, but a particular "record" of it.

The copy-on-write snapshot process works as follows: when a frozen image is required, any unfinished transactions or changes to the source data are allowed to complete, but new changes are temporarily stalled. The source is momentarily idled (made quiescent), and a *snapshot driver* is injected into the host operating system. Once the snapshot driver is activated, new transactions or changes (writes) to the source data are allowed to take place. However, the snapshot driver briefly intercepts or holds the write requests. While holding those requests, it copies to cache any blocks that will be affected by those writes, and keeps a record of the cached blocks. In other words, it reads each source block that is about to change, copies the block's current data to cache, and records the location and identity of the cached blocks. Then the intercepted writes are allowed to take place in the source blocks. (See figure "Copy-on-write snapshot process" on page 14.)

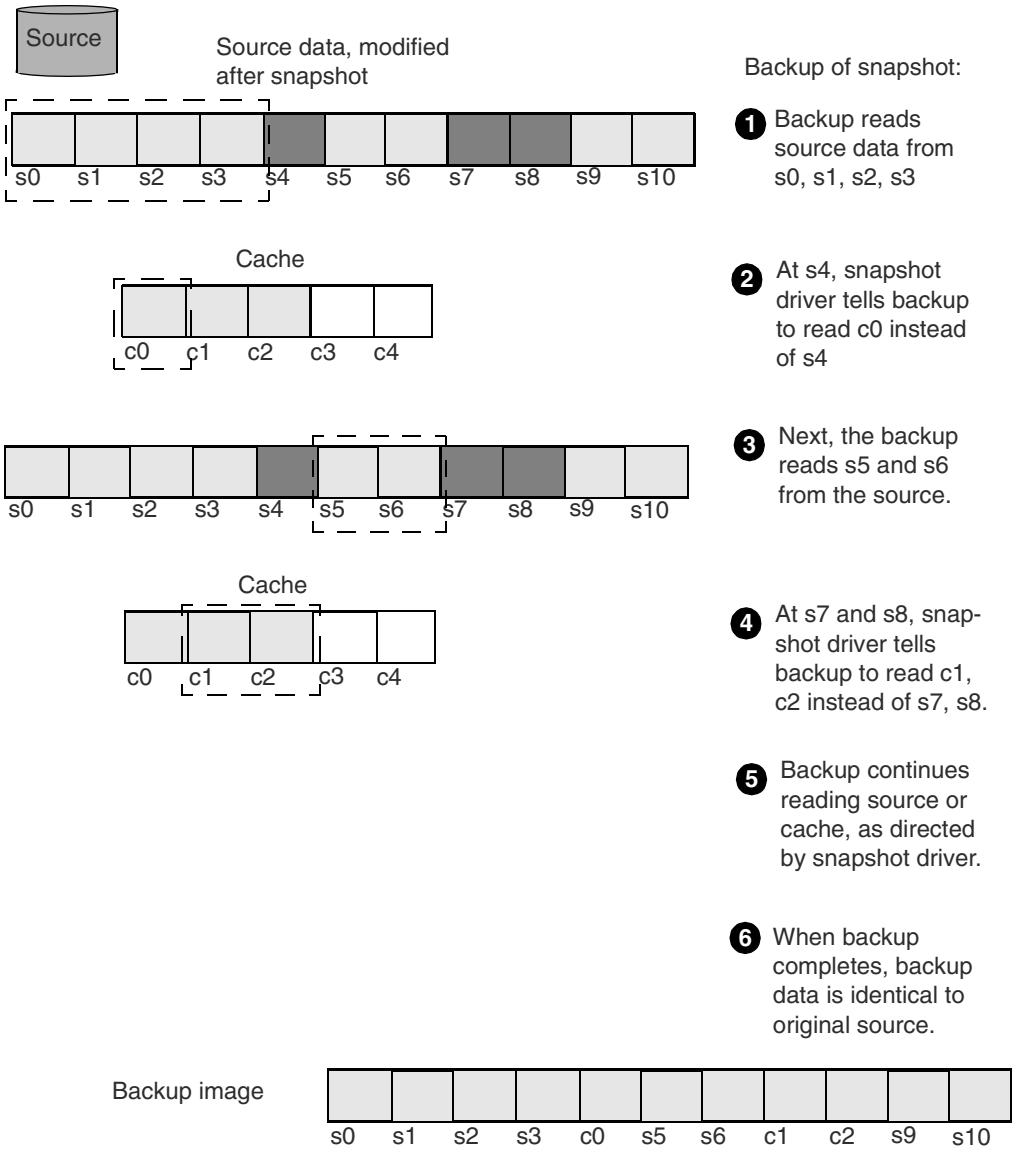
Copy-on-write snapshot process



The immediate results of the snapshot are the following: a cached copy of those portions of the source that were about to change at a certain moment (see step 3 above), and a record of where those cached portions (blocks) are stored (4).

The copy-on-write snapshot does not produce a copy of the source; it creates cached copies of the blocks that have changed and a record of their location. The backup process refers to the source data or cached copy of the data as directed by the snapshot driver (see figure "Backing up a snapshot-type frozen image" on page 15).

Backing up a snapshot-type frozen image



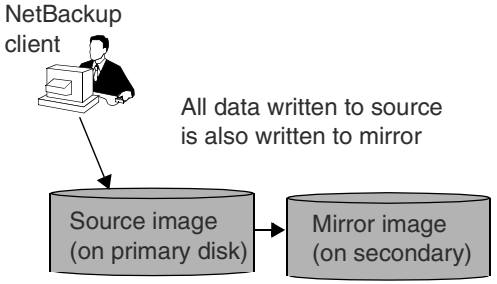
As shown in "Backing up a snapshot-type frozen image," an accurate backup image is obtained by combining the unchanged portions of the data with the snapshot cache. When a backup of the snapshot frozen image begins, the backup application copies the source data ❶ until it comes to a block that changed after the snapshot driver was activated. The snapshot driver tells the backup process to skip that changed block and read in its place the cached (original) copy ❷. The backup application continues copying

source data ❸ until it comes to another changed block. Cache is read again ❹ as the snapshot driver dictates. The backup, when finished, is an exact copy of the source as it existed the moment the snapshot driver was activated.

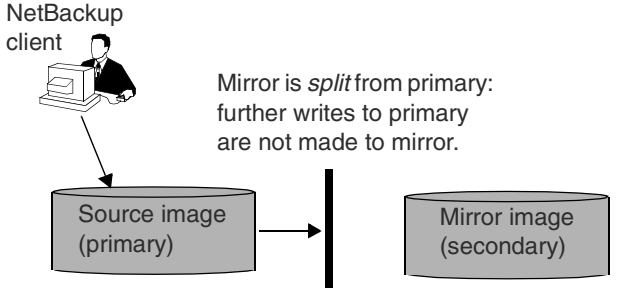
In NetBackup ServerFree Agent, the `nbu_snap` and `fsclone` frozen image methods provide support for copy-on-write snapshot frozen images. These are included in the Core Frozen Image Services option.

Mirror

Unlike a copy-on-write snapshot, a *mirror* is a complete data copy stored on a separate disk, physically independent of the source. Every change or write to the source data on the primary disk is also made to the copy on the secondary disk. This creates a "mirror" image of the source data.



As in a copy-on-write snapshot when a frozen image is required, transactions are allowed to finish and new I/O on the primary disk is briefly halted. When the mirror image is brought up-to-date with the source (made identical to it), the mirror is *split* from the primary, meaning that new changes can be made to the primary but not to the mirror. At this point the mirror can be backed up (see next diagram).



Since mirroring requires an exact, complete copy of the primary on a separate device (equal in size to the disk being mirrored), it consumes more disk space than a copy-on-write snapshot.

In NetBackup ServerFree Agent, the following frozen image methods support mirror frozen images:

- **vxvm** (part of the Core Frozen Image Services option)
- **TimeFinder** (for EMC disk arrays; part of the Extended Frozen Image Services option)
- **ShadowImage** (for Hitachi disk arrays; part of the Extended Frozen Image Services option)
- **BusinessCopy** (for HP disk arrays; part of the Extended Frozen Image Services option)

For basic configuration instructions, and details on vxvm, refer to the "NetBackup Configuration" chapter. For details on TimeFinder, ShadowImage, and BusinessCopy, refer to the chapter titled "Extended Frozen Image Services (Array Integration Option)."

Snapshot vs. Mirror: Which to Choose?

Benefits of copy-on-write snapshot:

- Consumes less disk space: no need for secondary disks containing complete copies of source data.
- Easier to configure.

Note If cost of the additional disk drives needed for mirroring is prohibitive, choose a copy-on-write snapshot frozen image method (**nbu_snap** or **fsclone**). See usage considerations under "Configuration Tips" in the chapter titled "NetBackup Configuration."

Benefits of mirror:

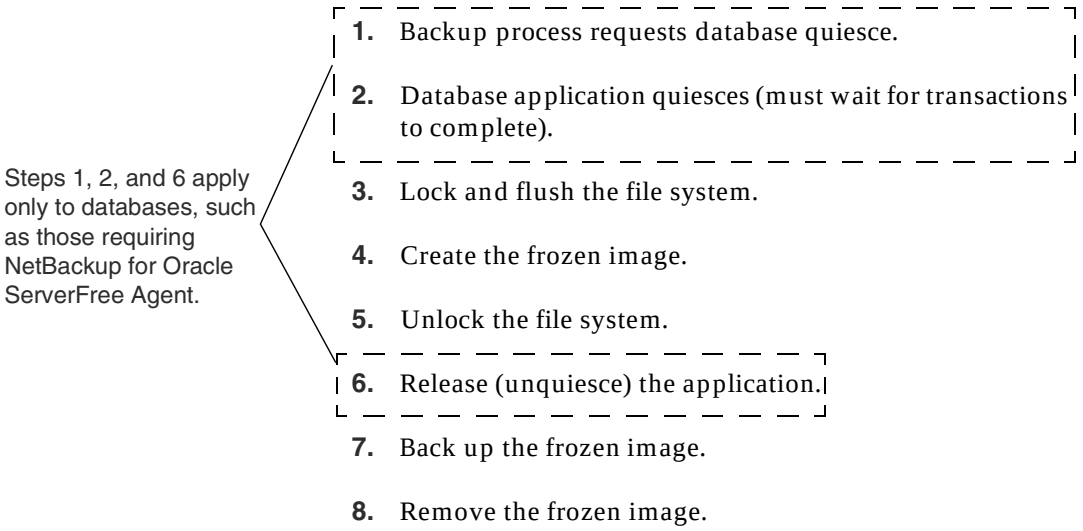
- Has less impact on the performance of the application or database host being backed up (NetBackup client), because there is no need to run the copy-on-write mechanism.
- Allows faster backups: the backup process reads data from a separate disk (mirror) operating independently of the primary disk that holds the client's source data. This means that, unlike the copy-on-write snapshot, there is no need to share disk I/O with other processes or applications. Apart from NetBackup, no other applications have access to the mirror disk. During a copy-on-write snapshot, the source data can be accessed by other applications as well as by the copy-on-write mechanism, causing disk I/O delays.

Note If additional disk drives are available and virtual volumes have already been configured with the VERITAS Volume Manager 3.1 or later, choose a mirror frozen image method.

Processing Before and After the Frozen Image

NetBackup performs several vital functions prior to creating a frozen image, as outlined below and in the following text. Without this pre-processing, the integrity of the frozen image cannot be guaranteed and the backup data may be of no value.

NetBackup Processing Before and After Creating the Frozen Image



Getting the Dust to Settle: Quiescing the System

Before a useful frozen image can be created, the target data must be transactionally consistent or complete. A transaction is a single data action, such as updating a patient's record in a medical database, or creating a record for a new patient. Such a transaction is composed of multiple I/O requests (search, copy, send, write, and so forth). Until the transaction's I/O requests are complete, the data is inconsistent and may be unsuitable for backup.

Transactions affect all levels of the storage management stack (file system, volume manager, and so forth), generating further transactions as a request is handed off to the next level of the stack. From the viewpoint of the file system, for instance, an I/O request issued by a database application constitutes a transaction and may be split into many disk references, all of which must be complete for the original request to be fulfilled. As a result, the creation of the frozen image must be coordinated with any application or other process that can affect the transactional consistency of the data.

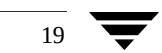
The means of coordination is called *quiesce* (literally, to make quiet or place in repose). This involves pausing the database application or process until the data is transactionally consistent. Applications and the storage management stack must all be quiesced before a useful frozen image can be made.

Quiescing the Database Application

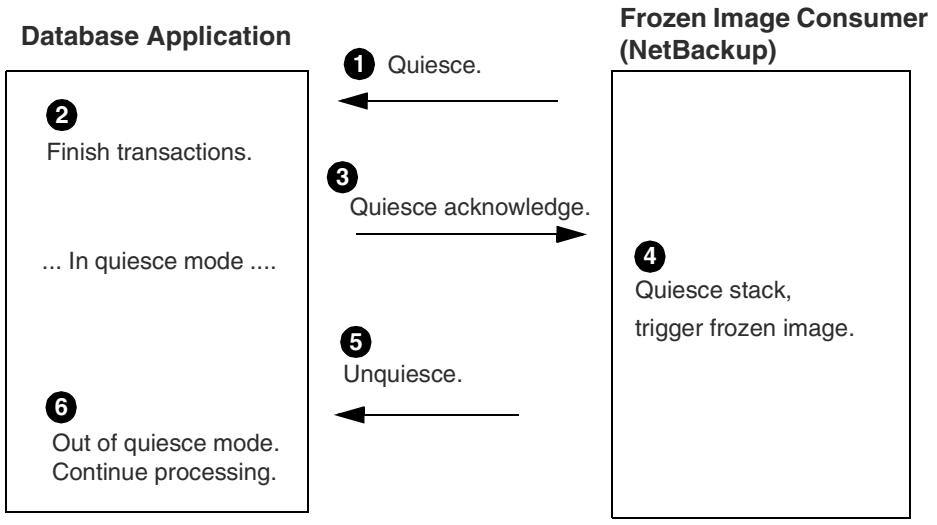
Most database applications are transactionally consistent only at particular points in time. Sometimes, they are consistent only after they have been shut down. Since there is a growing need for database applications to remain up and available constantly, many applications are now designed to reach a point of transactional consistency at regular intervals or in response to an external event. This process is called *application quiesce*, described below and in the figure.

In database application quiesce, an external signal or message is sent to a receptive database. In response, the database finishes the current transaction or group of transactions, signaling the frozen image consumer when this is complete. (The database then waits for a second signal indicating that normal operations can resume.) After the database signals that it has reached a state of transactional consistency, the frozen image consumer proceeds with the final steps of creating the frozen image.

Once the frozen image has been created, another signal is sent to the waiting database telling it to resume processing. This is called *unquiescing* the application.



Dialog for Quiesce/Unquiesce



Quiescing the Stack

The storage management stack is a layered arrangement of software elements. An I/O request originated by a database application passes from element to element until a hardware request to move data reaches the storage network. Each stack element performs a variety of functions, some of which treat I/O requests like transactions to assure their completion. Before a frozen image is created, therefore, the stack must be quiesced (made transactionally consistent).

Since the file system is the front-line interface to applications for managing files and performing I/O, file system quiesce is a critical part of quiescing the stack.

File System

Two of the principal tasks of quiescing the file system are the following:

- Prohibit new I/O requests from initiating, which is called *locking the file system*.
- *Flush* file system cache (write cached data back to disk). The system must complete any outstanding application I/O and note completion of outstanding metadata updates.

Volume Manager

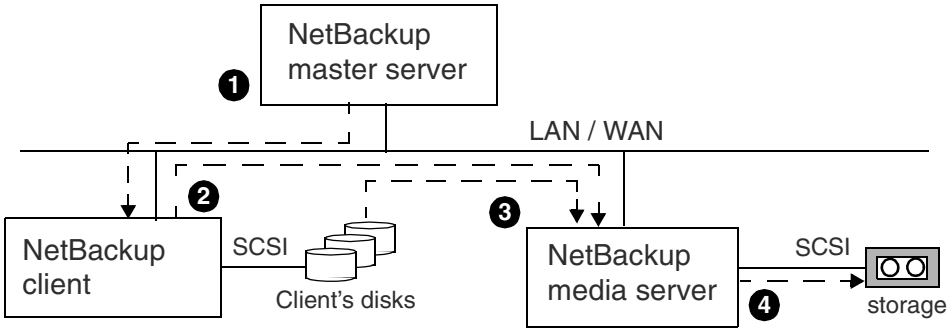
As in a file system, the volume manager's data caching may have to be flushed and disabled until the frozen image is created. As long as volume manager caching is enabled, data required for a consistent image may be lingering in volume manager cache rather than being available on disk when the frozen image is created.

Local Backup of Frozen Image (Local Host)

A frozen image can be backed up to locally attached storage devices, using the Local Host backup method combined with a frozen image method. A fibre channel network or SAN is not required.

The following diagram shows a network configuration sufficient for a Local Host backup of a frozen image. The network configuration is identical to that for normal NetBackup (no frozen image).

Frozen Image Backup on Local Network (No Fibre channel/SAN Required)



1. Client backup is initiated by master server, which tells the NetBackup client to create the frozen image data on the disk.
2. Client sends the data to the media server.
3. Media server processes the backup and reads the client data.
4. Media server writes data to local storage.

Offhost Backup Overview

The primary goal of NetBackup ServerFree Agent is to move I/O processing off the NetBackup client (application host) to either of the following:

- A backup agent executing on another server
- A fibre-channel attached third-party copy device

Note that the disk(s) containing the client's data must be "shared," that is, visible to both the NetBackup client and the NetBackup media server. The disk(s) can be connected locally, or through a SAN.

The backup agent reads data from the frozen image and writes the data to a storage device. Since backup agents are unaware of logical organizations of data such as file systems and volume managers, they can access the data only from its physical disk address location. In order for NetBackup to perform an offhost backup, it must first translate the logical representation of the data to its physical disk addresses. This logical-to-physical translation process is referred to as *mapping* the data. During an offhost backup, the mapping information is transmitted to the backup agent.

File/Volume Mapping Methods

The mapping methods used by NetBackup ServerFree Agent are installed as part of the NetBackup ServerFree Agent product. When a backup is initiated, the correct mapping method is automatically selected by NetBackup, depending on whether the backup data is configured over physical devices, logical volumes, or file systems.

Offhost Backup Methods

NetBackup ServerFree Agent supports two offhost backup methods: *NetBackup Media Server* and *Third-Party Copy Device*.

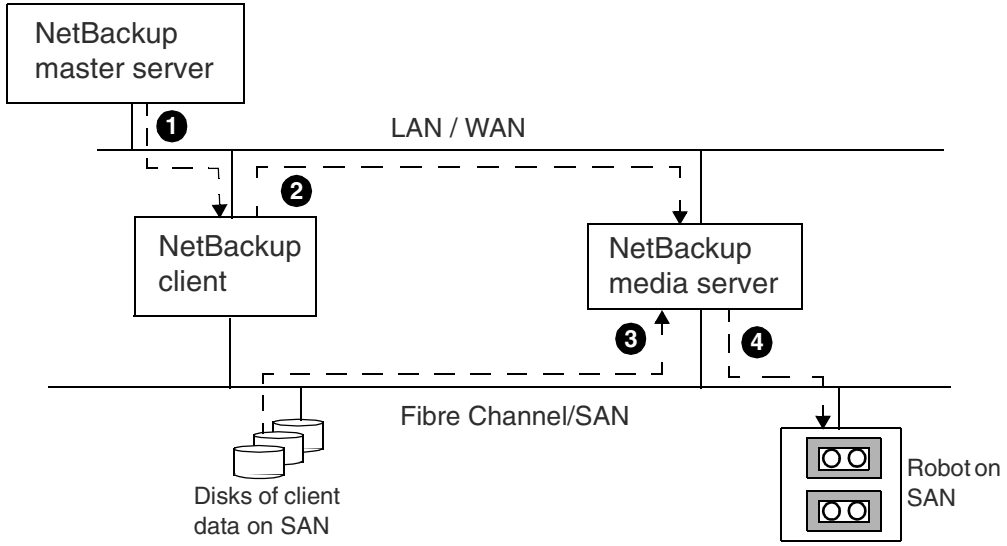
NetBackup Media Server

In this offhost backup method, the NetBackup media server performs the data movement.

The figure "NetBackup Media Server" shows the basic components used in the NetBackup Media Server method. A NetBackup media server handles the backup processing and sends the backup data over Fibre Channel to the storage device.

Note If you have a multi-ported SCSI disk array, a fibre channel SAN is not required. See "Offhost Backup Without a SAN" on page 25.

NetBackup Media Server



1. On LAN, client backup is initiated by master server, which tells the NetBackup client to map the frozen image data on the disk.
2. On LAN, client sends the mapping information to the media server.
3. Media server processes the backup and reads client data over the SAN, from the addresses specified by the client.
4. Media server writes data across the SAN to storage.

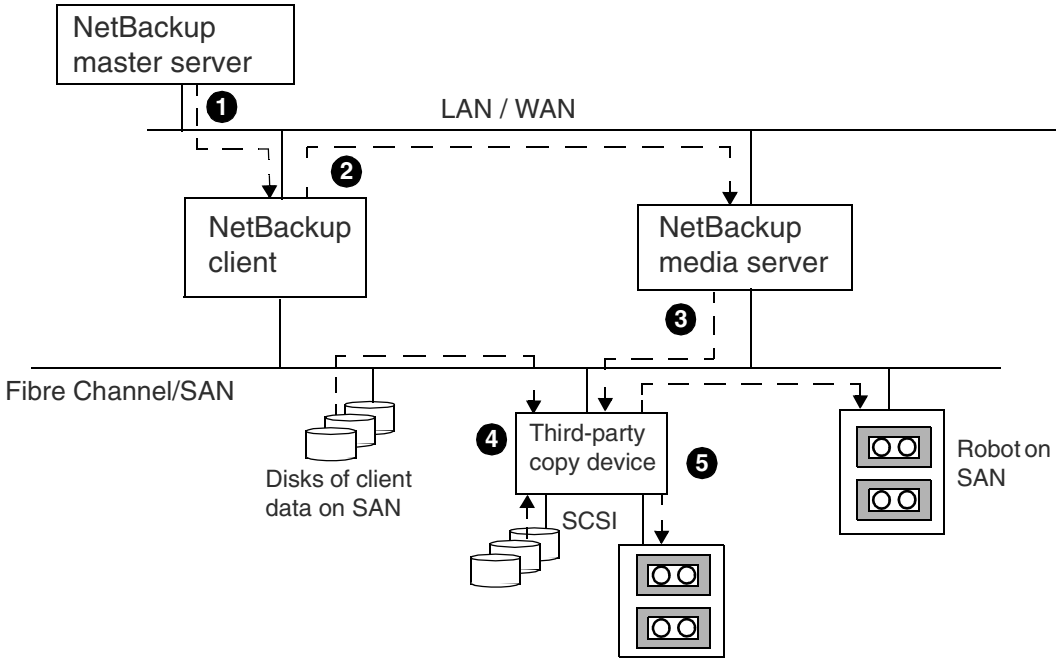
Third-Party Copy Device

In this offhost backup method, a third-party copy device performs the I/O processing of the backup (data movement).

Choose this option if processing time on the NetBackup client is critical and off-loading backup processing to a third-party copy device may save time.

Figure “Third-Party Copy” shows the basic components used in the Third-Party Copy Device method. A third-party copy device (not a component of NetBackup) handles the backup data movement.

Third-Party Copy

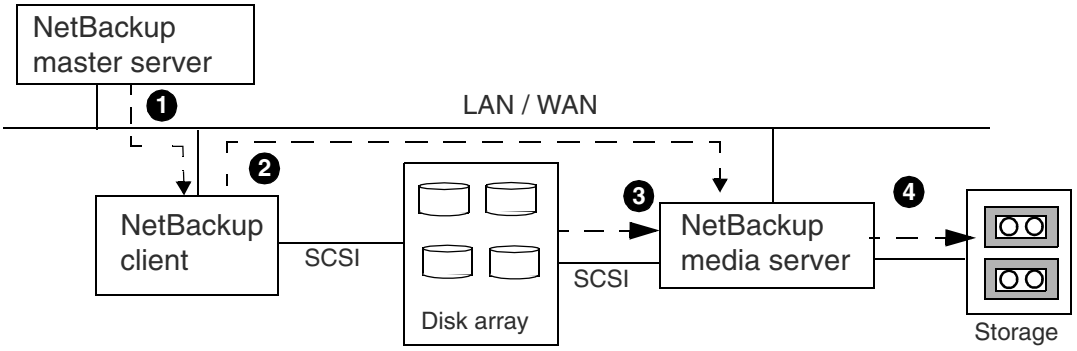


1. On LAN, client backup is initiated by master server, which tells the client to map the frozen image data.
2. On LAN, client sends the mapping information to the media server.
3. Media server sends third-party copy commands to the third-party copy device over the SAN.
4. Third-party copy device reads the client data from either SAN-attached or SCSI-attached disk.
5. Third-party copy device writes data to SAN-attached or SCSI-attached storage.

Offhost Backup Without a SAN

Offhost backup does not require a fibre channel SAN. You can configure a multi-ported SCSI disk array on a LAN or WAN (as shown below) to support a NetBackup media server offhost backup. The NetBackup media server performs the data movement.

NetBackup Media Server with Multi-Ported Disk Array (No SAN)

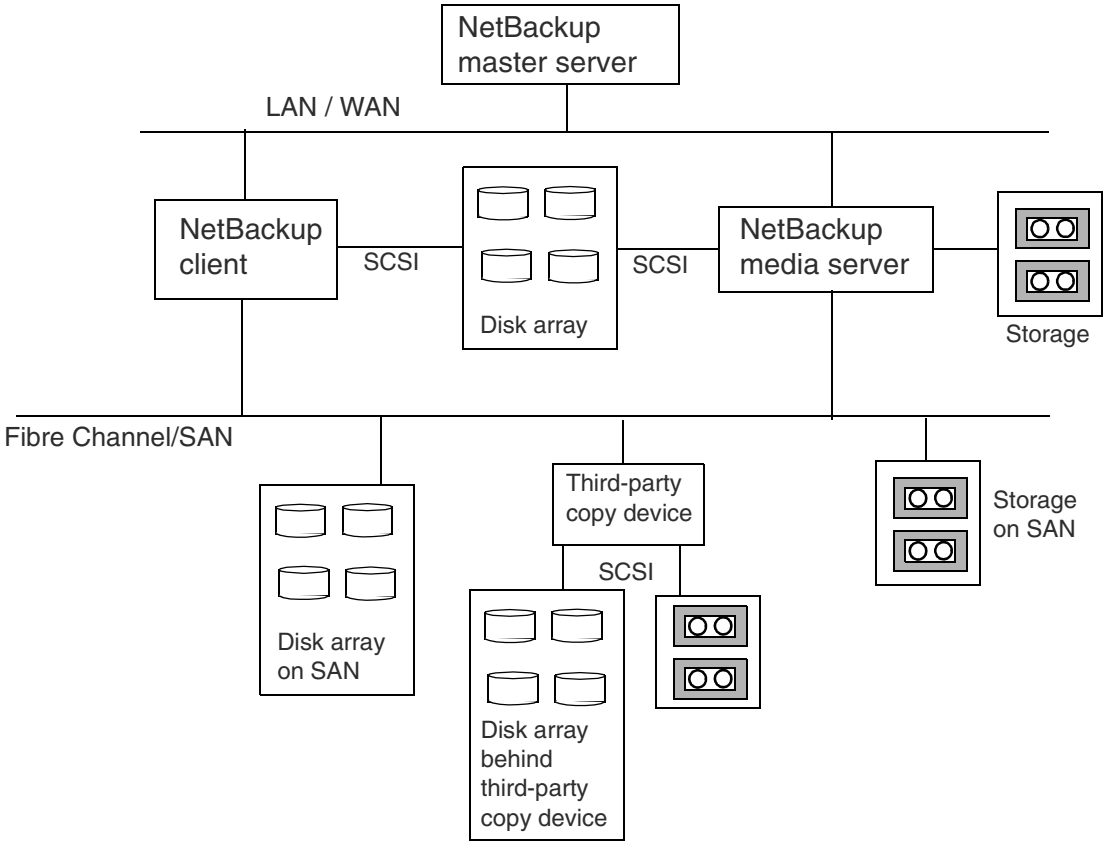


1. Client backup is initiated by master server, which tells the NetBackup client to map the frozen image data on the disk.
2. Client sends the mapping information to the media server.
3. Media server processes the backup and reads client data from the addresses specified by the client.
4. Media server writes data to storage.

Offhost Backup: All the Options

A multi-ported disk array can be combined with fibre channel to support either a NetBackup media server or third-party copy backup. The diagram below shows the following placement options for the disk array:

- On the LAN using SCSI connections to the NetBackup client and media server
- On the SAN behind a third-party copy device
- Directly attached to the SAN



Tables of Features and Required Software

The following table shows the types of backup you can configure with ServerFree Agent, and the corresponding NetBackup features and requirements. The table on the following page shows the software and hardware requirements for each frozen image method.

ServerFree Agent Features and Requirements

Type of Backup	NetBackup ServerFree Agent Feature	NetBackup Software Required	Other Software Required
Local host: client and storage devices on local network.	*NetBackup ServerFree Agent not required.*	NetBackup 4.5 or earlier.	Refer to appropriate *NetBackup Release Notes*.
Local, instantaneous: client and storage devices on local network; active data must remain online during backup.	- Frozen image method: nbu_snap, fsclone, vxvm. For particular arrays: TimeFinder, ShadowImage, Businesscopy. See next table. - Offhost backup method: Local Host.	- Core Frozen Image Services and Extended Frozen Image Services. - FlashBackup needed only for backing up clients in a FlashBackup policy. - Oracle ServerFree Agent needed only for backing up clients in an Oracle policy.	- Requirements depend on the frozen image method (see next table). - For Oracle clients, Oracle8i must be installed prior to installing NetBackup ServerFree Agent.
Offhost: client and storage devices on SAN; third-party copy device available.	- Frozen image method: nbu_snap, fsclone, vxvm. For particular arrays: TimeFinder, ShadowImage, Businesscopy. See next table. - Offhost backup method: Third-Party Copy Device.	- Core Frozen Image Services and Extended Frozen Image Services. - Offhost and SAN Data Movement Services. - FlashBackup needed only for backing up clients in a FlashBackup policy. - Oracle ServerFree Agent needed only for backing up clients in an Oracle policy.	- Requirements depend on the frozen image method (see next table). - For Oracle clients, Oracle8i must be installed prior to installing NetBackup ServerFree Agent.
Offhost: client and storage devices on SAN; third-party copy device *not* available.	- Frozen image method: nbu_snap, fsclone, vxvm. For particular arrays: TimeFinder, ShadowImage, Businesscopy. See next table. - Offhost backup method: NetBackup Media Server.	- Core Frozen Image Services and Extended Frozen Image Services. - Offhost and SAN Data Movement Services. - FlashBackup needed only for backing up clients in a FlashBackup policy. - Oracle ServerFree Agent needed only for backing up clients in an Oracle policy.	- Requirements depend on the frozen image method (see next table). - For Oracle clients, Oracle8i must be installed prior to installing NetBackup ServerFree Agent.

The following table describes each frozen image method and its requirements.

Note Note that ServerFree Agent's frozen image methods and offhost backup methods perform mapping of the underlying file system and volume structure being backed up. This mapping has been verified for the I/O system components listed in this table under "Data Type Supported."

The use of other components in the I/O system, such as other volume managers or storage replicators, may result in an unreliable backup. Such configurations are not supported by ServerFree Agent. For an updated list of supported storage configurations, refer to "ServerFree Agent Information on the Web" on page xiv.

Frozen Image Methods and Requirements

Frozen Image Method	Type	Data Type Supported (for file list and frozen image source entries)	Requirements and Restrictions	Where to Obtain Required Software
nbu_snap (Solaris only)	Copy-on- write snapshot	File systems: - ufs (Solaris) - VxFS Raw partitions: - VxVM volumes - raw disks*	- Core Frozen Image Services option (NetBackup add-on product)	www.veritas.com
fsclone (Solaris only)	Copy-on- write file system snapshot (storage checkpoint).	File system: VxFS.	- Core Frozen Image Services (NetBackup add-on product) - VxFS 3.4 **Note**: Does not support any raw-partition type backups (whether FlashBackup or Standard policy).	VxFS 3.4 is part of VERITAS Database Edition for Oracle 2.2: www.veritas.com
vxvm (Solaris or HP)	Snapshot mirror	File systems: - ufs (Solaris) - VxFS - Online JFS (HP only) Raw partitions: - VxVM volumes	- Core Frozen Image Services (NetBackup add-on product) - VxVM 3.1 or later **Note**: vxvm cannot be used with VxVM volumes configured as RAID-5. **Note**: The frozen image source must be configured with a VxVM 3.1 snapshot mirror (see "Creating a Snapshot Mirror of the vxvm Frozen Image Source" in the *NetBackup ServerFree Agent System Administrator's Guide*).	For VERITAS Volume Manager (VxVM) 3.1: www.veritas.com

Frozen Image Methods and Requirements

Frozen Image Method	Type	Data Type Supported (for file list and frozen image source entries)	Requirements and Restrictions	Where to Obtain Required Software
TimeFinder (Solaris or HP)	Mirror	File systems: - ufs (Solaris) - VxFS - Online JFS (HP only) Raw partitions: - VxVM volumes - raw disks*	- Extended Frozen Image Services (NetBackup add-on product) - EMC TimeFinder Symapi **Note**: TimeFinder frozen image method is for EMC Symmetrix disk arrays only.	www.veritas.com Contact EMC for Symapi
ShadowImage (Solaris or HP)	Mirror	File systems: - ufs (Solaris) - VxFS - Online JFS (HP only) Raw partitions: - VxVM volumes - raw disks*	- Extended Frozen Image Services (NetBackup add-on product) - ShadowImage (HOMRCF) **Note**: ShadowImage frozen image method is for Hitachi Data Systems disk arrays.	www.veritas.com Contact Hitachi Data Systems for Hitachi Raid Manager
BusinessCopy (Solaris or HP)	Mirror	File systems: - ufs (Solaris) - VxFS - Online JFS (HP only) Raw partitions: - VxVM volumes - raw disks*	- Extended Frozen Image Services (NetBackup add-on product) - Business Copy Services - ShadowImage (HOMRCF) **Note**: BusinessCopy frozen image method is for HP XP series disk arrays.	www.veritas.com Contact Hewlett Packard for Business Copy Services

* Supported raw disks are SCSI (local or fibre channel attached), with sd, dad, and ssd drivers (Solaris) or sdisk drivers (HP).

Configuration Checklist 2

This chapter reviews the basic steps for configuring ServerFree Agent. Each step includes a reference to other parts of this manual for detailed information.

This checklist covers all phases of ServerFree Agent, from hardware setup to NetBackup policy and client configuration. Once these steps are complete, you should be ready to run a backup using frozen image and offhost backup methods.

Checklist

▼ **For installation:**

1. Install NetBackup DataCenter 4.5 server and client software.

   For detailed instructions, refer to the *NetBackup DataCenter Installation Guide*.

2. Install NetBackup ServerFree Agent software. Select the required options under the NetBackup Add-On Product Software menu, as follows.

   - **Core Frozen Image Services**. This is required for using the default frozen image capabilities of ServerFree Agent, and is also required for doing offhost backup.
   - **Offhost and SAN Data Movement Services**. This is required for offhost backup.
   - **Extended Frozen Image Services** (also known as the Array Integration option). This is required for the following disk-array frozen image capabilities: EMC TimeFinder, Hitachi ShadowImage, HP BusinessCopy.

   For detailed instructions, refer to the "Installation" chapter of this manual.

Note For the NetBackup master server, NetBackup 4.5 ServerFree Agent software may be installed on any UNIX platform.

3. Be sure to distribute the ServerFree Agent software to your Solaris / HP-UX clients.

   For detailed instructions, refer to the "Installation" chapter of this manual.

▼ **For hardware configuration:**

4. Set up and verify the functionality of your network equipment and storage devices, including disk arrays, robots and tape drives, switches, hubs, host-bus adapters, routers and / or third-party copy devices.

   - For offhost backup: To verify NetBackup access to your SAN devices, configure HBA drivers, and create NetBackup configuration files, refer to the "SAN Configuration for ServerFree Agent" chapter of this manual. For additional configuration assistance with particular devices, see "ServerFree Agent Information on the Web" on page xiv.
   - For assistance with disk array configuration, refer to the "Extended Frozen Image Services (Array Integration Option)" chapter of this manual. That chapter begins with an important checklist specifically for disk array configuration.

5. Install the proper versions of all required firmware and device drivers.

For details on supported platforms and peripherals, see "ServerFree Agent Information on the Web" on page xiv.

6. Install and configure other software required by NetBackup. This may include VERITAS Volume Manager (VxVM) or VERITAS File System (VxFS), depending on the type of backup you want to perform.
   - For software requirements, refer to the "Tables of Features and Required Software" in the Introduction of this manual.
   - For VxVM, refer to the VERITAS *Volume Manager Administrator's Guide* and the *Volume Manager Storage Administrator Administrator's Guide*. For VxFS, refer to the VERITAS *File System Administrator's Guide*.

▼ **For a frozen image backup of data on a local network:**

7. Start the NetBackup Administration Console by entering:

   ```
   /usr/openv/netbackup/bin/jnbSA &
   ```

8. Expand **Host Properties** and click on **Clients**. In the right pane, double click on the client you want to configure for frozen image backup. In the Client Properties dialog, expand **UNIX Client** and click **Client Settings**. Click the **Frozen Image Configuration** button. On the Frozen Image Client Configuration display, click **New**. Select a frozen image source type, enter or select the path for the frozen image source, then select a frozen image method. Specify frozen image parameters as required. (For example, for **nbu_snap**, enter the raw partition to be used for cache.) Click **OK**.

   For notes and instructions, refer to the "NetBackup Configuration" chapter of this manual. For notes on the frozen image methods designed for particular disk arrays, refer to the "Extended Frozen Image Services (Array Integration Option)" chapter of this manual.

9. Repeat step 8 for each client you want to configure for frozen image backup.

10. In the left pane of the NetBackup Administration Console, click **Policies**. On the **Attributes** tab, select **Local Host** for the offhost backup method, and select **Allow frozen image clients**. Then click **Apply**.

▼ **For offhost backup of data (server-free):**

11. To set up the required configuration files, refer to Chapter 4, "SAN Configuration for ServerFree Agent." *Chapter 4 contains important information and should be read carefully.*

12. Configure a frozen image method (refer to step 8). Repeat that step for each client you want to configure.

13. Configure an offhost backup method, as follows.

    - Click **Policies** in the NetBackup Administration Console. Open the New (or Change) Policy dialog. Select **NetBackup Media Server** or **Third-Party Copy Device** for the offhost backup method. Then click **Apply**.

Note For **Policy storage unit**, do NOT select **Any_available**.

▼ **For troubleshooting help:**

For help with particular NetBackup status codes, refer to the *NetBackup Troubleshooting Guide*. Additional information is available in the "Troubleshooting" chapter of this ServerFree Agent Guide.

Installation 3

This chapter explains how to install NetBackup ServerFree Agent software.

Prerequisites

- NetBackup DataCenter 4.5 or later server software must be installed on the master / media servers. For performing local (not offhost) backups, the master / media server can be running any supported UNIX platform. For offhost backups, the NetBackup media server must be installed on Solaris 2.6, 7, 8, or 9, or HP-UX 11.00 or 11i.

  For a detailed list of platform versions supported by NetBackup ServerFree Agent, refer to the *NetBackup Release Notes*, or to "ServerFree Agent Information on the Web" on page xiv.
- NetBackup DataCenter 4.5 or later client software must be installed on clients running Solaris 2.6, 7, 8, or 9, or HP-UX 11.00 or 11i.

Installing NetBackup ServerFree Agent

Loading From Media

1. Log in as root on the NetBackup master server.
2. In a separate window, make sure valid license keys for your NetBackup ServerFree Agent options have been installed (these options are listed under step 6 on page 36). To do this, enter the following command to list and add keys:

   `/usr/openv/netbackup/bin/admincmd/get_license_key`
3. Insert the CD-ROM.
4. Change your working directory to the CD-ROM directory:

```
cd /cd_rom_directory
```

Where *cd_rom_directory* is the path to the directory where you can access the CD-ROM. It may be necessary to mount this directory.

5. To install NetBackup 4.5 software on the NetBackup master server and clients, execute the following:

   ```
   ./install
   ```

   The Installation Options menu appears.

6. Select **NetBackup Add-On Product Software**.

   A second menu appears. Select one or more of the following options:

   - **Core Frozen Image Services**. This is required for using any of the frozen image capabilities of ServerFree Agent, and is also required for doing offhost backup.
   - **Offhost and SAN Data Movement Services**. This is required for offhost backup.
   - **Extended Frozen Image Services** (also known as the Array Integration option). This is required for the following disk-array frozen image capabilities: EMC TimeFinder, Hitachi ShadowImage, HP BusinessCopy.

Note **Offhost and SAN Data Movement Services** and **Extended Frozen Image Services** each require the installation of **Core Frozen Image Services**.

7. Enter **q** to quit selecting options. When asked if the list is correct, answer **y**.

NetBackup ServerFree Agent software is installed in

`/usr/openv/netbackup/vfms/`*hardware*`/`*os*`/`*version*`/`

Where:

- *hardware* is Solaris, HP9000-700, or HP9000-800
- *os* is Solaris 2.6, Solaris 7, Solaris 8, Solaris 9, or HP-UX 11.00
- *version* is a six digit number representing the NetBackup version

Installing NetBackup 4.5 on Clients

You must install NetBackup 4.5 (DataCenter) client software on the clients before performing the next procedure. For instructions, refer to the *NetBackup DataCenter Installation Guide for UNIX*.

Distributing ServerFree Agent Software to Clients

Note If the master server is a Solaris or HP-UX system and the master server is also a client, you do not have to distribute ServerFree Agent software to the master. This distribution is done automatically when you load the software from the media (see previous step). However, you must distribute the software as explained below to all other clients that will be using ServerFree Agent.

You must install the ServerFree Agent software on your Solaris / HP-UX clients. Note: you should also perform this procedure if you are doing either of the following:

- Installing a software upgrade (patch)
- Reinstalling ServerFree Agent software on a Solaris client

Execute the following as the root user on the NetBackup 4.5 master server.

1. Check whether `bprd` is running by executing:

   `/usr/openv/netbackup/bin/bpps`

   If only one `bprd` shows up in the `bpps` output, there are no active backups or restores. In that case, terminate the `bprd` daemon by executing:

   `/usr/openv/netbackup/bin/admincmd/bprdreq -terminate`

   If more than one `bprd` appears, wait until the backups and / or restores are complete and then run the `/usr/openv/netbackup/bin/bpps` command again. When only one `bprd` shows up, terminate the `bprd` daemon.

2. You can distribute the ServerFree Agent software to Solaris and HP-UX clients in either of two ways:

   a. Distribute the software to all currently defined clients by executing the following command:

      `/usr/openv/netbackup/bin/update_clients -Install_VFMS`

   b. Distribute the software to specific clients.

      - Create a file that lists the specific clients. For each client, enter a line in this file containing the following three parameters:

        hardware_type operating_system clientname

        For example:

        `Solaris Solaris2.6 mysparc`

        or

        `Solaris Solaris7 othersparc`

or

```
Solaris Solaris8 othersparc
```

or

```
HP9000-800 HP-UX11.00 myhp
```

- Execute the following command (all on one line):

  /usr/openv/netbackup/bin/update_clients -Install_VFMS -ClientList *file*

  Where *file* is the name of the file that you created in the previous step.

Note ServerFree Agent software cannot be distributed to clients by means of the NetBackup Administration Console.

3. Start the NetBackup daemon as the root user on the master server by executing:

   /usr/openv/netbackup/bin/initbprd

When Upgrading from NetBackup 4.0V

Offhost backup (using either the **NetBackup Media Server** or **Third-Party Copy Device** method) requires a configuration file named `3pc.conf`. In NetBackup 4.5, both the format and location of this file have changed.

At NetBackup 4.0V:

```
/usr/openv/netbackup/3pc.conf
```

At NetBackup 4.5:

```
/usr/openv/volmgr/database/3pc.conf
```

Note Because of the new format of this file, copying your existing `3pc.conf` file to the new location will not be sufficient. To run offhost backups, you must recreate the `3pc.conf` file. For assistance, refer to “Create the 3pc.conf File” in the “SAN Configuration for ServerFree Agent”chapter.

The only entries that may be worth saving from your 4.0V version of the `3pc.conf` file are the world-wide name entries for each device.

De-installing NetBackup ServerFree Agent

Server Deinstall

On the master server where you initially loaded the NetBackup ServerFree Agent software, do the following:

1. Check the Activity Monitor in the NetBackup Administration Console to make sure no NetBackup ServerFree Agent backups are active or running (the **State** field should read `Done`).

2. If you installed any NetBackup ServerFree Agent packages, execute the following:

   For the Offhost and SAN Data Movement Services product:

   ```
   pkgrm VRTSnbodm
   ```

   For the Extended Frozen Image Services product:

   ```
   pkgrm VRTSnbefi
   ```

   For the Core Frozen Image Services product:

   ```
   pkgrm VRTSnbfis
   ```

Client Deinstall

1. On the master server, check the Activity Monitor in the NetBackup Administration Console to make sure no NetBackup ServerFree Agent backups are active or running for the client (the **State** field should read `Done`).

2. Execute the following command to deinstall the NetBackup ServerFree Agent software on the client:

   ```
   /usr/openv/netbackup/bin/install_vfms -d
   ```

3. This step applies to Solaris systems only:

Note Do NOT do the following if your NetBackup installation also includes FlashBackup. The following procedure removes the snapshot software; FlashBackup, however, requires the snapshot software.

   Remove the snap driver by executing the following on the client:

   ```
   /usr/sbin/rem_drv snapctl
   rm -rf /dev/rdsk/snap /dev/dsk/snap
   ```


```
rm -f /usr/kernel/drv/snapctl
rm -f /usr/kernel/drv/snapctl.conf
```

If the client is running Solaris 7, 8, or 9, also execute the following:

```
rm -f /usr/kernel/drv/sparcv9/snapctl
```

SAN Configuration for ServerFree Agent 4

Due to the complex and rapidly changing nature of SAN configuration, this chapter describes SAN issues pertaining to NetBackup ServerFree Agent only. Please note the following assumptions:

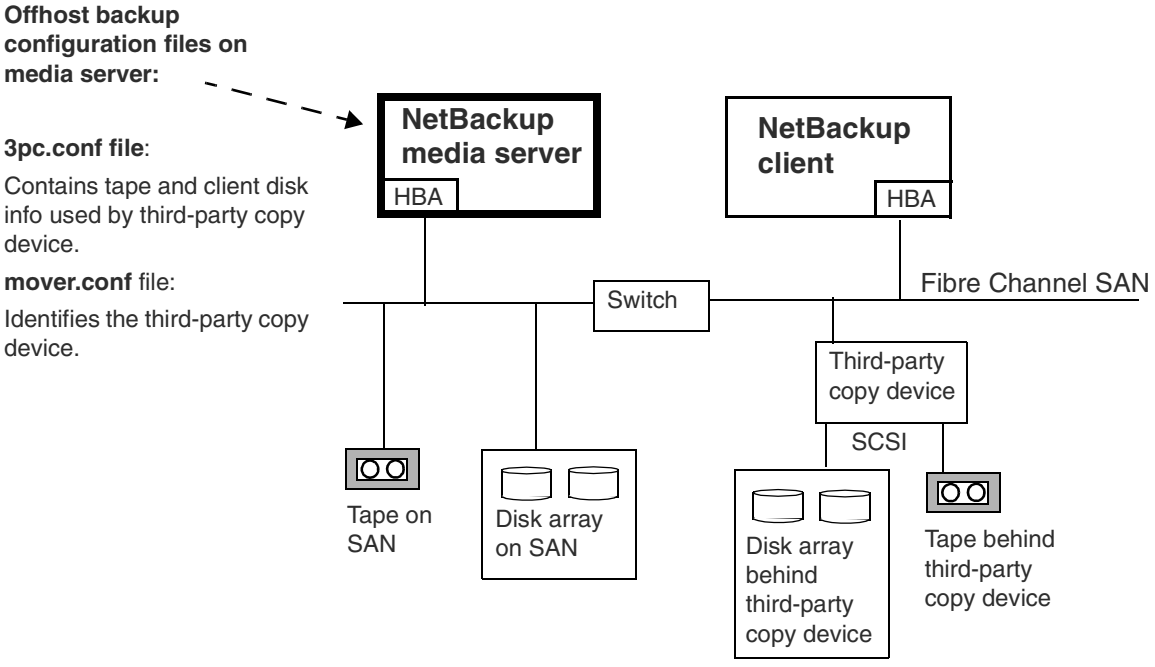
- You have considerable technical expertise in both SAN and NetBackup configuration.
- Your hardware environment is already configured and functional, including switches, hubs, optional bridges or third-party copy devices, robots, tape drives, and disk arrays.

This chapter includes the following topics:

- SAN Configuration Diagram
- Offhost Configuration Requirements
- Offhost Configuration Flowcharts
- Verify NetBackup Access to SAN Devices
- Solaris only: Configure HBA Drivers for Offhost Backup
- Create Offhost Backup Configuration Files

SAN Configuration Diagram

The following diagram shows the devices and configuration files described by the procedures in this chapter. This diagram shows devices configured behind a third-party copy device (bridge) as well as directly attached to the SAN (through the switch).



Supported Peripherals

A complete list of ServerFree Agent supported peripherals can be found on the VERITAS support web site. For instructions, refer to “ServerFree Agent Information on the Web” on page xiv.

Offhost Configuration Requirements

NetBackup ServerFree Agent has two offhost backup methods: NetBackup Media Server and Third-Party Copy Device. The configuration requirements for these methods are different:

- The information needed for the NetBackup Media Server method is easily obtained by means of the `bptpcinfo` command described later in this chapter.
- The information needed for the Third-Party Copy Device method requires use of the `bptpcinfo` and `bpmoverinfo` commands. Depending on your devices, you may also need the following: the VERITAS SANPoint Control product for locating the world-wide port name, and / or the instructions provided with your HBA and bridge / router / third-party copy device. The VERITAS support web site also contains information to help you configure devices (see “ServerFree Agent Information on the Web” on page xiv for instructions).

Diagram for NetBackup Media Server

In this offhost backup method, the NetBackup media server handles the backup processing and sends the backup data over Fibre Channel to the storage device.

Note If you have a multi-ported SCSI disk array, a fibre channel SAN is not required. See "Offhost Backup Without a SAN" on page 25.

NetBackup Media Server

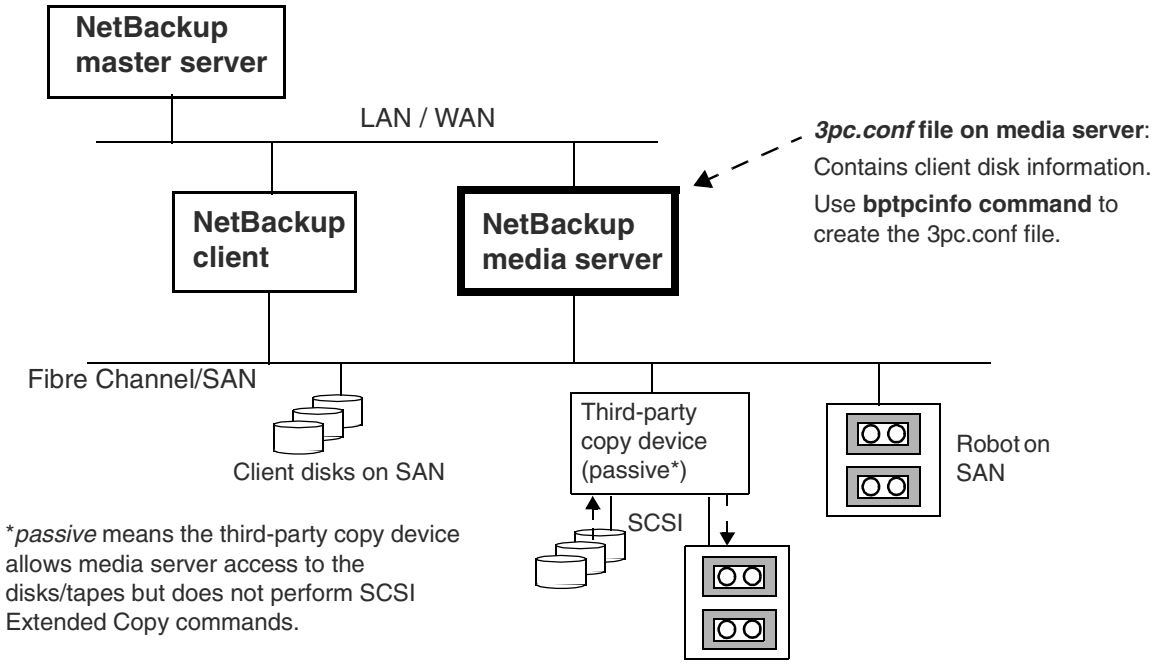


Diagram for Third-Party Copy Device

In this offhost backup method, a third-party copy device performs the I/O processing of the backup (data movement).The 3pc.conf file describes the disks to be backed up and the tape devices for data storage. Be sure to use the flowcharts and accompanying instructions provided under “Offhost Configuration Flowcharts” on page 47.

Third-Party Copy

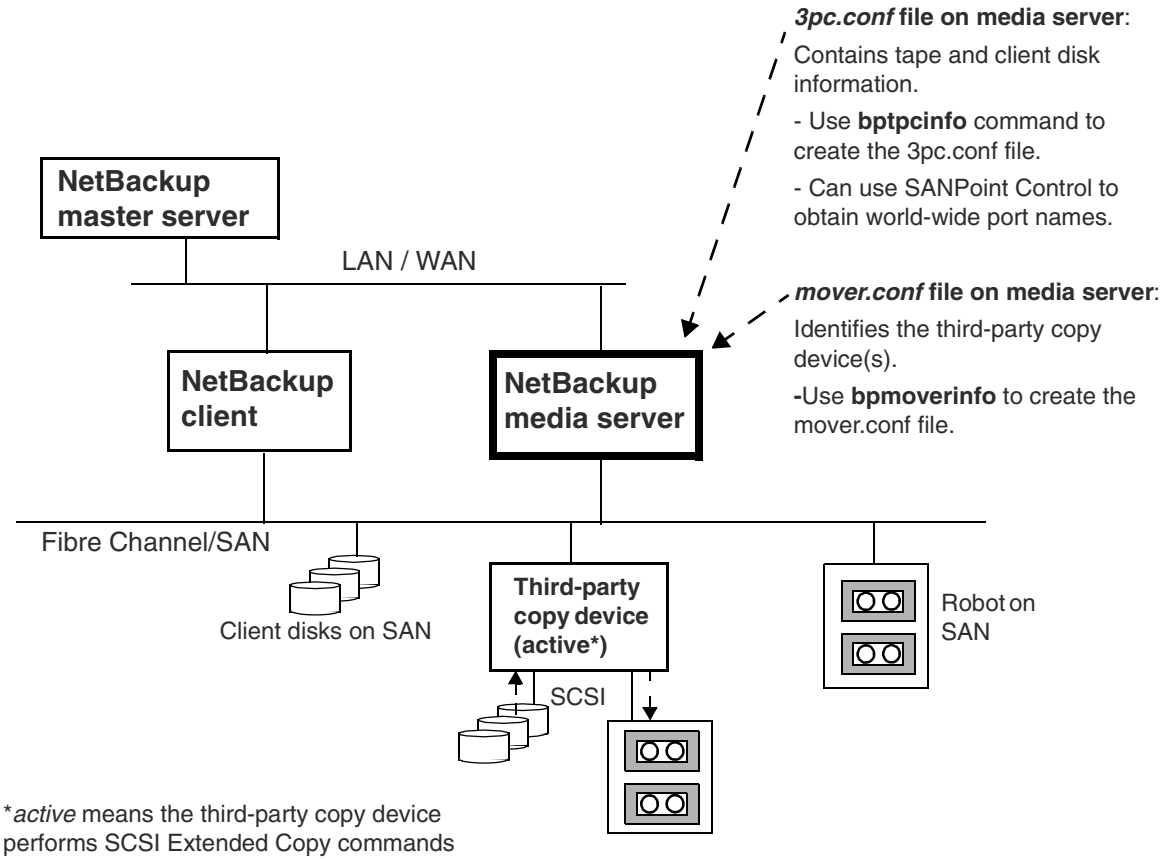
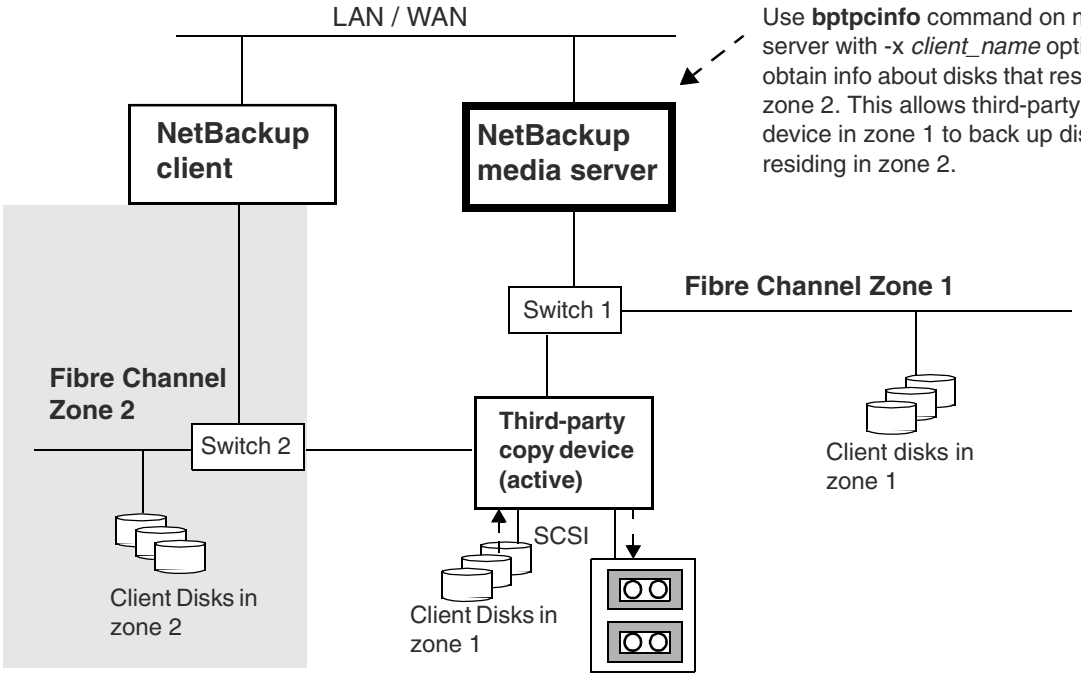


Diagram for Third-Party Copy Device - Remote

In this configuration, the NetBackup media server and the disks containing the client data are on different fibre-channel networks (due to zoning or LUN-masking). The media server can communicate with the NetBackup client by means of the LAN, but does not have access to the client's disks located on a different fibre channel network (or zone). In this case, the 3pc.conf file must be modified with the `bptpcinfo` command using the `-x` *client_name* option, to include information about the client disks.

Third-Party Copy: Remote



Offhost Configuration Flowcharts

The following four charts show the process for setting up configuration files for offhost backup. The instructions for each chart are included later in this chapter.

Chart I: Verify SAN Device Visibility

For instructions, see "Verify NetBackup Access to SAN Devices" on page 51.

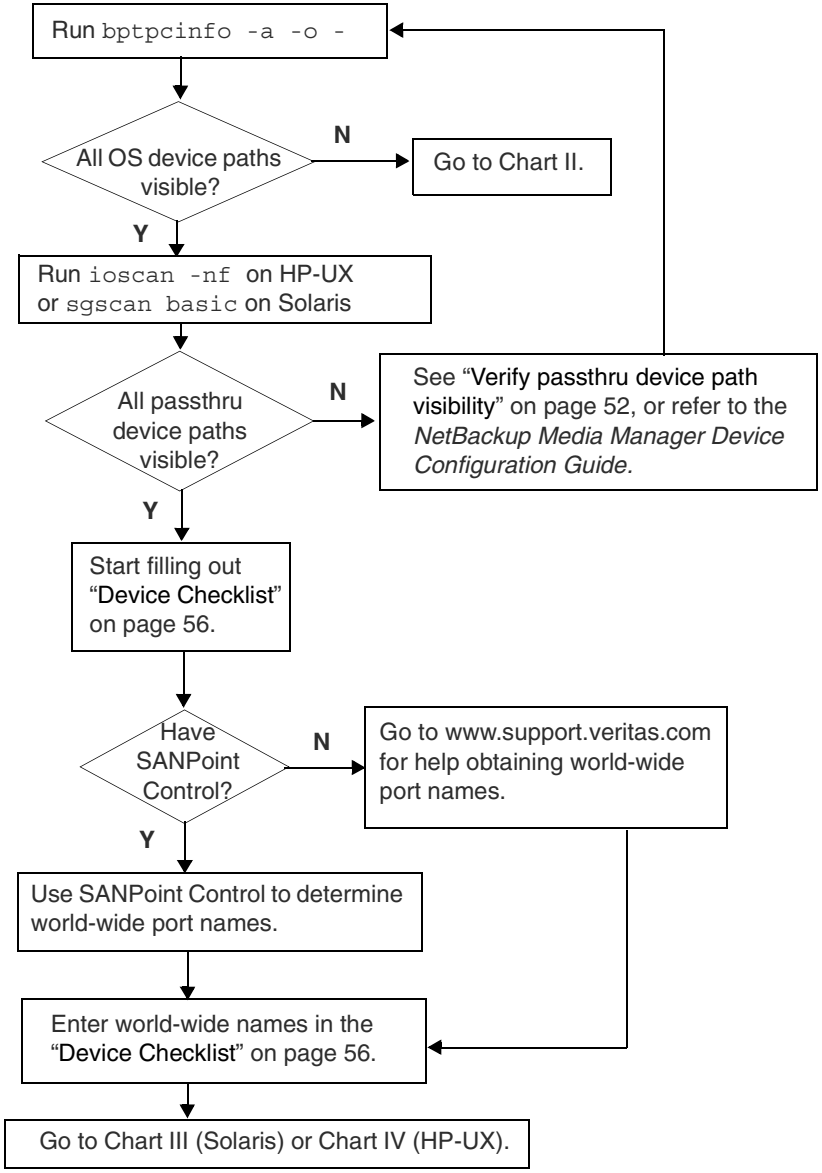


Chart II: Verify OS Device Paths Visibility

For instructions, see “Making OS device paths visible” on page 51.

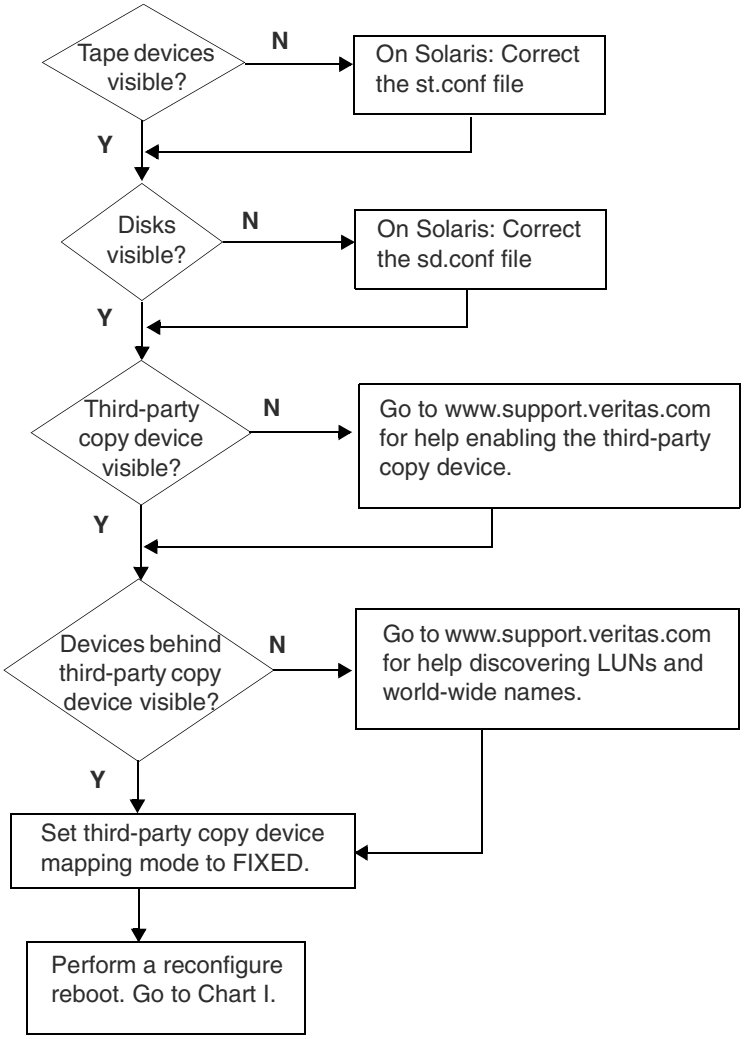


Chart III: Solaris only: Configure HBA Drivers

For instructions, see "Solaris only: Configure HBA Drivers for Offhost Backup" on page 57.

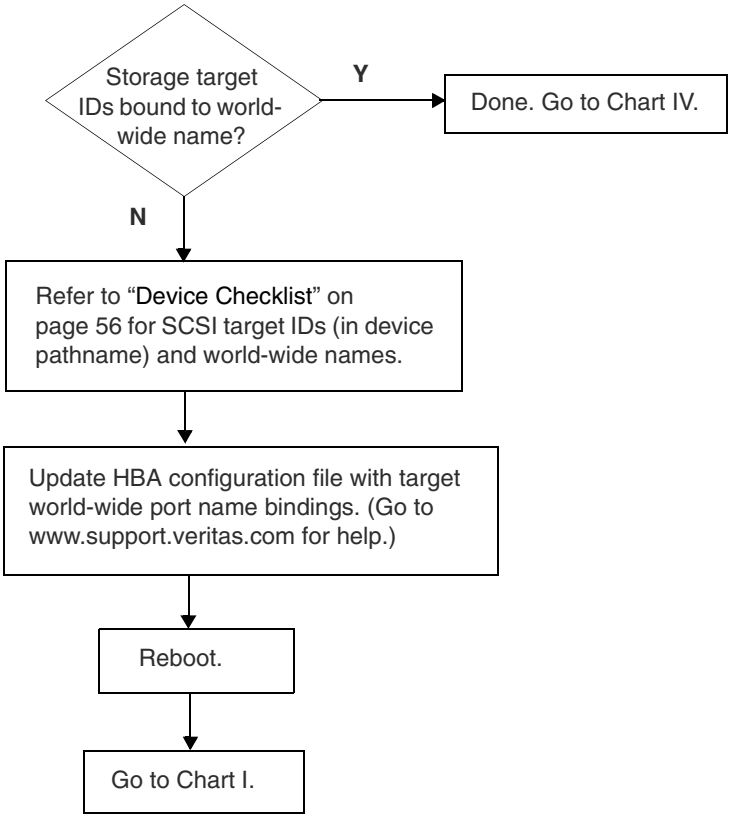
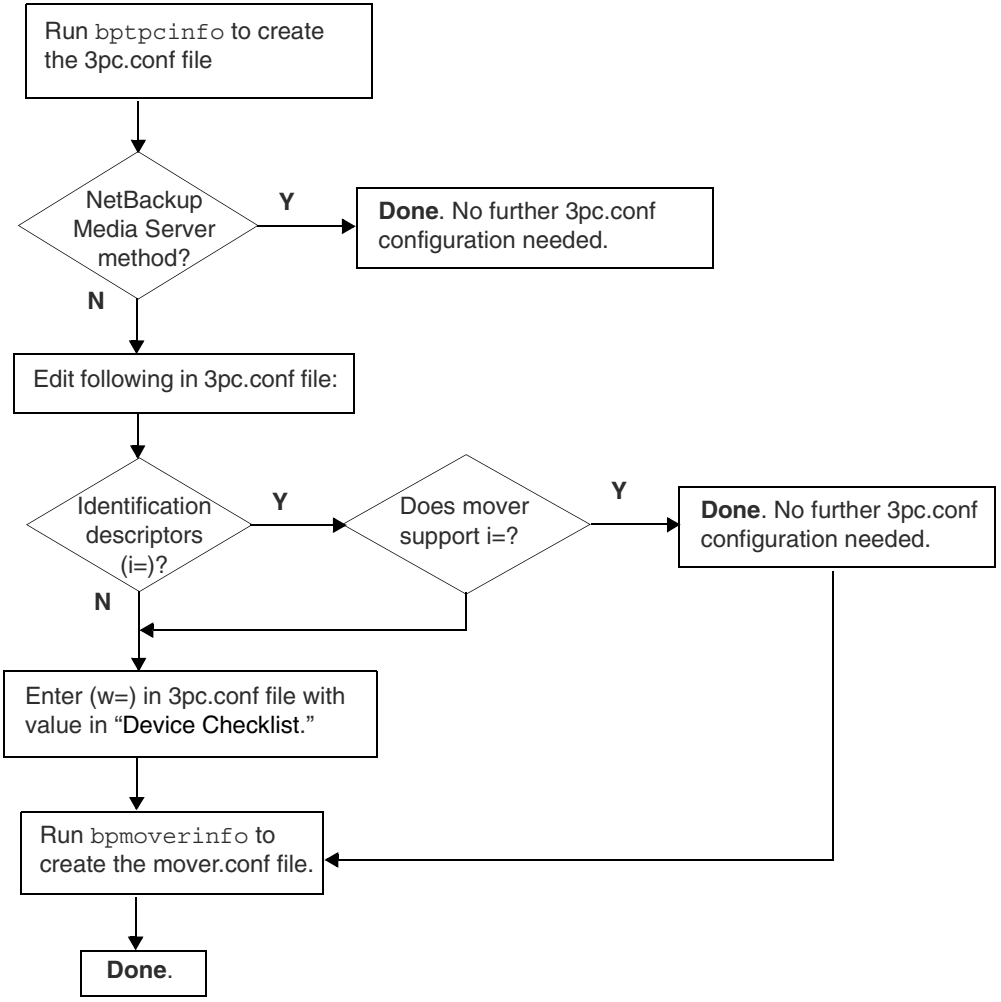


Chart IV: Create the Offhost Backup Configuration Files

For instructions, see "Create Offhost Backup Configuration Files" on page 58.



Verify NetBackup Access to SAN Devices

Note It is assumed that NetBackup and all device drivers are installed, and that devices are properly connected and powered up.

▼ Verify OS device path visibility

1. On the media server, run the `bptpcinfo` command.

   The following sends the output to the screen, using -o - (note the space before the final hyphen).

   `/usr/openv/netbackup/bin/bptpcinfo -a -o -`

   The following sends the output to a file:

   `/usr/openv/netbackup/bin/bptpcinfo -a -o` ***`output_file_name`***

2. Examine the `bptpcinfo` output to see if your OS device paths are listed. If all devices are listed, go to step 8 for HP-UX or to step 9 for Solaris.

▼ Making OS device paths visible

3. **For Solaris:** If your tape devices are not listed in the `bptpcinfo` output, make sure you have target and LUN values for each tape device in the `st.conf` file.

4. **For Solaris:** If your disks are not listed in the `bptpcinfo` output, make sure you have target and LUN values for each disk in the `sd.conf` file.

5. If the devices behind the bridge (or third-party copy device) are not listed in the `bptpcinfo` output, or if the third-party copy device is not enabled for third-party copy data movement, consult the VERITAS support website for assistance (see “ServerFree Agent Information on the Web” on page xiv).

6. On the bridge or third-party copy device, set the address mapping mode to FIXED. This prevents the addresses from changing when the devices are reset. For help configuring supported third-party copy devices, go `www.support.veritas.com`. (See “ServerFree Agent Information on the Web” on page xiv.)

7. Enter the following to reboot the operating system on the media server:

   Solaris:

   ```
   reboot -- -r
   ```

   HP-UX:

   ```
   reboot
   ```


▼ Verify passthru device path visibility

8. **For HP-UX:** Enter the following to list all passthru devices:

   ```
   ioscan -nf
   ```

   a. If all devices now appear, enter the following to regenerate HP-UX special files:

      ```
      insf -e
      ```

      Then go to step 10 on page 53.

   b. If some devices do not appear in the `ioscan` output, check hardware connections to the devices that are not appearing. Then repeat step 8.

Note On HP-UX, there is a limit of eight devices per target. For instance, if you have a JBOD disk array consisting of ten disks, and the array is connected to a bridge, it may be that only the first eight disks in the array are accessible.

9. **For Solaris:**

   a. Perform an `sgscan` to list all passthru devices. Check for proper output and recognition of devices.

      Here is sample output from `sgscan`:

      ```
      barney# sgscan
      /dev/sg/c0t6l1: Disk (/dev/rdsk/c1t6d1): "SEAGATE ST39175LW"
      /dev/sg/c0t6l4: Tape (/dev/rmt/2): "QUANTUM DLT7000"
      /dev/sg/c0t6l5: Changer: "HP      C6280-7000"
      ```

   b. If tape devices still do not show up, make sure you have entries for all SCSI target and LUN combinations in the `sg.links` and `sg.conf` files. Refer to the *Media Manager Device Configuration Guide*, Chapter 2, under "Understanding the SCSI Passthru Drivers."

      - If tape devices are fibre attached, make sure you have entries for the tape devices in the above files.
      - If tape devices are behind a bridge (or third-party copy device), make sure you have entries for the tape devices AND for the bridge/third-party copy device.

      For an example, refer to "Solaris only: Example for sg.links, sg.conf, and st.conf files" on page 54.

If you are unsure how to acquire the SCSI target and LUN values for your configuration, see "ServerFree Agent Information on the Web" on page xiv for help with particular devices. For instance, if your tape drives are configured behind a bridge, router or other fibre-channel device, you may need to telnet into the device to determine the target ID and LUN for each tape drive.

c. When finished updating the `sg.links`, `sg.conf`, and `st.conf` files, remove the old `sg` configuration:

```
rm /kernel/drv/sg.conf
rem_drv sg
```

d. Run the `/usr/openv/volmgr/bin/driver/sg.install` script to copy the files into the correct locations.

e. Copy the `sg.links` and `sg.conf` files (in `/usr/openv/volmgr/bin/driver`) to another location, for future reference. Whenever NetBackup is re-installed, these files in `/usr/openv/volmgr/bin/driver` are overwritten.

10. Run the `bptpcinfo` command again to see which devices are now visible to the media server. Repeat at step 2 if any of your SAN devices are not showing up in the `bptpcinfo` command output.

11. When all devices are listed in the `bptpcinfo` command output, use that information to fill in the device pathname (p=), serial number (s=), and LUN (l=) in the "Device Checklist" on page 56 for each device.

▼ Determine the world-wide name for each device

There are two options:

- Use VERITAS SANPoint Control (step 12).
- Otherwise, refer to "ServerFree Agent Information on the Web" on page xiv for help determining the world-wide name of your devices. Then go to step 13.

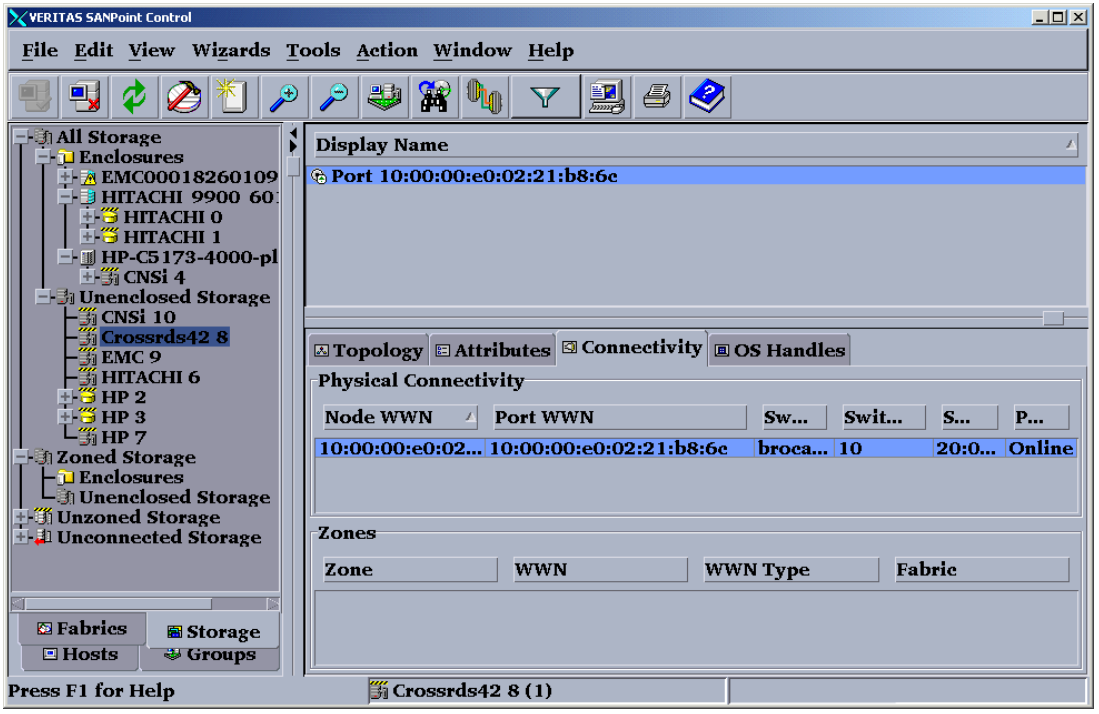
12. You can use VERITAS SANPoint Control to determine the world-wide port names for the devices.

a. Start the SANPoint Control console by entering the following:

```
/opt/VRTSspc/bin/spc &
```

b. Click on the **Storage** tab in the left pane, then click on a device in the left pane (you may have to drill down in the tree).

c. Click the **Connectivity** tab to find the world-wide port name of the device (**Port WWN**). Repeat these steps for each device.



13. Update the “Device Checklist” on page 56 with the world-wide port names of your devices.

Note It is important to record this information! It will be needed again, to complete the configuration.

14. For Solaris: continue with “Solaris only: Configure HBA Drivers for Offhost Backup” on page 57. For HP-UX, continue with “Create Offhost Backup Configuration Files” on page 58.

Solaris only: Example for sg.links, sg.conf, and st.conf files

The following is an example for step 9 on page 52. For the devices in this example, fibre channel LUNs 0, 1, 4, and 5 are needed for target (Loop ID) 6. In this example, LUN 0 is the third-party copy device, LUN 1 is the tape controller, and LUNs 4 and 5 are the tape drives.

- Add entries in the /usr/openv/volmgr/bin/driver/sg.links file so that the necessary /dev/sg/* nodes are created.

  Note that the target and LUNs in the address part of the sg.links entries are hexadecimal, but are decimal in the sg/c\N0tmln part of the entries. Also, make sure there are tabs between the columns, not spaces.

  ```
  type=ddi_pseudo;name=sg;addr=6,0;       sg/c\N0t6l0
  type=ddi_pseudo;name=sg;addr=6,1;       sg/c\N0t6l1
  type=ddi_pseudo;name=sg;addr=6,4;       sg/c\N0t6l4
  type=ddi_pseudo;name=sg;addr=6,5;       sg/c\N0t6l5
  ```

- Add additional target and LUN entries to the /usr/openv/volmgr/bin/driver/sg.conf file.

  ```
  name="sg" class="scsi" target=6 lun=0;
  name="sg" class="scsi" target=6 lun=1;
  name="sg" class="scsi" target=6 lun=4;
  name="sg" class="scsi" target=6 lun=5;
  ```

- In the /kernel/drv/st.conf file, do the following:

  - Add (or un-comment) the appropriate drive entries in the tape-config-list section.

    ```
    tape-config-list =
    "DEC     TZ89",          "DEC DLT",              "DLT7k-data";
    ```

  - Then add (un-comment) the matching data-property-name entry:

    ```
    DLT7k-data = 1,0x38,0,0x39639,4,0x82,0x83,0x84,0x85,2;
    ```

- For each tape drive, add a name entry to the st.conf file.

  Here is an example name entry:

  ```
  name="st" class="scsi" target=6 lun=4;
  name="st" class="scsi" target=6 lun=5;
  ```

  Make sure you have entries for all target and bus combinations for each device.

Device Checklist

Use this checklist or one like it to record information about each of your SAN devices. Some of this information is provided by the bptpcinfo command (such as device pathname and serial number), and some has to be obtained by other means as explained in these procedures. It is vital that the information be recorded accurately.

Type of Device (disk or tape)	Device pathname used by UNIX host (p=)	Serial number (s=)	LUN (l=)	World-wide port name (w=)

Solaris only: Configure HBA Drivers for Offhost Backup

Fibre channel devices should be bound to specific SCSI target IDs by modifying the driver configuration files for your host bus adapter (HBA). This binding ensures that the host HBA and the third-party copy device are in agreement as to the target and LUN values for each device. The binding also ensures that the target ID does not change after a system reboot or after a fibre-channel reconfiguration. If the target ID changes, the offhost backup configuration files (3pc.conf, mover.conf) will also be incorrect and will have to be recreated.

The binding process is unique to each vendor and product. For assistance, refer to the documentation provided for your HBA, or to the VERITAS support website. (See "ServerFree Agent Information on the Web" on page xiv.) The binding requires the fibre-channel world-wide port name.

Note Each time a device is added or removed, the binding must be updated to reflect the new configuration.

If storage device SCSI target IDs are bound to world-wide port names in your HBA configuration file, skip this section and go to "Create Offhost Backup Configuration Files" on page 58.

▼ **To configure HBA drivers on the media server:**

1. If storage device target IDs are not already bound to world-wide port names, refer to your "Device Checklist" on page 56 (filled out in the previous procedure) for the world-wide names. Use the world-wide names to make the binding for each device.

2. Update your HBA configuration file by binding all SCSI device target IDs to their associated world-wide port name.

   For assistance with your particular HBA file, see "ServerFree Agent Information on the Web" on page xiv.

3. Reboot the media server (`reboot -- -r`).

4. To ensure device visibility, repeat the steps described under "Verify NetBackup Access to SAN Devices" on page 51.

   When you are finished, the `bptpcinfo` command should list device pathnames and serial numbers for all of your devices. Update the "Device Checklist" with those values if needed.

5. Continue with "Create Offhost Backup Configuration Files."

Create Offhost Backup Configuration Files

To set up offhost backup, you must create these configuration files on the media server (described in the following sections):

- `/usr/openv/volmgr/database/3pc.conf`
- `/usr/openv/volmgr/database/mover.conf`

Note These files are needed only for the Third-Party Copy Device or NetBackup Media Server backup methods. If not using either of these backup methods, you do not need to create these files.

The 3pc.conf and mover.conf Files: An Overview

The NetBackup media server needs certain information about the devices available on the SAN in order to coordinate an offhost backup. This information is provided in two files:

- `3pc.conf`:

  Identifies the client disks on the SAN that can be backed up, and the robotic libraries / tape drives on which NetBackup can store the data. The NetBackup media server uses this information to access client disks when performing an offhost backup. It also uses this information to generate the SCSI Extended Copy commands required by third-party copy devices.

- `mover.conf`:

  Identifies the third-party copy devices. These are devices that can execute the SCSI Extended Copy commands. A variety of devices can be designed to operate SCSI Extended Copy, such as routers, bridges, robotic libraries, and disk arrays. The `mover.conf` file is needed for the Third-Party Copy Device backup method only, not for the NetBackup Media Server method.

3pc.conf Description

In the `3pc.conf` file, each SAN device needs a one-line entry containing several kinds of values. The values required depend on several factors (explained below). Typically, these include (but are not limited to) the device ID, host-specific device path, and serial number. One or more of the following are also required: the identification descriptor, logical unit number (LUN) and world-wide port name. See “Determining Requirements” on page 61.

Some of this information will be automatically discovered and filled in by the `bptpcinfo` command, as described under “What bptpcinfo Automatically Provides” on page 61. The procedure for using the `bptpcinfo` command is under “Create the 3pc.conf File” on page 65.

Example 3pc.conf file

Below is an example `3pc.conf` file, followed by descriptions of each field.

Example 3pc.conf

```
# devid [p=devpath]    [s=sn]  [n=npid]              [l=lun]      [w=wwpn]     [i=iddesc]
  0    p=/dev/rdsk/c1t2d4s2   s=SEAGATE:ST39175LW:3AL02ERE00001936JFVL      l=4    w=6005013000B05497
  1    p=/dev/rdsk/c1t2d9s2   s=IBM:DDYS-T18350N:4EY1E957                   l=9    w=5005076706C0BB55
  2    p=/dev/rdsk/c1t2d13s2  s=IBM:DDYS-T36950N:TFF6M960                   l=13   w=5005076207C35B38
  3    p=/dev/rdsk/c1t2d14s2  s=SEAGATE:ST336605FC:3FP001Z000008122HWSD     l=14   w=200000203742595A
  4    p=/dev/rdsk/c1t2d15s2  s=SEAGATE:ST336605FC:3FP003KC00008122HWD1     l=15   w=20000020374259B5
  5    p=/dev/rdsk/c1t2d3s2   s=IBM:DDYS-T18350N:4EY1G401                   l=3    w=5005076706C0C0F9
 40    p=/dev/rdsk/c1t20d1s2  s=HITACHI:OPEN-9:0159000000          l=1    w=500060e802eaff04
 41    p=/dev/rdsk/c9t20d1s2  s=HITACHI:OPEN-9:60159000000                  l=1    w=500060e802eaff04
 22    p=/dev/rdsk/c1t18d0s2  s=SEAGATE:ST336605FC:3FP001Z000008122HWSD l=0    i=103200000203742595A
 23    p=/dev/rdsk/c1t19d0s2  s=SEAGATE:ST336605FC:3FP003KC00008122HWD1     l=0    i=10320000020374259B5
```

The `3pc.conf` file can contain the following types of entries (keyword, if any, is in parentheses):

device ID (devid)

A unique NetBackup number for the device. In the 3pc.conf file, the device ID numbers need not be in sequential order, but must be unique.

device path (p=devpath)

The path to the Fibre Channel device. This entry must be specific to the media server on which the `3pc.conf` file resides.

serial number (s=sn)

The serial number of the device, of the form:

Vendor ID:Product ID:device serial number

Note Disk devices used for offhost backup must support SCSI serial-number inquiries or page code 83 inquiries. If a page code inquiry returns an identification descriptor (i=) for a disk, the serial number is not required.

nport ID (n=npid)

The fibre channel n-port ID, which identifies the device on the SAN. This value is usually not required. If you cannot use i=, or w= and l=, refer to "ServerFree Agent Information on the Web" on page xiv to obtain configuration notes including information on the nport ID.

lun (l=lun)

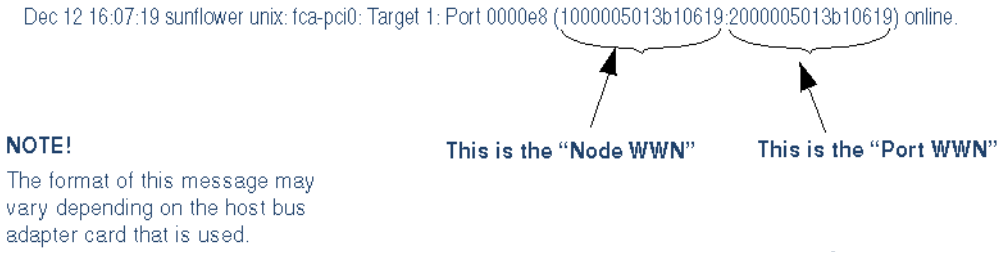
The device's logical unit number. The LUN allows NetBackup to identify devices that are attached by SCSI connection to the third-party copy device, bridge, or other SAN device, or that are directly attached to the fibre channel.

world-wide port name (w=wwpn)

The device's fibre channel *world-wide port name,* which identifies the device on the SAN. This is a 16-digit identifier, consisting of an 8-digit manufacturer name, and an 8-digit device name (numeric).

The following is an example message showing a world-wide name for a device, written to the `/var/adm/messages` log on the server. Note there are two versions of the world-wide name: the *node* wwn and *port* wwn. **For ServerFree Agent, use the port wwn.**

Example of World-Wide Name in /var/adm/messages log



NOTE!
The format of this message may vary depending on the host bus adapter card that is used.

On some devices, the world-wide port name can be found on the back of the device or in the boot-time messages written to the `/var/adm/messages` log on the NetBackup media server.

identification descriptor (i=iddesc)

When available, this value (up to 23 characters) identifies the device on the SAN. If available, the identification descriptor is automatically included in the `3pc.conf` file when you run the `bptpcinfo` command. See "Determining Requirements" for more information on this value.

Determining Requirements

The following determines which values are required in the `3pc.conf` file.

identification descriptor

The identification descriptor is optional, and is not supported by all vendors. (To produce this descriptor, the device must support a page code inquiry with a type 2 or 3 descriptor of less than 20 bytes.) The NetBackup `bptpcinfo` command (explained below) will detect the device's identification descriptor and place it in the `3pc.conf` file if the identification descriptor is available.

Even when this descriptor is available, some third-party copy devices do not support its use.

Note If an identification descriptor is available and the third-party copy device supports it, the descriptor is used to identify the device on the SAN; in this case, there is no need for the LUN or world-wide name. To determine whether your third-party copy device supports identification descriptors, go to www.support.veritas.com (see "ServerFree Agent Information on the Web" on page xiv).

---

world-wide port name

If an identification descriptor is not available or the third-party copy device does not support identification descriptors, the device's world-wide port name must be included in the 3pc.conf file.

What bptpcinfo Automatically Provides

The NetBackup `bptpcinfo` command detects some or all of the device information needed for the offhost backup and places that information in the `3pc.conf` file, as follows:

- The `bptpcinfo` command provides the device path, serial number, identification descriptor (if available), and the LUN.
- The `bptpcinfo` command does not provide the world-wide name.

What the Backup Methods Require

For the NetBackup Media Server offhost backup method, the `bptpcinfo` command provides all the information you need (no manual editing is required).

The Third-Party Copy Device method requires more information for each disk. In some instances, the `bptpcinfo` command cannot gather all the information required.

mover.conf Description

The /usr/openv/volmgr/database/mover.conf file identifies the third-party copy devices that NetBackup can use for the Third-Party Copy Device backup method. This file is not needed for the NetBackup Media Server method.

If your site has only one third-party copy device, use the bpmoverinfo command (see "Create the mover.conf File" on page 67) to create the mover.conf file. The bpmoverinfo command makes the appropriate entry in the mover.conf file and no further configuration is needed.

Example mover.conf files

For sites that have one third-party copy device

- The mover.conf file can consist of one line specifying the device by means of its sg driver device path (Solaris) or sctl device path (HP-UX).

  For example, on Solaris:

  ```
  /dev/sg/c6t1l0
  ```

  On HP-UX:

  ```
  /dev/sctl/c6t1l0
  ```

  That is all you need in the mover.conf file. You can use the following command to determine the SG driver device path:

  ```
  sgscan basic
  ```

  Here is some sample sgscan output (see notes following):

  ```
  /dev/sg/c6t1l0: dev type ch PATHLGHTSAN Gateway     0016
  /dev/sg/c6t1l1: dev type 0h SEAGATE ST39173N        6244
  /dev/sg/c6t1l2: dev type 0h FUJITSU MAG3182L SUN18G 1111

  /dev/sg/c6t4l0: dev type 3h CNSi    FS1310          jj01
  /dev/sg/c6t4l1: dev type 0h FUJITSU MAG3182L SUN18G 1111
  /dev/sg/c6t4l2: dev type 0h FUJITSU MAG3182L SUN18G 1111
  ```

  Notes:

  - "dev type ch PATHLGHTSAN Gateway" indicates a Pathlight SAN Gateway device. Its device path in this example is /dev/sg/c6t1l0.

- "dev type 3h CNSi" indicates a Chaparral device. Its device path in this example is /dev/sg/c6t4l0.

- An alternative: the mover.conf file can consist of one line specifying the device by means of the /dev/rmt/*device_file_name*, where *device_file_name* specifies the actual file name of the device. Note that the tape device you specify must be the same as the device that NetBackup selects for the backup.
- Another alternative: if the third-party copy device is a tape drive, the mover.conf file can consist of a single entry: TAPE. For more information, refer to "Keywords in Mover File," below.

For sites that have multiple third-party copy devices

- In the mover.conf file, if you want to specify one of the third-party copy devices and prevent the others from being used, specify the device by means of its sg or sctl driver device path (such as /dev/sg/c6t1l0 on Solaris or /dev/sctl/c6t1l0 on HP-UX), or specify its /dev/rmt/*device_file_name*.
- If you want to use any available tape drive that is third-party-copy capable, specify the TAPE keyword. For more information, refer to "Keywords in Mover File," below.
- If you want to limit the third-party copy device to that of a particular vendor or type, while including a variety of devices in the file, use the END keyword. First enter the device(s) you want to use, followed by END, then specify any other devices you might want to use at another time. For more information, refer to "Keywords in Mover File," below.

Keywords in Mover File

The following keywords can be included in the mover file:

TAPE

The TAPE keyword tells NetBackup to attempt to use the current tape device if that device has third-party copy functionality. This has two advantages:

- There is no need to specify a device path or passthru driver device path. Instead, NetBackup uses the assigned tape device if it has third-party copy capability.
- Allows better concurrent backup processing, so that two or more backup jobs can execute simultaneously.

Note To use a tape unit as a third-party copy device, a SCSI passthru device path must have been configured for that tape device.

END

END tells NetBackup to stop searching the `mover.conf` file for third-party copy devices for the current third-party copy backup.

If there are two or more third-party copy devices in the mover.conf file, NetBackup tries them sequentially, starting with the first one listed in the file, until one is found that can successfully move the data. END means do not look further in the current mover file and do not look in any other mover files, even if the last device tried was unsuccessful. If no successful device is found before END is reached, the backup fails.

The END keyword limits the search for a third-party copy device in a `mover.conf` file that contains entries for more than one device. This can save you the trouble of deleting device entries and re-entering them later.

For example, if the `mover.conf` file contains the following:

```
/dev/sg/c6t4l0
END
/dev/sg/c6t4l2
/dev/sg/c6t4l3
```

NetBackup will try to use device `/dev/sg/c6t4l0` and will not try the other devices.

Naming the Mover File

In addition to the standard `mover.conf` file name, there are two other options for naming the mover file:

Per Policy

`/usr/openv/volmgr/database/mover.conf.`*policy_name*

where *policy_name* is the name of a NetBackup policy. All backups for this policy will use the third-party copy device specified in this `mover.conf.`*policy_name* file.

For a disk that has third-party copy device capability, use the `mover.conf.`*policy_name* form to specify the disk as the third-party copy device for the policy that backs up that disk.

Per Storage Unit

`/usr/openv/volmgr/database/mover.conf.`*storage_unit_name*

where *storage_unit_name* is the name of a storage unit. This allows a third-party copy device to use a particular storage device by means of a storage unit name. Here is an example `mover.conf` file name of the *storage_unit_name* type:

```
mover.conf.nut-4mm-robot-tl4-0
```

where `nut-4mm-robot-tl4-0` was selected as the storage unit in the Change Policy dialog.

Note The *storage_unit_name* in this file name must exactly match the name of the storage unit as it appears in the "Policy storage unit" field of the Change Policy dialog.

Mover File: Order of Searching

NetBackup looks for an appropriate `mover.conf` file in the following order:

1. `mover.conf.`*policy_name*
2. `mover.conf.`*storage_unit_name*
3. `mover.conf`

Create the 3pc.conf File

The `/usr/openv/volmgr/database/3pc.conf` file contains a list of all disk and tape devices on the SAN that NetBackup ServerFree Agent can use for offhost backups.

Note If you are using the Local Host backup method, there is no need to create a `3pc.conf` file.

1. Create a `3pc.conf` file as follows when no backups are in progress.

   On the media server, run the `bptpcinfo` command:

   ```
   /usr/openv/netbackup/bin/bptpcinfo -a
   ```

   - If a `3pc.conf` file already exists in `/usr/openv/volmgr/database`, you are asked if you want to overwrite it. You can use the `-o output_file_name` option to send the output to a temporary file. However, the correct output must be included in the `/usr/openv/volmgr/database/3pc.conf` file before offhost backups can succeed.
   - If a storage device is currently involved in a backup, the `bptpcinfo` command cannot gather information on that device and skips to the next device. If the `3pc.conf` file contains no entry for a storage device on your network, use the verbose mode (-v) of the `bptpcinfo` command to determine if the device was busy (see the commands appendix for more information on `bptpcinfo`).

Note For the NetBackup Media Server offhost backup method, no more configuration is needed. The `3pc.conf` file only needs the device ID, device path (p=), and serial number (s=) of each device. You can skip the rest of this chapter.

2. **For the Third-Party Copy Device method only:**

   If the media server does not have access to all disks (due to zoning or LUN-masking issues), run `bptpcinfo` with the -x option as follows:

   ```
   /usr/openv/netbackup/bin/bptpcinfo -a -x client_name
   ```

   where *client_name* is the name of a NetBackup client on the fibre channel network where the third-party copy device is located. The `3pc.conf` file will be updated with information about the disks on this network, allowing the media server to "see" those disks. This information may have to be edited by adding the world-wide name (wwn=) of each device, as explained in the next step.

   Note that the entries added by the -x option do not include path names (p=). In the following example, lines 168 and 169 were added by the -x option:

   ```
   162   p=/dev/rdsk/c4t14d0 s=EMC:SYMMETRIX:601092092000        l=0
   163   p=/dev/rdsk/c4t14d1 s=EMC:SYMMETRIX:601092093000         l=0
   164   p=/dev/rdsk/c4t15d0 s=EMC:SYMMETRIX:601092094000            l=0
   165   p=/dev/rdsk/c4t15d1 s=EMC:SYMMETRIX:601092095000            l=0
   166   p=/dev/rmt/c19t0d1BESTnb s=QUANTUM:DLT7000:TNB01S0623         l=1
   w=2000005013b10027
   167   p=/dev/rmt/c19t0d2BESTnb s=QUANTUM:DLT7000:TNA49S0151         l=2
   w=2000005013b10027
   168   s=IBM:DDYST1835SUN18G:1HY964        l=0 i=1035005076506C90C44
   169   s=IBM:DDYST1835SUN18G:1J5049        l=0 i=1035005076506C92409
   ```

3. **For the Third-Party Copy Device method only:**

   Edit the `3pc.conf` file as follows:

   a. For each storage device listed in the `3pc.conf` file, you may need to provide world-wide port names, depending on what NetBackup was able to discover about the device and what the third-party copy device supports.

      These are the editing tasks:

      - In the `3pc.conf` file, if each device that will be backed up with ServerFree Agent has an identification descriptor (i=), and if the third-party copy device supports the use of identification descriptors, the `3pc.conf` file is complete. No editing is needed; skip the rest of this section and continue with "Create the mover.conf File" on page 67.

- If the `3pc.conf` file does not have an identification descriptor for each device (or the descriptor is not supported by the third-party copy device), enter the world-wide port name (w=) for each device. (Obtain the world-wide port name from your "Device Checklist" on page 56.)

Create the mover.conf File

This section describes how to create a list of the available third-party copy devices in a `mover.conf` file (required for the Third-Party Copy Device method only).

1. On the NetBackup media server, enter the following command:

   ```
   /usr/openv/netbackup/bin/admincmd/bpmoverinfo
   ```

   This creates the following file:

   ```
   /usr/openv/volmgr/database/mover.conf
   ```

   The `bpmoverinfo` command discovers any third-party copy devices available on the SAN and lists them in the `mover.conf` file. Any tape drives with third-party copy capability are listed first.

   For a description of the `bpmoverinfo` command, refer to the commands appendix.

Note For `bpmoverinfo` to correctly list third-party copy devices in the `mover.conf` file, the third-party copy devices must already have passthru paths defined. For an example, see "Solaris only: Example for sg.links, sg.conf, and st.conf files" on page 54.

2. If you need to control the circumstances under which a third-party copy device is used, create a separate mover.conf file for a policy or storage unit:

   ```
   /usr/openv/volmgr/database/mover.conf.policy_name
   ```

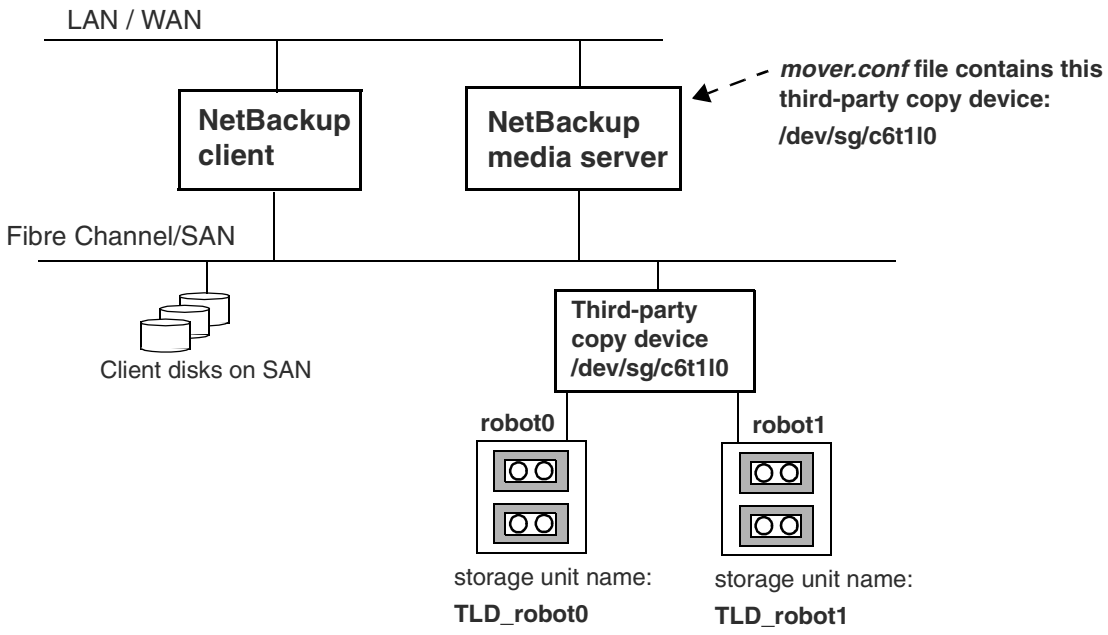
   or

   ```
   /usr/openv/volmgr/database/mover.conf.storage_unit_name
   ```

   For information on these naming formats and possible mover file entries, refer to "mover.conf Description" on page 62 and "Naming the Mover File" on page 64.

   Following are example storage environments and `mover.conf` files.

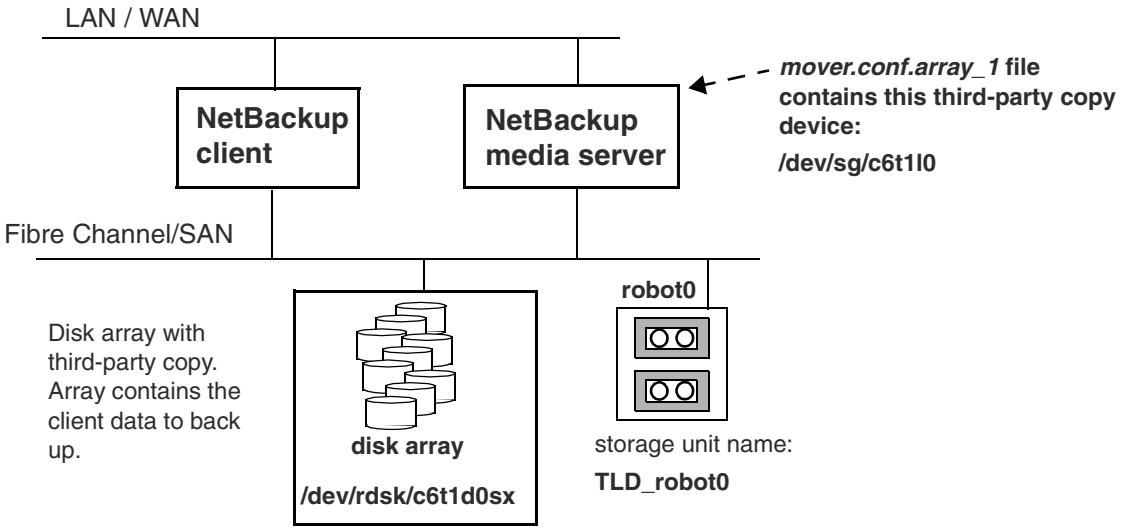
Example `mover.conf` file for a site with one third-party copy device



In the above example, all offhost backups will use third-party copy device `/dev/sg/c6t1l0` specified in the `mover.conf` file. The backup uses the storage unit (`TLD_robot0` or `TLD_robot1`) specified for the policy on the Change Policy dialog.

See the next figure for an example configuration involving a disk array with third-party copy device capability.

Example `mover.conf.`*policy_name* file for site with third-party copy capability in disk array



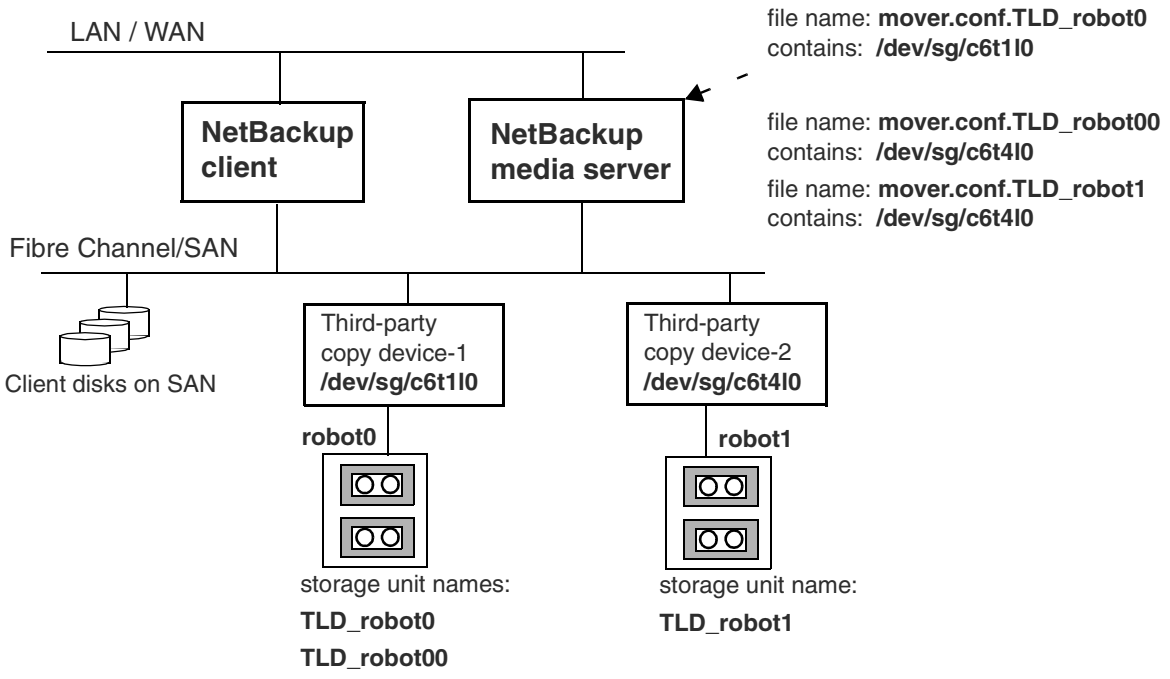
In this example, policy `array_1` is configured to back up the client data contained on the disk array. The backup uses storage unit `TLD_robot0` to store the data.

All backups configured in this policy will use the disk array as the third-party copy device. The `mover.conf.array_1` file specifies that array.

Note The client data must reside in the array that is used as the third-party copy device.

See the next figure for an example configuration with two third-party copy devices, where both devices can use the same robot.

Example mover.conf.*storage_unit_name* files for two third-party copy devices



The above example shows two robots (robot0 and robot1). Robot0 has been assigned two storage unit names, `TLD_robot0` and `TLD_robot00`. Robot1 has been assigned one storage unit name, `TLD_robot1`.

The above example also shows two third-party copy devices, device-1 with a SCSI passthru device path of `/dev/sg/c6t1l0`, and device-2 with a SCSI passthru device path of `/dev/sg/c6t4l0`.

- To allow third-party copy device-1 to use robot0, create a file named `mover.conf.TLD_robot0`. In the file, include the device path of device-1 (`/dev/sg/c6t1l0`).
- To allow third-party copy device-2 to use the same robot (robot0), create a file named `mover.conf.TLD_robot00`. In the file, include the device path of device-2 (`/dev/sg/c6t4l0`). Notice that the file name must refer to a different storage unit, `TLD_robot00`, which is assigned to robot0.
- To allow third-party copy device-2 to use robot1, create a file named `mover.conf.TLD_robot1` that includes the device path of device-2 (`/dev/sg/c6t4l0`).

Note The *storage_unit_name* portion of the `mover.conf.`*storage_unit_name* file name must exactly match the actual name of the storage unit. See under “Configuring a Backup Method” on page 79 for an example Change Policy dialog showing a storage unit name in the **Policy storage unit** field.

NetBackup Configuration 5

This chapter explains how to configure NetBackup ServerFree Agent for making frozen image and offhost backups. For a detailed discussion of NetBackup configuration (apart from ServerFree Agent issues), see the *NetBackup DataCenter System Administrator's Guide for UNIX*.

The following topics are covered in this chapter:

- Prerequisites
- Configuration at a Glance
- Configuring a Frozen Image Method
- Configuring a Backup Method
- Configuration Tips

Prerequisites

Before proceeding with this chapter, make sure the following steps have been completed.

- The following must be installed on the NetBackup master server and clients (refer to the "Installation" chapter):
  - NetBackup 4.5.
  - The "Core Frozen Image Services" product, for using frozen images and offhost backup.
  - The "Offhost and SAN Data Movement Services" product, for offhost backup.
  - The "Extended Frozen Image Services product, for using disk array frozen image methods (EMC TimeFinder, Hitachi ShadowImage, HP BusinessCopy).
- For offhost backup, a fibre channel network (or multi-ported SCSI disk array) must be configured.
- Configure storage devices (you can use the Device Configuration wizard).
- Create a policy with a backup schedule, and specify the client and files to back up (file list). Be sure to specify the client type as Solaris or HP-UX. (If you use the Backup Policy Configuration wizard, see "Backup Policy Configuration Wizard" on page 84.)

Note For frozen image backups, the maximum pathname length is 1000 characters (as opposed to 1023 characters for backups that do not use a frozen image method). Refer to "Maximum Pathname Length" on page 81 for more information on this restriction. The *NetBackup DataCenter System Administrator's Guide* describes other file-path rules.

- Create the following troubleshooting debug directories (use an access mode of 755):

  `/usr/openv/netbackup/logs/online_util` (on the NetBackup client)

  `/usr/openv/netbackup/logs/bpbkar` (on the NetBackup client)

  `/usr/openv/netbackup/logs/bptm` (on the NetBackup media server)

  `/usr/openv/netbackup/logs/bpbrm` (on the NetBackup media server)

Configuration at a Glance

The configuration sections in this chapter do the following:

1. Help you choose a frozen image method. The frozen image method is configured for a particular client, not for a policy.

Note Use of a frozen image method does not require offhost backup. You can use a frozen image method to capture a frozen image of locally available data (file systems, raw devices, volumes, and databases).

2. Help you choose an offhost backup method (no offhost backup is called **Local Host**). Note that the backup method is a *policy* attribute.

Configuring a Frozen Image Method

This procedure explains how to configure a frozen image method. You must do this if either of the following apply:

- You are configuring an offhost backup.
- You want to capture a frozen image of locally available data (not offhost).

This procedure involves designating a *frozen image source*. The frozen image source can be a file system, logical volume, or raw partition, and is associated with the files specified in the policy's file list. (Two examples are provided in this chapter.)

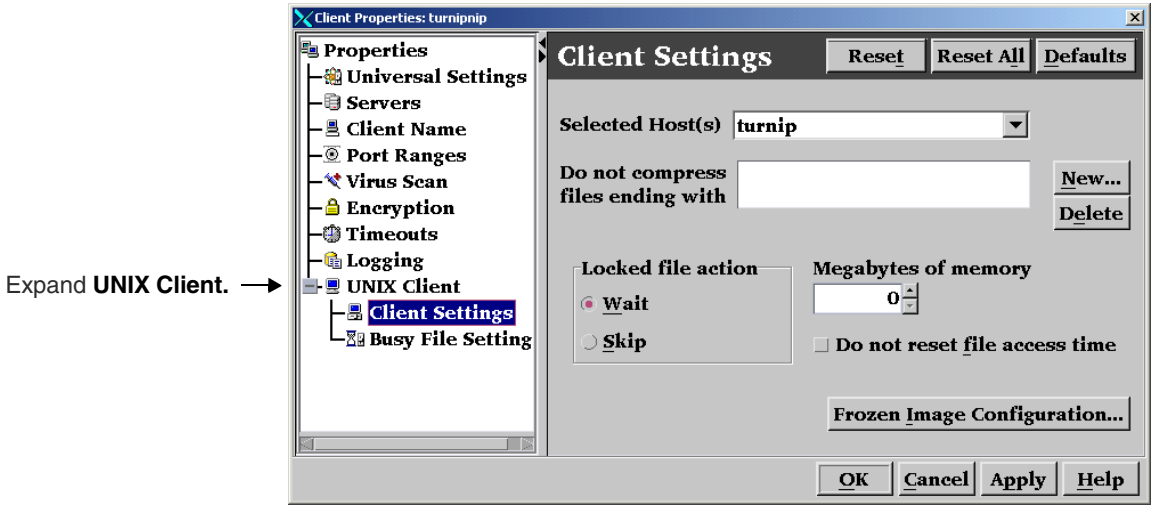
1. Start the NetBackup Administration Console by entering the following:

   ```
   /usr/openv/netbackup/bin/jnbSA &
   ```

2. Expand **Host Properties** and click on **Clients**.

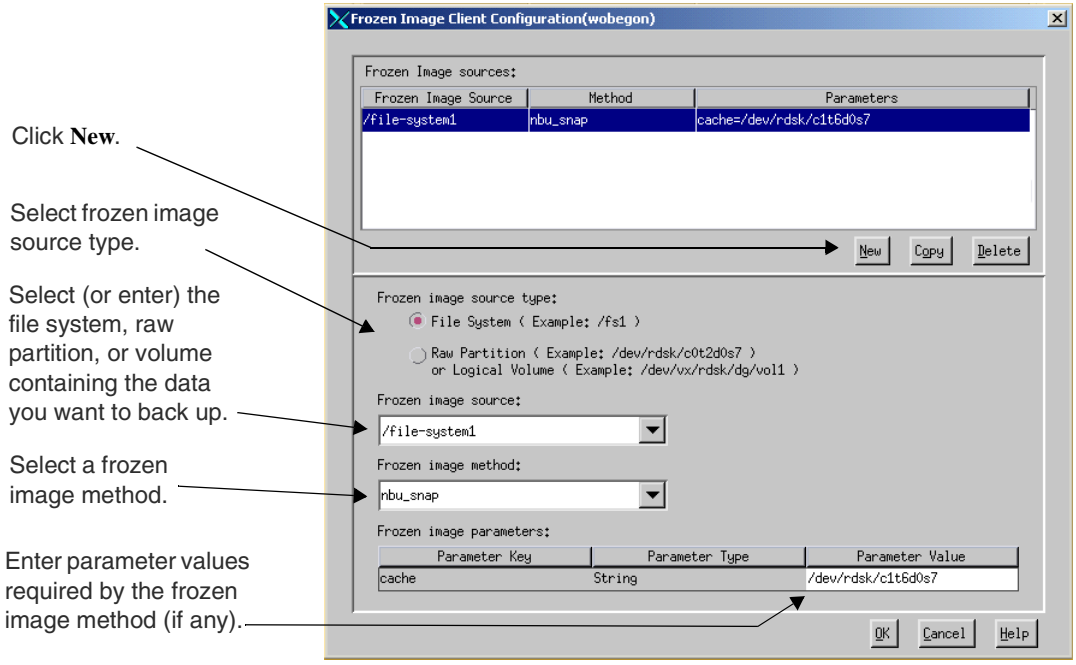
3. In the right pane, double click on the client you want to configure for frozen image backup. The Client Properties dialog appears.

4. In the left pane of the Client Properties dialog, expand **UNIX Client** and click **Client Settings**.



5. Click the **Frozen Image Configuration** button.

The Frozen Image Client Configuration dialog appears.†



6. Click **New**. A blank entry appears at the bottom of the Frozen Image Source list.

7. Select the **Frozen image source type** (file system, or raw partition or logical volume).

8. From the **Frozen image source** picklist**,** select the file system, raw partition, or Volume Manager volume. (You can also enter the name manually.) For example:

   `/file-system1` (for a file system)

   `/dev/rdsk/c0t2d0s7` (for a raw partition)

Note If the entries in the file list are regular files, the frozen image source must be the *mounted file system* that contains the files. Do not specify an individual file as the frozen image source! **For tips and examples, refer to "Frozen Image Source**" on page 81.

If you create and mount a file system after starting the NetBackup Administration Console, you must exit and restart the interface in order to select the new file system in the picklist.

†. This dialog can also be reached from the **Clients** tab of the Change Policy display.

9. Select a frozen image method from the picklist.

Note You cannot apply more than one method to the same frozen image source.

For guidance on nbu_snap, fsclone, and vxvm, refer to the "Core Frozen Image Services"chapter. For TimeFinder, ShadowImage, and BusinessCopy, refer to the "Extended Frozen Image Services (Array Integration Option)" chapter.

10. If you chose nbu_snap as the frozen image method, specify a raw partition for the snapshot cache by entering the cache partition's full path name in the **Parameter Value** field.

    For example: `/dev/rdsk/c2t0d3s3`

    Do not specify wildcards (such as `/dev/rdsk/c2*`).

Caution The partition's contents will be overwritten by the **nbu_snap** snapshot process.

11. If you chose TimeFinder, ShadowImage, or BusinessCopy as the frozen image method, specify values for the following. (Note that async_resync is also supported by the vxvm method.)

    synch_at_start: (Enter 0 or 1.) At start of backup, determines whether or not the primary and mirror devices are automatically synchronized (if they were not already synchronized) before the backup begins. Specify 1 to have unsynchronized devices synchronized before the backup begins. 0 means that unsynchronized devices will not be synchronized before the backup starts. In this case (0), if the primary and mirror devices are not synchronized, the backup will fail.

    async_resync: (Enter 0 or 1.) At end of backup, determines whether or not the backup job will wait for completion of the resync request. A value of 1 means that a resynchronize request will be issued, but the backup will not wait for the resync operation to complete. A value of 0 means that the backup job cannot reach completion status until the resynchronize operation has finished.

    Choosing 1 may allow more efficient use of backup resources. For example, if two backup jobs using Extended Frozen Image Services need the same tape drive, the second job can start even though the resync-at-end operation issued by the first job has not completed.

12. To configure another frozen image source for the client, repeat from step 6.

13. When finished configuring frozen image sources, click **OK**.

14. To configure a frozen image for another client, repeat from step 3.

Configuring a Backup Method

This procedure explains how to select a backup method for an existing NetBackup policy.

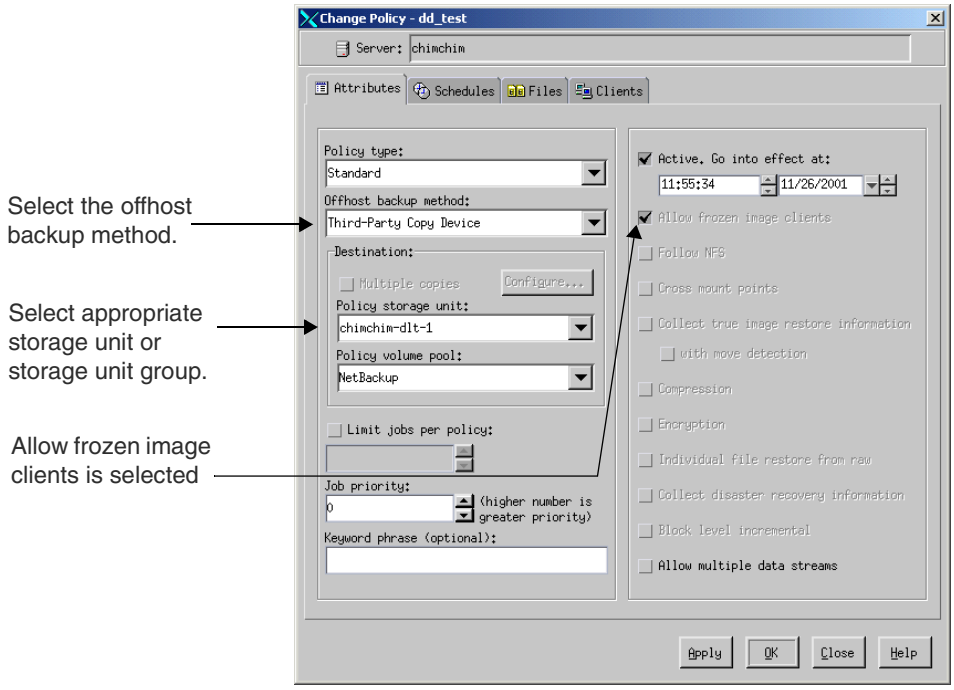
1. Start the NetBackup Administration Console by entering the following:

   `/usr/openv/netbackup/bin/jnbSA &`

2. Expand **Policies** in the left pane.

3. Double click on the name of the policy.

   The Change Policy dialog appears, showing the **Attributes** tab.



4. Choose a backup method from the **Offhost backup method** pull-down menu. For a frozen image backup that does not require offhost backup, select **Local Host**.

   These are the options for backup method:

   Local Host

   This option means no offhost backup. The backup will be done by the NetBackup client. If the NetBackup ServerFree Agent software is not installed, **Local Host** is displayed and the offhost backup menu is greyed out.

NetBackup Media Server

Backup processing will be handled offhost, by a NetBackup media server.

Third-Party Copy Device

Backup processing will be handled offhost, by a third-party copy device.

5. If you selected **Third-Party Copy Device** or **NetBackup Media Server** as the backup method, specify a particular policy storage unit or group of storage units in the **Policy storage unit** pull-down menu.

Note Do not select **Any_available**.

Instead of specifying a particular storage unit, you can create a storage unit group that designates devices configured on the SAN. Storage unit groups are described in the *NetBackup Media Manager System Administrator's Guide*.

6. If you selected **Local Host** in step 4 and you want to use a frozen image method, place a check mark beside **Allow frozen image clients**.

7. To save these settings, click **Apply**.

8. If not already done, use the **Schedules** tab to define an appropriate schedule for the policy, and use the **Files** tab to specify the files to be backed up (this defines the policy file list).

   Options for the policy schedule and file list are described in the *NetBackup DataCenter System Administrator's Guide*. These are standard NetBackup features, not new in the 4.5 release.

9. If you selected **Allow frozen image clients** or an offhost backup method (**Third-Party Copy Device** or **NetBackup Media Server**), you must configure a frozen image method. See "Configuring a Frozen Image Method" on page 76.

10. If you selected an offhost backup method (**Third-Party Copy Device** or **NetBackup Media Server**), you must also create configuration files. See Chapter 4.

Configuration Tips

Maximum Pathname Length

For frozen image backups, the maximum pathname length is 1000 characters (as opposed to 1023 characters for backups that do not use a frozen image method). This is because the frozen image is created on a new mount point which is added to the beginning of the file path. If this new mount point plus the original file path exceeds 1023 characters, the backup fails with a status code 1, "the requested operation was partially successful."

Refer to the *NetBackup DataCenter System Administrator's Guide* for other NetBackup file-path rules.

Frozen Image Source

- If the entries in the file list are regular files, specify the frozen image source as the mounted *file system* that contains the files. Do not specify an individual file as the frozen image source. See "Example 1: Basic File List Entries" on page 82. When the backup occurs, only the files in the file list are backed up, not the entire file system.
- In the file list, be sure to specify absolute path names. Refer to the *NetBackup DataCenter System Administrator's Guide for UNIX* for help specifying files in a file list.
- If the file list includes files that do NOT reside within a frozen image source, and the **Allow frozen image clients** attribute is selected, the backup will fail.
- If an entry in the file list is a symbolic (soft) link to another file, ServerFree Agent backs up the *link*, not the file to which the link points. This is standard NetBackup behavior. To back up the actual data, include the file path to the actual data in the file list. The frozen image source should be the mounted file system that contains the actual data. See "Example 2: Symbolic Links" on page 83.
- On the other hand, a raw partition can be specified in its usual symbolic-link form (such as `/dev/rdsk/c0t1d0s1`): you do not have to specify the actual device name that `/dev/rdsk/c0t1d0s1` is pointing to. For raw partitions, ServerFree Agent automatically resolves the symbolic link to the actual device.
- The **Cross mount points** policy attribute is not available for policies that are configured for frozen images. This means that NetBackup will not cross file system boundaries during a backup of a frozen image. A backup of a high-level file system, such as / (root), will not back up files residing in lower-level file systems unless those file systems are also specified as separate entries in the file list. To back up `/usr` and `/var`, for instance, both `/usr` and `/var` must be included as separate entries in the file list.

For more information on **Cross mount points**, refer to the *NetBackup DataCenter System Administrator's Guide for UNIX*.

Example 1: Basic File List Entries

Refer to the following diagram. If the policy file list contains `/usr/file1` and `/usr/file2`, specify the mounted file system `/usr` as the frozen image source. If the file list also contains `/var/config`, you must create another frozen image source that designates the mounted file system `/var`.

For volumes and raw partitions, the frozen image source should be the name of the volume or partition as it appears in the file list. For instance, if the file list contains raw disk partition `/dev/rdsk/c0t1d0s1`, create a frozen image source called `/dev/rdsk/c0t1d0s1`.

Policy: Jungle

Client: Tiger

Tiger contains these mounted file systems, Volume Manager volume, and raw partition:

/usr
/var
/dev/vx/rdsk/volgrp1/vol1
/dev/rdsk/c0t1d0s1

File list:

/usr/file1
/usr/file2
/var/config
/dev/vx/rdsk/volgrp1/vol1
/dev/rdsk/c0t1d0s1

Specify these frozen image sources:

/usr
/var
/dev/vx/rdsk/volgrp1/vol1
/dev/rdsk/c0t1d0s1

Example 2: Symbolic Links

As in standard NetBackup, if an entry in the file list is a symbolic (soft) link to another file, ServerFree Agent backs up the *link*, not the file to which the link points. To back up the file's data, the file list must also include the file path to the actual data.

Likewise, to make a frozen image of the data, the frozen image source should be the mounted file system that contains the actual data. Refer to the following diagram.

Example Symbolic Links and their Objects:

Link	Points to actual data on:
/fs1/file1	/fs2/file1
/fs1/dir1	/fs2/dir2

File list:	Specify this frozen image source:
/fs1/file1 (the link) /fs2/file1 (the data) /fs1/dir1 (the link) /fs2/dir2 (the data)	/fs2

Example 3: Multiple Clients in Policy

Policy: Jungle

Clients in this policy:

Tiger and **Lily**

Tiger contains these mounted file systems and raw partition:
/dir1
/dir2
/dev/rdsk/c0t0d0s1

Lily contains this mounted file system and Volume Manager volume:
/lily1
/dev/vx/rdsk/volgrp1/vol1

File list for policy Jungle*

/dir1
/dir2/file7
/dev/rdsk/c0t0d0s1
/lily1/file1
/dev/vx/rdsk/volgrp1/vol1

Define these frozen image sources for *Tiger*:

/dir1
/dir2
/dev/rdsk/c0t0d0s1

Define these frozen image sources for *Lily*:

/lily1
/dev/vx/rdsk/volgrp1/vol1

* Since the file list contains items that are not found on both clients, NetBackup will return status code 1, “the requested operation was partially successful.” This is normal NetBackup reporting, not specific to the 4.5 release.

Backup Policy Configuration Wizard

The Backup Policy Configuration Wizard helps you set up a basic NetBackup policy. If you used this wizard to configure a policy for NetBackup, please note the following:

- If you chose **Back up all local drives**, the wizard placed an entry called ALL_LOCAL_DRIVES in the policy file list. NetBackup 4.5 does not support the ALL_LOCAL_DRIVES option for offhost backup (either **NetBackup Media Server** or **Third-Party Copy Device**). For offhost backups, be sure to remove the ALL_LOCAL_DRIVES entry from the policy file list (use the **Files** tab on the Change Policy dialog).
- The wizard automatically sets your storage device to **Any_available**. This is correct for local backups. However, to use an offhost backup method (**Third-Party Copy Device** or **NetBackup Media Server)**, you must select a particular storage unit—do not select **Any_available**.

FlashBackup Policies

When applying a frozen image method to a client in a FlashBackup policy, note the following:

- The **nbu_snap** and **vxvm** frozen image methods are valid for clients in a FlashBackup policy. The **fsclone** frozen image method, however, is not valid for clients in a FlashBackup policy. Although the Frozen Image Client Configuration dialog allows you to select **fsclone** for such clients, the backup will fail.
- For a FlashBackup policy containing a client configured with a frozen image method as described earlier in this chapter, the file list should specify the files(s) but not the cache partition (do not include the `CACHE=` entry). For the **nbu_snap** method, the cache partition is specified in the Frozen Image Client Configuration dialog, explained under "Configuring a Frozen Image Method" on page 76.

  However, for a FlashBackup policy that does not contain any clients configured with a frozen image method, the file list must specify the files(s) AND a cache partition (the `CACHE=` entry). Refer to the *NetBackup FlashBackup System Administrator's Guide*.

Multiple Data Streams

Note Multiple data streams are not supported for the Third-Party Copy Device method.

In NetBackup, if the **Allow multiple data streams** policy attribute is selected, all streams must be set to **Active** for the backup to be successful. This means that all streams must be able to start at the same time (no backups can be queued waiting for others to complete). For backups, make sure that the following are set to allow the number of active streams to be equal to or greater than the number of streams in the file list:

- Policy attribute: **Limit jobs per policy**
- Schedule setting: **Media multiplexing**
- Storage unit setting: **Maximum multiplexing per drive**
- System configuration setting: **Maximum jobs per client**

Core Frozen Image Services 6

This chapter provides additional information about the nbu_snap, fsclone, and vxvm frozen image methods (the Core Frozen Image Services option).

The following topics are covered in this chapter:

- Core Frozen Image Services: Overview
- Creating a Snapshot Mirror of the vxvm Frozen Image Source
- Cache for nbu_snap (Parameter Value field)

Core Frozen Image Services: Overview

The following three frozen image methods require installation of the “Core Frozen Image Services” product. These methods are hardware independent: the client data may be on any disk supported by NetBackup.

- **nbu_snap** (Solaris only)

  The **nbu_snap** frozen image method is for making copy-on-write snapshot frozen images (for ufs or VERITAS VxFS file systems).

- **fsclone** (Solaris only)

  The **fsclone** frozen image method is for making copy-on-write snapshot frozen images. VERITAS Database Edition for Oracle 2.2, with VERITAS File System (VxFS) 3.4, must be installed on NetBackup clients. VERITAS recommends that the **fsclone** frozen image method only be used with Oracle databases.

  - The **fsclone** frozen image method is not supported for backing up raw partitions (whether **FlashBackup** or **Standard** policies).
  - Make sure there is enough disk space available for the clone. The file system containing the frozen image source must have at least 5% free space in order to successfully implement the clone.

- **vxvm** (Solaris or HP-UX)

  The **vxvm** frozen image method is for making mirror frozen images with VERITAS Volume Manager 3.1 or later snapshot mirrors.

  The **vxvm** frozen image method works for any file system mounted on a VxVM volume. However, before the backup is performed, the frozen image source must be configured with a VxVM 3.1 or later snapshot mirror (otherwise, the backup will fail). For help configuring a snapshot mirror, refer to “Creating a Snapshot Mirror of the vxvm Frozen Image Source” on page 89, or to your *VERITAS Volume Manager* documentation.

Note Since VxVM does not support fast mirror resynchronization on RAID-5 volumes, the **vxvm** frozen image method must not be used with VxVM volumes configured as RAID-5. If the **vxvm** frozen image method is selected for a RAID-5 volume, the backup will fail.

Creating a Snapshot Mirror of the vxvm Frozen Image Source

To use the **vxvm** frozen image method, you must create a snapshot mirror of the frozen image source before making a backup. Before specifying a frozen image source as described in this chapter, create a snapshot mirror on the client by using one of the following methods:

- In the Volume Manager Storage Administrator interface, select the volume that will be the frozen image source, right click on it, and select **Snapshot** from the pop-up menu. In the Volume Snapshot dialog, select **Enable FMR** (if available, see note below) and click the **Snapstart** button. For details, refer to the *Volume Manager Storage Administrator Administrator's Guide - Solaris*.

Or:

- Enter the following commands:

  /usr/sbin/vxassist -g *disk_group* **snapstart** *volume_name*
  /usr/sbin/vxvol -g *disk_group* **set fmr=on** *volume_name*

  where:

  - *disk_group* is the Volume Manager disk group to which the volume (frozen image source) belongs.
  - *volume_name* is the name of the volume designated at the end of the frozen image source path (for example, `vol1` in `/dev/vx/rdsk/dg/vol1`).
  - `fmr=on` sets the Fast Mirror Resynchronization attribute, which resynchronizes the mirror with its primary volume but only copies the blocks that have changed, rather than performing a full resynchronization. Fast mirror resynchronization can dramatically reduce the time required to complete the backup.

    Fast Mirror Resynchronization (FMR) is a separately available product for VERITAS Volume Manager.

Designating a frozen image source is described under "Configuring a Frozen Image Method" in the "NetBackup Configuration" chapter.

Note If an offhost backup method is used, the disks that make up the disk group must meet the requirements spelled out under "Disk Requirements for Offhost Backup" on page 122.

Cache for nbu_snap (Parameter Value field)

Note the following regarding the cache for nbu_snap, specified in the Parameter Value field of the Frozen Image Client Configuration display:

- The cache specifies a raw disk partition: either a logical volume or physical disk. This is used for storing the portions of the frozen image source that are changed by incoming write requests while the snapshot is in progress.
- Do not specify an active partition containing valuable data. Any data in that partition will be lost when the **nbu_snap** snapshot process is complete.
- Enter the full path name of the raw partition. Do not specify wildcards (such as `/dev/rdsk/c2*`) as paths.
- Specify the actual character special device file. **nbu_snap** will not work for *block* special device files.

Basic Requirements For Cache Partition

- Must reside on the same host as the frozen image source that you have specified.
- For offhost backup, the host containing the frozen image source and cache must be visible to NetBackup (refer to the chapter titled “SAN Configuration for ServerFree Agent”).
- Must be unmounted.
- Must have enough space to hold all the writes to the partition that may occur during the backup. Note that backups during nonworking hours normally require a smaller cache than a backup during peak activity.
- If an offhost backup method is used, the disk containing the cache must meet the requirements spelled out under “Disk Requirements for Offhost Backup” on page 122.

Extended Frozen Image Services (Array Integration Option) 7

This chapter provides in-depth configuration instructions for the “Extended Frozen Image Services” option (also known as the Array Integration option). These instructions are for setting up the disk arrays and configuring Volume Manager.

For help configuring a frozen image method, refer to “Configuring a Frozen Image Method” on page 76.

The following topics are covered in this chapter:

- Configuration Checklist
- Overview
- Disk Configuration Requirements
- Configuring Primary and Secondary Disks
- Volume Manager Configuration
- Best Practices
- Migrating from NetBackup for EMC

Configuration Checklist

This checklist includes major caveats and important information. READ THIS TABLE before setting up your disk arrays for Extended Frozen Image Services. The right column refers to sources for more information.

CHECK THE FOLLOWING !	Refer to these topics for help
If you want your client data configured over Volume Manager volumes, make sure your arrays and operating system are supported by Volume Manager (VxVM).	Refer to the *NetBackup Release Notes*, or go to `www.support.veritas.com` (see "ServerFree Agent Information on the Web" on page xiv).
Make sure the client data is correctly mirrored to secondary disks in the array.	See "Configuring Primary and Secondary Disks" on page 98.
When configuring a backup policy, be sure to select a frozen image method that supports your arrays.	See "The Frozen Image Methods" on page 93.
Ask your array support technician to configure your array as follows: - The NetBackup clients must have access (visibility) to primary and secondary disks in the array - The media server must have access to the secondary disks.	See "Disk Configuration Requirements" on page 96.
If you are upgrading from the NetBackup for EMC product (for NetBackup 3.4), ask your array support technician to reconfigure your arrays so that NetBackup clients have access to the primary disks AND TO THE SECONDARY disks in the array.	See "Disk Configuration Requirements" on page 96.
If client data is configured over Volume Manager volumes, label all secondary disks using the `format` command (`label` option).	See "Disk Configuration Requirements" on page 96.
Solaris: The EMC Symmetrix array must be configured in *Common Serial Number Mode* to support multiple client SCSI and / or fibre channel connections.	See "Multiple Connectivity to EMC Array: Common Serial Number mode" on page 98
Do not include secondary disks in a Volume Manager disk group. Be sure to follow this and other restrictions when using Volume Manager.	See "Disk Types" on page 111.
Read the "Best Practices" section.	See "Best Practices" on page 115.

Overview

This section describes the frozen image methods provided in the Extended Frozen Image Services option, explains the need for data mirroring, and introduces terms used in this chapter.

The Frozen Image Methods

The “Extended Frozen Image Services” option allows you to configure mirror-type frozen image backups. The client data to back up must reside on one of the following types of disk arrays: EMC Symmetrix, Hitachi Data Systems, or Hewlett Packard XP. To make the frozen image, you configure NetBackup to use one of the following methods:

- **TimeFinder**

  The **TimeFinder** frozen image method is for making mirror frozen images on EMC Symmetrix disk arrays with TimeFinder Symapi (with or without VERITAS Volume Manager 3.1 or later). Supports UFS and VxFS file systems, logical volumes, and raw partitions.

- **ShadowImage**

  The **ShadowImage** frozen image method is for making mirror frozen images on Hitachi Data Systems (HDS) disk arrays with ShadowImage (HOMRCF). Supports UFS and VxFS file systems, logical volumes, and raw partitions.

- **BusinessCopy**

  The **BusinessCopy** frozen image method is for making mirror frozen images on HP XP series disk arrays with BusinessCopy Services. Supports UFS and VxFS file systems, logical volumes, and raw partitions.

Note Select Timefinder, ShadowImage, or BusinessCopy according to the vendor-type of disk array that contains the backup data. If the frozen image method does not match the vendor-type of the array, the backup will fail.

As shown in the following table, each of these methods must be used for its own array-type.

Match Frozen Image Method to Type of Array

To Use Extended Frozen Image Services to back up the following:	Use this frozen image method:
EMC Symmetrix disk arrays	**TimeFinder**
Hitachi disk arrays	**ShadowImage**
HP XP disk arrays	**BusinessCopy**
◆ These frozen image methods cannot be switched: for example, selecting TimeFinder to back up an Hitachi array will cause the backup to fail. ◆ For the latest information on supported disk arrays and vendors, go to `support.veritas.com`. (See "ServerFree Agent Information on the Web" on page xiv for instructions.)	

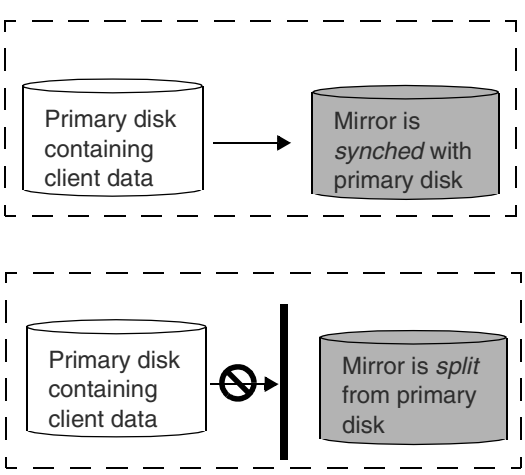
Configuration of client data over VxVM volumes is supported only on certain combinations of disk arrays and platforms. You can go to the VERITAS support web site to locate an up-do-date list of VxVM supported arrays / platforms (see "ServerFree Agent Information on the Web" on page xiv).

If client data is not configured over VxVM, all above arrays are supported (no restrictions).

Note As an alternative, the vxvm frozen image method (part of Core Frozen Image Services) can be used in backing up any of the above disk arrays on either Solaris or HP-UX, if the client data is configured over Volume Manager volumes.

Client Data Must Be Mirrored

When NetBackup makes a mirror-type frozen image, the client data on the primary disk must be mirrored on a secondary disk prior to the backup.



For mirror frozen image, client data must be on mirror disk that has been:

1, synched (brought up-to-date with primary disk)

Done by the system administrator, or by sync_at_start frozen image option. For information on sycn_at_start, see step 11 on page 78.

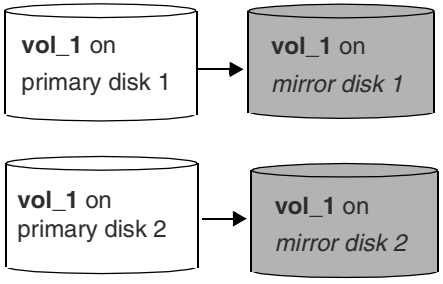
2, split (separated from primary, no further writes allowed to mirror).

Done automatically by NetBackup

If the client's data is distributed across two or more primary disks by means of a VxVM volume, an equal number of mirror disks must also contain the same data.

NetBackup client data in VxVM volumes:

where vol_1 is distributed across primary disk_1 and disk_2



Client's data must be distributed on mirror disks just as on primary disks

Disk Terms

The terms used in this manual for array disk mirroring are *primary* and *mirror* (or *primary* and *secondary*). Some array vendors refer to these as follows:

- EMC: The primary is called the *standard*, and the mirror is called a *BCV*.

- Hitachi and HP: Primary and secondary are called *primary volume* and *secondary volume*.

Disk Configuration Requirements

Contact the array's support technicians for help in configuring arrays to your specifications.

Access to Disk Arrays

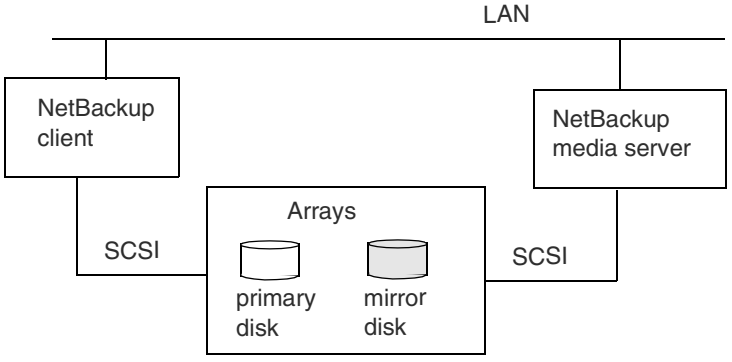
- NetBackup clients must have access to both primary and secondary disks (via SCSI or fibre channel, or both). If the clients do not have access to both primary and secondary disks, the backup will fail.
- NB media server requires access to the secondary disks only (via SCSI or fibre channel, or both). If the media server does not have access to the secondary disks, the backup will fail.

Note Although the above configuration is required by NetBackup, a support technician for your disk array vendor must configure this access.

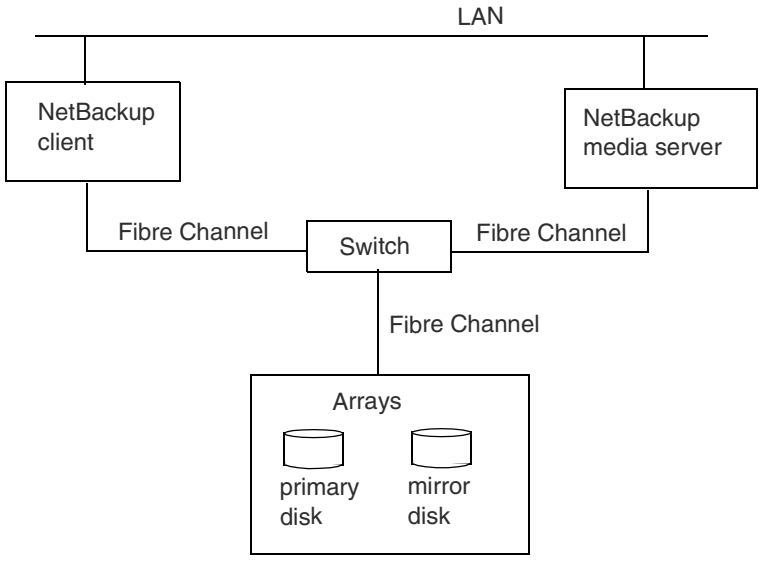
Connection to Disk Array: SCSI and Fibre Channel

NetBackup supports three configurations, each requiring setup assistance from your array vendor. Note that Fibre Channel and SCSI are both supported.

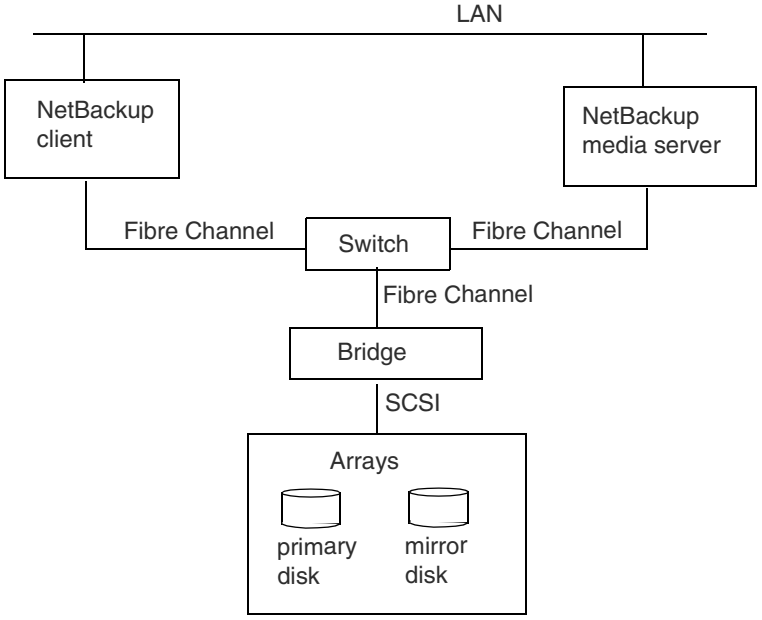
Configuration 1: Local SCSI (no Fibre Channel)



Configuration 2: Array on Fibre Channel



Configuration 3: Array Behind Bridge; Bridge on Fibre Channel



Multiple Connectivity to EMC Array: Common Serial Number mode

EMC Symmetrix disk arrays with multiple connections from NetBackup clients and media servers (multiple SCSI or both fibre channel and SCSI) must be configured in Common Serial Number Mode.

If there are multiple SCSI connections (or fibre channel and SCSI connections) to the same disks in the array, NetBackup and Volume Manager will be presented with two different serial numbers for the same disk: one for the SCSI path and one for the fibre channel path. As a result:

- Volume Manager will be confused and will not be able to run in DMP (Dynamic Multipath) mode.
- NetBackup data movement services will be confused, since the disk serial number is used to identify the proper disk to back up.

To prevent these problems, the array must be configured in Common Serial Number Mode.

Caution If Common Serial Number Mode is not configured for an EMC disk array that has multiple client and media server connections, the backup may fail.

Configuring Primary and Secondary Disks

The following is a brief listing of the commands required for making the primary-to-mirror disk association, for EMC, Hitachi, and HP arrays. The primary-to-mirror association can be set up before or after installation of NetBackup ServerFree Agent, but must be done prior to running the backup.The primary-to-mirror association is done on the NetBackup client only.

Note If a mirror disk is not correctly associated and synchronized with the primary disk, a frozen image of the client's data cannot be made. (A frozen image has to be made on the mirror, not on the primary.) In that case, if the backup policy is configured with a mirror-type frozen image, the backup will fail.

EMC Symmetrix

For an EMC Symmetrix disk array on the NetBackup client, you need to create device groups, add primary and mirror (secondary) devices to the groups, and associate or pair the primaries with the secondaries. Once associated, the secondary disks must be synchronized with the primary disks. During synchronization, the primary disks are copied to the secondaries.

Use the following commands.

Note Please refer to your EMC TimeFinder Symapi documentation for more details on these commands.

symdg

Creates a disk group.

symld

Adds primary disk to the disk group.

symbcv

Associates a secondary disk with a primary disk.

▼ Create the EMC Symmetrix disk groups

1. Create a disk group that will contain any number of primary and secondary disks.

   ```
   symdg create nbfim_test
   ```

   Creates disk group named nbfim_test.

2. Add primary disks to the disk group.

   ```
   symld -g nbfim_test add dev 02A
   ```

   Adds primary disk 02A to disk group nbfim_test.

3. Add secondary (BCV) disks to the disk group.

   ```
   symbcv -g nbfim_test associate dev 08C BCV001
   ```

   Adds the secondary disk 08C to the same disk group.

4. Synchronize the secondary disks with the primaries in the disk group.

   ```
   symmir -g nbfim_test establish
   ```


Pairs, or associates, the primary with the mirror, and synchronizes the mirror with the primary. If there are multiple primaries and mirrors, they are paired according to the order in which they were added to the group.

5. Show the output.

```
symmir -g nbfim_test query
```

When the above commands are successfully entered, NetBackup can execute frozen image requests involving primary device 02A and its associated mirror 08C.

Hitachi and HP Arrays

The procedure for setting up Hitachi arrays is identical to that for HP arrays. For more detail on the commands and files described below, refer to your Hitachi Data Systems or HP documentation.

The basic steps are these (details follow), entered on the NetBackup client only:

1. Create array configuration files.
2. Add array service names to `/etc/services` file.
3. Start the RAID Manager daemons.
4. Set the instance number and enable the listing of output.
5. View the state of the arrays.
6. Configure the arrays, depending on your requirements.

▼ Create array configuration files

You need a configuration file for each set of primary disks, and another file for each set of mirror (secondary) disks. The entries in the file must be space-delimited.

1. Create a configuration file for your primary disks. Use this path and file name:

```
/etc/horcmX.conf
```

where *X* is an integer. For example: `/etc/horcm0.conf`. This integer is called the *instance number*.

2. Create a configuration file for your mirror disks, using the same path and file name as above, but with a different instance number.

For example: `/etc/horcm1.conf`

Following are two example files. Note that entries must be separated by spaces.

Except for comment lines (#), the file must contain the HORCM_MON, HORCM_CMD, HORCM_DEV, and HORCM_INST parameters, followed by appropriate entries (explained below).

Example 1: configuration file `/etc/horcm0.conf` for three *primary* disks

Entries must be space delimited

Host where the configuration file resides.

Port name for this instance.

One line per primary disk.

Also enter this in /etc/services file

```
HORCM_MON
#host              service        poll(10ms)     timeout(10ms)
turnip             horcmgr0       1000           3000

HORCM_CMD
#cmd_dev_file            cmd_dev_file       cmd_dev_file
/dev/rdsk/c2t8d14s2

HORCM_DEV
#dev_group        dev_name       port#          TargetID       LU#     MU#
wiltest           dev1           CL1-A          8              0
wiltest           dev2           CL1-A          8              1
wiltest           dev3           CL1-A          8              2

HORCM_INST
#dev_group        partner host   partner service
wiltest           turnip         horcmgr1
```

HORCM_MON

Enter values for the following:

- host: the NetBackup client where this configuration file resides. The NetBackup client accesses the disks specified in this file under HORCM_DEV, when backing up or restoring data using the **ShadowImage** or **BusinessCopy** frozen image method.
- service: the port name of the RAID Manager instance (for this configuration file) to be registered in the /etc/services file.
- poll: the interval at which the disks are monitored, expressed as tens of milliseconds.
- timeout: time-out period for attempting to communicate with the “partner” service, expressed as tens of milliseconds.

HORCM_CMD

Enter values for the following:

- cmd_dev_file: the command device file(s) for the array. For example, /dev/rdsk/c2t8d14s2.

  You can use the NetBackup bptpcinfo command to determine the command device file, as follows:

  ```
  bptpcinfo -d /dev/rdsk -o- | grep CM
  ```

  Below is sample output showing a command device file for an Hitachi device and for an HP device.

  ```
  Command
  device files    p=/dev/rdsk/c2t8d14s2    s=HITACHI:OPEN-9-CM:60159001C00
  (note "CM"):    p=/dev/rdsk/c2t5d35s2    s=HP:OPEN-3-CM:30436002500
  ```

  The format of the output is:

  p=/dev/rdsk/c#t#d#s2 s=*VID:PID:SN*

  where:

  - VID (vendor ID) must be HP or HITACHI.
  - PID (product ID) must include -CM.
  - The first five characters of the serial number (SN) must match the serial number of the disks.

  In this example, the command device file for the Hitachi array is /dev/rdsk/c2t8d14s2 and for the HP array it is /dev/rdsk/c2t5d35s2.

HORCM_DEV

Enter values for the following:

- dev_group: a user-defined name of a logical grouping of primary and secondary disks.
- dev_name: a user-defined name assigned to a primary-secondary pair of disks within the logical group.

  The dev_group and dev_name parameters are used on the "pair" configuration commands described later in this section.

- port #: the port number specified for the disk, configured by means of the array's dedicated console (not from a NetBackup host).

- Target ID: the SCSI or fibre channel target ID number of the disk, configured by means of the array's dedicated console (not from a NetBackup host).
- LUN: the SCSI or fibre channel logical unit number of the disk, configured by means of the array's dedicated console (not from a NetBackup host).
- MU: a numeric mirror descriptor for cascading disks (default 0). If you are not using cascading disks, this value may be left blank. A cascading disk has more than one mirror (secondary) associated with a given primary.

HORCM_INST

Enter values for the following:

- dev_group: same as under HORCM_DEV.
- partner host: the host where the corresponding secondary (or primary) configuration file resides (may be the same as the host specified under HORCM_MON). For this example, the host and partner host are both turnip. (See under "partner service" for a discussion of *partner*.)
- partner service: the port name of the RAID Manager instance for the corresponding secondary (or primary) configuration file, to be registered in the /etc/services file.

  For the example /etc/horcm0.conf file, the partner service for horcmgr0 (entered under HORCM_MON, service) is horcmgr1. For the secondary-disk configuration example /etc/horcm1.conf file (below), the partner service is the opposite: horcmgr0.

  Partner is a relative term. From the viewpoint of the configuration file for the primary disks (/etc/horcm0.conf file), the *partner* file would be /etc/horcm1.conf (for the secondary disks). It is the same with partner service and partner host: each refers to the secondary from the viewpoint of the primary, or to the primary from the viewpoint of the secondary.

Note The partner service value must be entered in the /etc/services file.

Example 2: configuration file `/etc/horcm1.conf`, for three *secondary* disks

Entries must be space delimited

Contains same parameters (HORCM_MON, etc.) as in config file for primary disks. Disk-related entries refer to the secondary disks.

Port name for this instance

One line per secondary disk

Also enter this in /etc/services file

```
HORCM_MON
#host              service         poll(10ms)      timeout(10ms)
turnip             horcmgr1        1000            3000

HORCM_CMD
#cmd_dev_file            cmd_dev_file        cmd_dev_file
/dev/rdsk/c2t8d14s2

HORCM_DEV
#dev_group         dev_name        port#           TargetID        LU#     MU#
wiltest            dev1            CL2-A           16              32
wiltest            dev2            CL2-A           16              33
wiltest            dev3            CL2-A           16              34

HORCM_INST
#dev_group         partner host    partner service
wiltest            turnip          horcmgr0
```

See under first example configuration file (`/etc/horcm0.conf`) for a description of these entries.

- Add array service names to `/etc/services` file

  The values listed under "service" in the configuration files (`horcmgr1` and `horcmgr0` in the above examples) must be entered in `/etc/services` file.

- **Restart the inetd daemon**

  For example:

  ```
  kill -SIGHUP pid_of_inetd
  ```

- **Start the RAID Manager daemons**

  Enter the following command to start the RAID Manager daemons:

  ```
  /bin/horcmstart.sh x x
  ```

where x is the instance number of each configuration file. For the above example files, the command would be:

```
/bin/horcmstart.sh 0 1
```

The daemons must be running in order to configure your primary and secondary disks.

▼ Set the instance number and enable the listing of output

If you are using the Bourne shell, and the instance number for your primary disks is 0, enter the following:

```
HORCMINST=0
HORCC_MRCF=1
export HORCMINST HORCC_MRCF
```

If using the C shell, enter the following:

```
setenv HORCMINST 0
setenv HORCC_MRCF 1
```

The `HORCMINST` parameter determines three things:

- The array to which commands will be sent.
- Which disk is the primary and which is the secondary, when using the `paircreate` command (described below).
- Which disk (primary or secondary) is listed first in each pair when using the `pairdisplay` command to view the state of the arrays (described below). In this example (`HORCMINST=0`), the primaries are listed first. That is because the configuration file that defines the primary disks is named `/etc/horcm0.conf`, with 0 as the instance number.

▼ View the state of the arrays

1. To display status information on all the disks, enter the following:

   `pairdisplay -g` *groupname* `-CLI -fc`

   where *groupname* is the name specified in the configuration files under `dev_group`. CLI and fc are options:

   `-CLI` formats headers and columns in the resulting display.

   `-fc` includes the percentage of synchronization progress in the display.

   For example:

   ```
   pairdisplay -g wiltest -CLI -fc
   ```


Resulting output:

```
Group    PairVol  L/R  Port#  TID  LU-M  Seq#   LDEV#  P/S     Status %    P-LDEV#   M
wiltest  dev1     L    CL1-A  8    0  0  60159  0      P-VOL   PAIR   100  43        -
wiltest  dev1     R    CL2-A  16   32 0  60159  43     S-VOL   PAIR   100  0         -
wiltest  dev2     L    CL1-A  8    1  0  60159  1      P-VOL   PSUS   99   44        W
wiltest  dev2     R    CL2-A  16   33 0  60159  44     S-VOL   SSUS   99   1         -
wiltest  dev3     L    CL1-A  8    2  0  60159  2      SMPL      -    -    -         -
wiltest  dev3     R    CL2-A  16   34 0  60159  45     SMPL      -    -    -         -
```

2. For status information on a particular pair of disks, enter the following:

   `pairdisplay -g` *groupname* `-d` *dev_name* `[-CLI] [-fc]`

   where *dev_name* is the name specified in the configuration files under `dev_name`.

Note If no primary-secondary associations (pairings) exist, all disks are listed as SMPL in the P/S column. To create a primary-secondary pairing, see "If disks are not paired:" on page 108.

The following describes important headers in the `pairdisplay` listing.

`Group`

This is the `dev_group` name defined in the configuration file.

`PairVol`

Lists the devices by device name. In the above output, dev1 is listed twice: the first line is the primary disk, the second is the mirror (secondary). This is shown under the P/S column: P-VOL indicates the primary, S-VOL the secondary.

L/R

Indicates local or remote host, with respect to the current instance number.

`Port#`

The port number for the disk, configured by means of the array's dedicated console (not from a NetBackup host).

`TID`

The SCSI or fibre channel target ID number of the disk, configured by means of the array's dedicated console (not from a NetBackup host).

LU-M

LU indicates the SCSI or fibre channel logical unit number of the disk, configured by means of the array's dedicated console (not from a NetBackup host). M is the numeric mirror descriptor for cascading disks. A cascading disk has more than one mirror (secondary) associated with a given primary.

Seq#

This is the unit serial number of the array.

LDEV#

Logical device number of the disk.

P/S

Indicates whether or not the disk is configured in a primary-secondary pair:

- P-VOL: the disk is the primary.
- S-VOL: the disk is the secondary.
- SMPL: the disk is not paired (associated) with any other disk.

Status

Shows the current state of each disk in the array:

- PAIR: the secondary disk in the pair is synchronized with the primary.
- PSUS: the pair is split (primary disk).
- SSUS: the pair is split (secondary disk).
- COPY: a synch or split is in progress. If synchronizing, the status changes to PAIR at completion of the COPY; if splitting, the result is PSUS for primary disk, or SSUS for secondary disk.

Note If a backup is attempted while a disk is split (PSUS, SSUS), the backup fails with a status code 11. If a backup is attempted while a disk is in the COPY state, there are two possible results: if the disks synchronize (shown as PAIR), the backup proceeds; if the disks split (PSUS, SSUS), the backup fails with a status code 11.

%

Shows the percentage of the status that has completed.

P-LDEV#

The LDEV number of the "partner" disk in the pair.

M

Indicates whether the secondary is writable, as a result of being split from the primary.

▼ Configure the arrays, depending on your requirements

The next steps depend on the results of the `pairdisplay` listings and the requirements of your site.

- If all required disks are correctly paired (status of PAIR), the primary-secondary configuration is finished.
- If required disks are paired but currently split (PSUS, SSUS), or if they are not paired at all (SMPL), you must resynchronize or configure them, respectively.

Note If a mirror-type frozen image backup attempts to access a disk that is split or not paired, the backup fails with a status code 11.

- If disks are paired but need to be unpaired or otherwise reconfigured, you must split them and create a new association.

If disks are split:

1. Enter the following to resynchronize the split disks:

   ```
   pairresync -g groupname -d dev_name
   ```

   where *groupname* is the name listed under `dev_group`, and *dev_name* is the device name, as defined in the configuration files. To resynchronize the disks listed as split (PSUS, SSUS) in the above example (see "Resulting output:" on page 106), enter:

   ```
   pairresync -g wiltest -d dev2
   ```

2. Enter the following to view the result:

   ```
   pairdisplay -g wiltest -d dev2 -CLI -fc
   ```

   When the resynchronization starts, the Status column reads COPY. When it is nearly completed, the Status column reads PAIR (see the **%** column for percentage completion).

If disks are not paired:

1. Enter the following to create a pair of primary and secondary:

   ```
   paircreate -g groupname -d dev_name -vl
   ```

   where *groupname* is the name listed under `dev_group`, *dev_name* is the device name, as defined in the configuration files, and -vl specifies that the current instance number is the primary.

   To associate the `dev3` disks as a pair (the ones listed as SMPL in the above example; see "Resulting output:" on page 106), enter the following:

```
paircreate -g wiltest -d dev3 -vl
```

2. Enter the following to view the result:

   ```
   pairdisplay -g wiltest -d dev3 -CLI -fc
   ```

   When the synchronization starts, the Status column reads COPY. When it is nearly completed, the Status column reads PAIR (see the **%** column for percentage completion).

If disks are paired but need to be split or reconfigured:

1. To split the secondary disk from the primary but maintain the pair association, enter the following:

   ```
   pairsplit -g groupname -d dev_name
   ```

   where *groupname* is the name listed under `dev_group`, and *dev_name* is the device name, as defined in the configuration files. The `pairdisplay` command will show a status of PSUS and SSUS.

   For example:

   ```
   pairsplit -g wiltest -d dev1
   ```

   This splits the secondary from the primary in the `dev1` pair.

2. To split the secondary disk from the primary and remove the pair association between them, enter the following:

   ```
   pairsplit -g groupname -d dev_name -S
   ```

   where -S means break the pair association. The `pairdisplay` command will show SMPL in the P/S column for the affected disks, meaning the disks are no longer paired.

   For more information on array configuration, refer to the documentation provided by the array's vendor.

Selecting a Mirror Disk for the Backup

On Hitachi and HP disk arrays, each primary disk can have up to three secondary (mirror) disks. These are devices 0, 1, and 2. For backups configured with the ShadowImage or BusinessCopy frozen image method, you have the option of selecting which of the three mirror disks will contain the frozen image. (The default is mirror disk 0.) Unless your site has special requirements for particular mirror disks, the default should be acceptable (see following note).

Note When making a frozen image on a mirror disk, NetBackup first splits the mirror disk from the primary. If your disk configuration demands that, of the three mirror disks, one or two particular disks must remain synchronized with the primary, do not select either of those disks for the frozen image backup. On the other hand, if any of the three mirrors can be split from the primary for the brief interval required for making a frozen image, you do not need to select a mirror: the default (0) will work.

▼ To select the mirror disk

1. Make a per policy copy of the frozen image configuration file

   ```
   cp /usr/openv/netbackup/fi.conf.master_server_name
     /usr/openv/netbackup/fi.conf.master_server_name.policy_name
   ```

   This prevents the any changes made in the Frozen Image Client Configuration display from overwriting your change in this file.

2. On the NetBackup client for which the backup has been configured / whose data is being mirrored, open the following frozen image configuration file:

   ```
   /usr/openv/netbackup/fi.conf.master_server_name.policy_name
   ```

   Here is the format of the entry:

   /*frozen_image_source frozen_image_method* `mirror=[0, 1, 2]`

   For example:

   ```
   /hds_vxfs ShadowImage mirror=1
   ```

   Mirror 1 will be used for this backup instead of the default mirror 0.

   This change only affects policy named on the file created above.

Volume Manager Configuration

Disk Label

On Solaris only: If client data is configured in Volume Manager volumes, be sure to label all secondary devices using the `format` command (`label` option). Labeling the secondary disks prevents Volume Manager from marking the disks as disabled (if they are split from their primary disks) during a system reboot.

While a secondary disk is synchronized with its primary, the secondary is invisible to Volume Manager. When the secondary is split off from its primary disk, the secondary becomes visible again. If the secondaries are labeled (using the `format label` command), Volume Manager will not disable the disks when they are split.

Disk Types

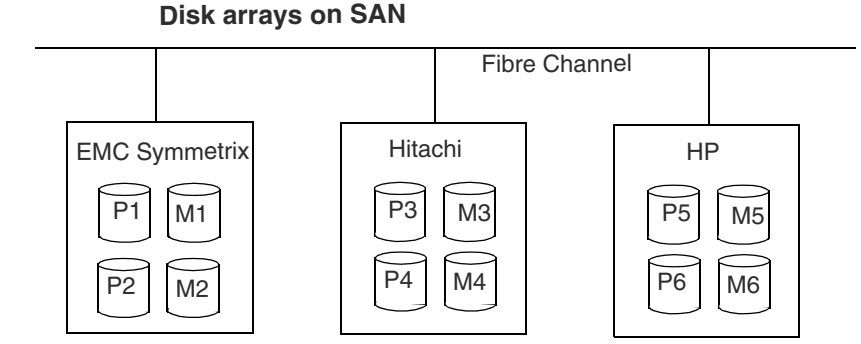
There are important restrictions involving the use of Volume Manager with NetBackup's Extended Frozen Image Services.

Note If these restrictions are not observed, the backup will fail.

- Do not include secondary (mirror) disks in a Volume Manager disk group.
- The Volume Manager disk group must contain disks of one vendor type only. Do not configure disks of different vendors in the same Volume Manager disk group.
- The vendor type of the frozen image method must match the vendor-type of the disks in the Volume Manager disk group.

Concerning these restrictions, refer to the next two diagrams.

Example VxVM Disk Groups: the Good and the Bad



P = primary disk in array

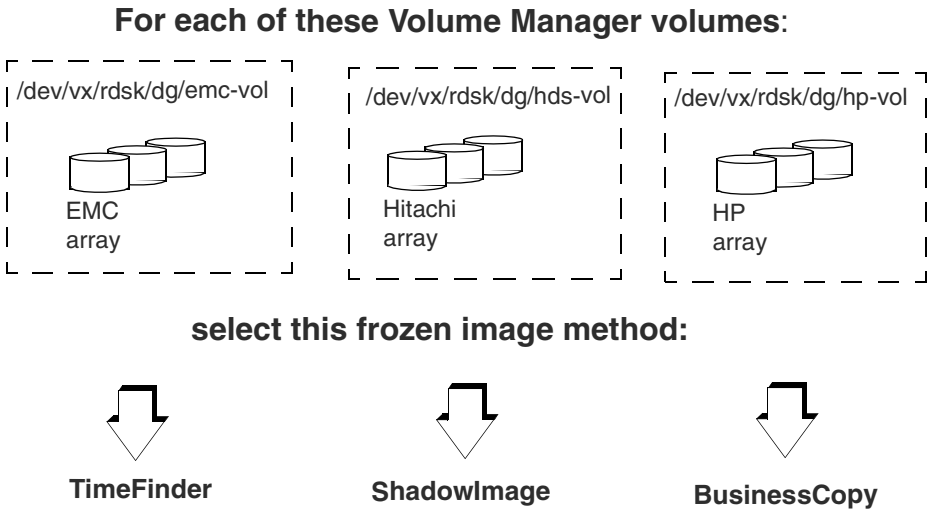
M = mirror (secondary) disk in array

Consider the following VxVM disk groups:

Disk group: P1, P2	**Good**: group contains only primary devices, of same vendor.
Disk group: P3, M3	**Bad**: group contains a secondary (mirror) disk.
Disk group: P1, P3, P5	**Bad**: group contains disks of different vendors.

As shown above, no secondary (mirror) disks should be included in VxVM disk groups, and groups must contain disks of the same vendor. These restrictions apply when using any of the Extended Frozen Image Service methods; they do NOT apply if you are using the **vxvm** frozen image method.

When Using Volume Manager and Extended Frozen Image Services



Disk Group Clones

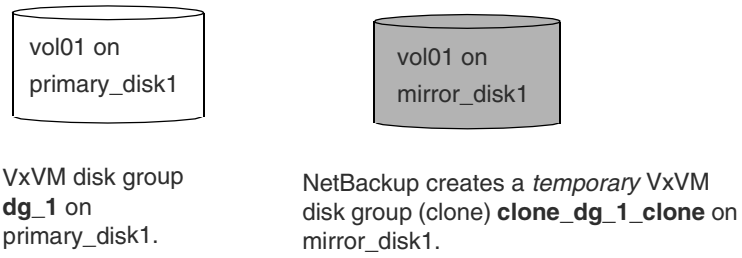
When using Extended Frozen Image Services with client data configured over a Volume Manager volume, NetBackup creates a temporary disk group (clone) of the disks containing the mirror volume. To avoid a naming conflict in the Volume Manager, NetBackup names the temporary disk group as follows:

`clone_`*`diskgroup_name`*`_clone`

While the backup is in progress, this clone appears in the output of the Volume Manager `vxdg` command. This is normal. When the backup completes, NetBackup automatically removes the disk group clone.

Disk Group Cloning Example:

Client data is in:
- file system **/fs_1**
- configured over VxVM volume **/dev/vx/rdsk/dg_1/vol01**



In the above example, NetBackup removes the VxVM disk group `clone_dg_1_clone` after the backup has completed. If a major system interruption occurs (such as a crash or unexpected reboot), NetBackup may not be able to remove the clone. In that case, you must use the `bpdgclone` command with the `-c` option to remove the clone, and then resynchronize the mirror disk with the primary disk. Refer to "Removing a VxVM Volume Clone" on page 132 for assistance.

When Secondary Disks are Split and Synched

This situation is described for your information only. A backup occurring in this circumstance should complete normally, in spite of the Volume Manager error described as follows.

When the secondary (mirror) device is split from its primary, Volume Manager will see the secondary disk as separate device. But when the secondary disk is then re-synched to its primary disk (provided Volume Manager had seen it before), the synched secondary disk is no longer visible and VxVM issues an I/O error. In addition, if DMP is enabled, the secondary disks are marked as disabled. The next time the secondary is split, it will reappear in Volume Manager, only to disappear when the disk is again synched to its primary.

Best Practices

The recommendations in this section apply primarily to the use of the Extended Frozen Image Services and Volume Manager, except where noted.

NetBackup Access to Arrays

In connection with the information listed under “Access to Disk Arrays” on page 96, note the following recommendation:

- The NetBackup media server only needs read access to the secondary disks in the array; it does not need access to the primary disks.

Resynchronizing Disks At End of Backup

Resynchronizing very large mirror disks can take time. If disk-resynchronization significantly delays completion of the backup, set the **async-resync** option to 1. This allows the backup to complete without waiting for the mirror disks to be resynchronized. The disks are resynchronized after the backup completes. Refer to step 11 on page 78 for more information on this option.

Volume Manager Disk Groups

- When creating a VxVM disk group, it is best to create a group that corresponds to the primary disks that were grouped as described under “Configuring Primary and Secondary Disks” on page 98. If you create an array disk group with two primary disks, then a VxVM disk group should be created with the same primaries. In other words, the VxVM disk group configuration should follow the array disk group configuration for the primaries.

Volume Manager with Dynamic Multipathing (DMP)

If you are using Volume Manager with DMP enabled, and there are multiple paths to the same disk array (for instance, one fibre channel connection and one SCSI), DMP will rename the array’s disks with DMP encapsulated names.

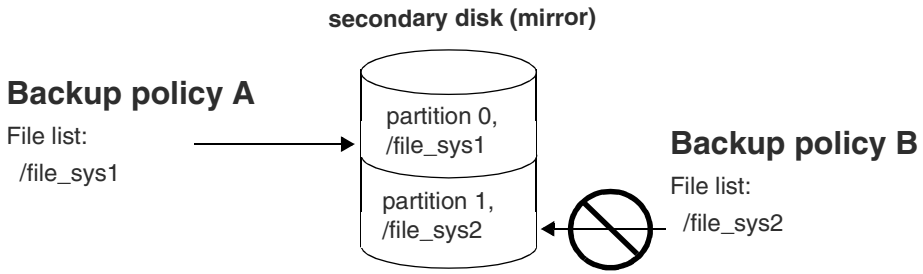
Backups Concurrently Accessing Same Disk (no VxVM)

A conflict occurs if two or more backups using Extended Frozen Image Services attempt to access a disk at the same time.

When the frozen image process is started, NetBackup reserves or “locks” the secondary (mirror) disk for that backup job, denying any other backup jobs access to that disk. If a second backup job requests a frozen image involving data on the same disk before the first job is complete, access is denied and the second job fails.

This conflict can arise when there are two backup policies, each using an Extended Frozen Image service, and each requires access to the same disk at the same time (see diagram).

Backup Policies in Conflict: Two Backups Accessing Same Disk



Backup policy A starts job to back up /file_sys1; mirror is locked to make frozen image. Backup policy B attempts to back up /file_sys2 and requests frozen image: mirror is already locked—access denied.

Note Frozen image disk locks are applied to the entire disk: when a backup job requires a frozen image, the entire disk is locked.

To avoid this conflict, see “Avoiding Concurrent Access Conflicts” later in this chapter.

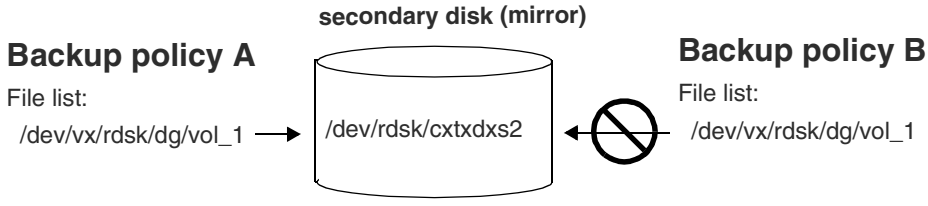
Backups Concurrently Accessing VxVM Volumes

A conflict occurs if two or more concurrent backups using Extended Frozen Image Services attempt to access data configured in the same Volume Manager volume or in volumes configured on the same disk(s).

Concurrent Access to Same VxVM Volume

In this case, a conflict occurs if two or more backups using Extended Frozen Image Services attempt to access the same Volume Manager volume at the same time.

Backup Policies in Conflict: Two Backups Accessing Same Volume



Backup policy A starts job to back up /vol_1; mirror is locked to make frozen image. Backup policy B attempts to back up /vol_1 and requests frozen image: mirror is already locked—access denied.

The above diagram shows `/dev/vx/rdsk/dg/vol_1` on a single disk. The same conflict will occur if `/vol_1` is distributed across two or more disks.

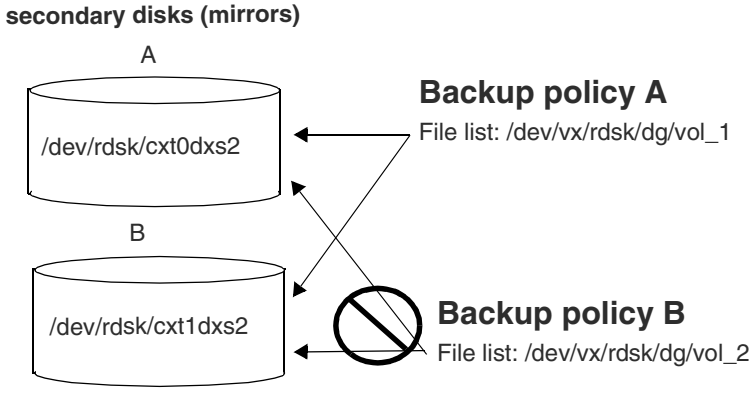
To avoid this conflict, see "Avoiding Concurrent Access Conflicts" later in this chapter.

Concurrent Access to Volume Manager Volumes on Same Disks

A conflict can occur if two or more concurrent backups using Extended Frozen Image Services attempt to access Volume Manager volumes that are distributed across the same disks.

VERITAS Volume Manager (VxVM) supports three means of distributing volumes across disks: striping, concatenating, and RAID5 (described in the Volume Manager documentation). Use of these distribution methods can lead to access problems for NetBackup Extended Frozen Image Services. The following diagram shows two VxVM volumes, `/dev/vx/rdsk/dg/vol_1` and `/dev/vx/rdsk/dg/vol_2`. Each is distributed across two disks in an array (using any of the three distribution methods). If two backups request frozen images of these volumes at the same time, a conflict occurs, even though the two backups are attempting to access different volumes. This happens because the Extended Frozen Image Services frozen image methods split the mirror disk from the primary disk at the disk device layer, not at the volume layer.

Backup Policies in Conflict: Two Backups Accessing Volume s Distributed on Same Disks



Backup policy A starts to back up /vol_1; *both disks A and B are locked* to make a frozen image of /vol_1. Backup policy B attempts to back up /vol_2 and requests frozen image: disks A and B are already locked—access denied.

Avoiding Concurrent Access Conflicts

These are recommendations for backups that encounter any of the concurrent-access problems when using Extended Frozen Image Services.

- Schedule the policies so that none can start a backup at the same time as another.
- If possible, combine the separate policies into one policy. The entries in the policy's file list will be backed up sequentially: backup of the first entry completes before the second begins. No frozen-image access conflicts can occur.
- If you want the backups to run concurrently, combine the separate policies into one and configure that policy for multiple data streaming. Multiple data streaming prevents concurrent backups from encountering frozen image conflicts. See the *NetBackup DataCenter System Administrator's Guide* for help with multiple data streams.
- If the data to back up is configured in Volume Manager (VxVM) volumes, use the vxvm frozen image method included in the Core Frozen Image Services option, rather than an Extended Frozen Image Service method. The vxvm method allows frozen image backups to run concurrently without conflicts, provided that the backup data consists of file systems mounted on VxVM volumes. See "Creating a Snapshot Mirror of the vxvm Frozen Image Source" on page 89 for help with the vxvm method.
- Use the Volume Manager administration interface to determine which disks the volumes are configured on, and configure the volumes on different disks.

Migrating from NetBackup for EMC

When upgrading from NetBackup 3.4 for EMC to Extended Frozen Image Services in NetBackup 4.5, note the following:

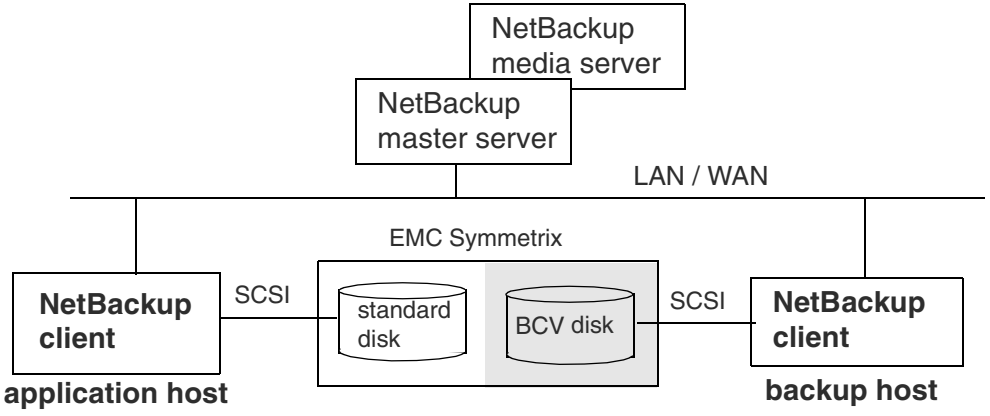
- Your NetBackup client must be reconfigured by an EMC support technician to have access to both the *primary (standard) disks AND to the secondary disks (BCVs)*. NetBackup media server needs access to only the secondary (BCV) disks.

  For the older NetBackup for EMC product, the NetBackup client that functioned as the application host needed access to the standard (primary) disks only. The NetBackup client that functioned as the backup host needed access to the BCV (secondary) disks only.

  When using Extended Frozen Image Services, if the NetBackup client does not have access to the secondary (BCV) disks, the backup will fail. Ask your array support technician to configure this access.

  The following diagrams show the old NetBackup for EMC disk access and the new disk access needed for Extended Frozen Image Services.

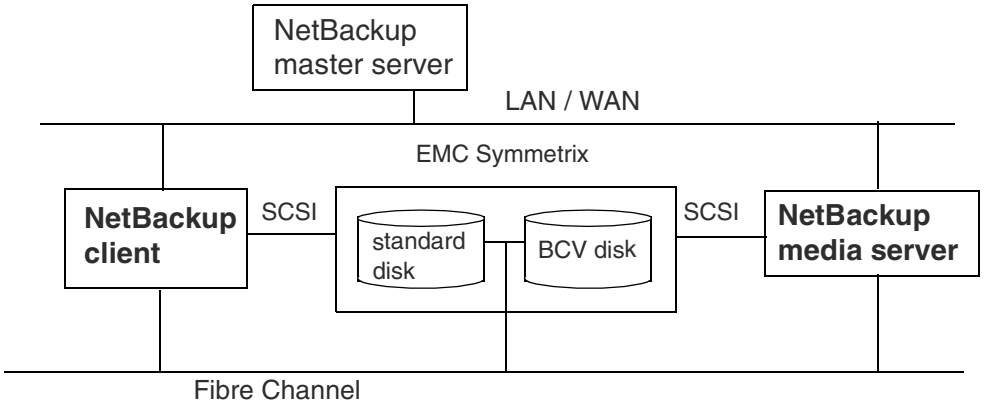
Old NetBackup for EMC Configuration: Clients Cannot Access BCVs



For old NetBackup for EMC product, clients did not need access to mirrors (BCVs).

In the following diagram, note that the machine running as the backup host is eliminated, replaced by the media server.

Extended Frozen Image Services: Clients Must Access Primary (Standard) and BCVs



For TimeFinder in NetBackup 4.5 Extended Frozen Image Services, the NetBackup client MUST HAVE ACCESS TO BCVs as well as to standard disks. NetBackup media server only needs access to the BCVs.

- When using Volume Manager volumes, configure disk groups that contain primary (standard) disks only. Do not include the secondary (BCV) disks in your Volume Manager disk groups.

  As a result, you do not need the EMC Foundation Suite for the cloning of disk groups. With the Extended Frozen Image Services option, disk group cloning is handled by NetBackup.

Notes on Offhost Backup 8

This chapter provides notes and restrictions regarding offhost (server-free) backup. For an introduction to offhost backup, refer to Chapter 1, “Introduction.”

The following topics are covered in this chapter:

- Disk Requirements for Offhost Backup
- ALL_LOCAL_DRIVES
- Multiplexing
- Raw Partition Offhost Backups

Disk Requirements for Offhost Backup

For offhost backups (**NetBackup Media Server** or **Third-Party Copy Device** offhost backup method), the client's data must be on one or more disks that meet the following criteria:

- The disk must be either a SCSI or Fibre Channel device.
- The disk must be visible to both the NetBackup client and to the NetBackup media server. The disk must be connected through a fibre channel SAN or through a disk array that has dual port SCSI connections.
- The disk must be able to return its SCSI serial number in response to a serial-number inquiry (serialization), or the disk must support SCSI Inquiry Page Code 83.

ALL_LOCAL_DRIVES

The policy's file list must not contain the ALL_LOCAL_DRIVES entry if you are using offhost backup (**NetBackup Media Server** or **Third-Party Copy Device** offhost backup method).

Multiplexing

The Third-Party Copy Device backup method is incompatible with multiplexing (the writing of two or more concurrent backup jobs to the same storage device). To prevent multiplexing on a third-party copy backup, you must set **Maximum multiplexing per drive** to 1 (on the "Add New Storage Unit" or "Change Storage Unit" dialog).

Raw Partition Offhost Backups

When entering a raw partition in the file list for an offhost backup, do not specify a *block device* as the raw partition. NetBackup 4.5 does not support offhost backups of block devices. Instead, specify the raw partition as a *character device*.

Using NetBackup 9

The following topics are covered in this chapter:

- Performing a Backup
- Performing a Restore

Performing a Backup

Note For the EMC **TimeFinder**, Hitachi **ShadowImage**, or HP **BusinessCopy** frozen image method, the client data to be backed up must reside on a mirror disk made by the corresponding vendor (EMC, Hitachi, or HP). Assistance from the disk array vendor's technical support may also be required. Refer to the chapter titled "Extended Frozen Image Services (Array Integration Option)."

Automatic Backup

The most convenient way to back up client data is to configure a Standard, FlashBackup, or Oracle policy and then set up schedules for automatic, unattended backups. To use NetBackup ServerFree Agent, you must configure a frozen image method and (optional) offhost backup method as described in the chapter titled "NetBackup Configuration." To add new schedules or change existing schedules for automatic backups, follow the guidelines in the *NetBackup DataCenter System Administrator's Guide for UNIX*.

Manual Backup

The administrator can use the NetBackup Administration interface on the master server to execute a backup for a Standard, FlashBackup, or Oracle policy. To use NetBackup 4.5 ServerFree Agent, you must configure a frozen image method and (optional) offhost backup method as described in the chapter titled "NetBackup Configuration."

See the *NetBackup DataCenter System Administrator's Guide for UNIX* for instructions on making manual backups.

User-Directed Backup and Archive

From a NetBackup 4.5 client, the user can execute a ServerFree Agent backup for a Standard or FlashBackup policy. The NetBackup administrator must configure a user-directed backup schedule, as well as a frozen image method and (optional) offhost backup method.

See the *NetBackup User's Guide for UNIX* for instructions on making user-directed backups and archives.

Performing a Restore

FlashBackup Policy

You can use the NetBackup Administration Console on the client to restore individual files or directories (or a raw partition) in a FlashBackup policy. See the *NetBackup FlashBackup System Administrator's Guide* for instructions.

Standard Policy

You can use the NetBackup Administration Console on the client to restore a file system, raw partition, or volume in a Standard policy. See the *NetBackup User's Guide* for instructions.

Troubleshooting 10

This chapter covers the following topics.

- Gathering Information and Checking Logs
- Important Notes
- Installation Problem
- Removing a Frozen Image
- Removing a VxVM Volume Clone
- VfMS Error Conditions
- Process Diagrams for Offhost Backup

Note For detailed information on the correct use of frozen images and offhost backup, refer to “Configuration Tips” in the “NetBackup Configuration” chapter.

Note For explanations of NetBackup status codes, refer to the “NetBackup Status Codes and Messages” chapter in the *NetBackup Troubleshooting Guide*.

Gathering Information and Checking Logs

You can resolve many problems on your own by setting up the appropriate logs, reproducing the problem, and then checking the logs. For an in-depth description of NetBackup logs, refer to Chapter 3 of the *NetBackup Troubleshooting Guide - UNIX*.

- To create detailed log information, put VERBOSE in the `bp.conf` file on the NetBackup master and client.

Note The directories under `/usr/openv/netbackup/logs` can eventually require a lot of disk space. Delete them when you are finished troubleshooting and remove the VERBOSE option from the `bp.conf` file.

- Backup and Debug Messages

During a backup, NetBackup ServerFree Agent messages are written to the following log directories: `online_util`, `bpbkar`, and `bptm`. Create these directories using an access mode of 755 so NetBackup can write to the logs.

`/usr/openv/netbackup/logs/online_util` (on the NetBackup client)

`/usr/openv/netbackup/logs/bpbkar` (on the NetBackup client)

`/usr/openv/netbackup/logs/bptm` (on the NetBackup media server)

- Restore Messages

During a restore, NetBackup ServerFree Agent messages are logged to the following debug logs on the master server. Create these directories using an access mode of 755.

`/usr/openv/netbackup/logs/bprestore`

`/usr/openv/netbackup/logs/bprd`

`/usr/openv/netbackup/logs/bpbrm`

`/usr/openv/netbackup/logs/bptm`

- snapctl Driver Messages

Messages from the `snapctl` driver are logged in the client's `/var/adm/messages` file along with other kernel messages.

Contacting VERITAS Customer Support

Before calling customer support, please gather as much log information as possible. Be sure to have the following information ready:

- NetBackup version
- Operating system version of the NetBackup master and media server and NetBackup ServerFree Agent client
- Note whether or not the action that failed had ever worked, and whether the problem is repeatable
- Log information

Important Notes

- The disk containing the client's data (the files to back up) must be a SCSI or Fibre Channel device if you are using offhost backup (**NetBackup Media Server** or **Third-Party Copy Device**).
- The disk containing the client's data must be visible to both the NetBackup client and the NetBackup media server if you are using offhost backup. The disk can be connected through SCSI or fibre channel.
- For offhost backup, a disk device must be able to return its SCSI serial number in response to a serial-number inquiry (serialization), or the disk must support SCSI Inquiry Page Code 83.
- When configuring offhost backup (**Third-Party Copy Device** or **NetBackup Media Server)**, a particular storage unit or group of storage units must be specified for the policy—do not choose **Any_available**. For offhost backup configuration instructions, refer to "Configuring a Backup Method" in the "NetBackup Configuration" chapter.
- The *storage_unit_name* portion of a `mover.conf.`*storage_unit_name* file name must exactly match the actual storage unit name (such as `nut-4mm-robot-tl4-0`) that you have defined for the policy. See "Naming the Mover File" on page 64 for help creating a `mover.conf.`*storage_unit_name* file.

  Similarly, the *policy_name* portion of a `mover.conf.`*policy_name* file name must match the actual name of the policy that the third-party copy device is to be associated with.
- For the **TimeFinder**, **ShadowImage**, or **BusinessCopy** frozen image methods, the client data must reside in a device group, with the data on the primary disk and synchronized with a mirror disk. Assistance from the disk array vendor may also be required. Refer to the chapter titled "Extended Frozen Image Services (Array Integration Option)."

Installation Problem

If you receive the following message during installation:

```
/usr/openv/netbackup/bin/version not found.
Add-On Product Installation Aborted.
```

you have tried to install the ServerFree Agent add-on software before installing the base NetBackup 4.5 software.

Removing a Frozen Image

NetBackup ordinarily removes frozen images after the ServerFree Agent backup completes. As a result of certain kinds of system failures, however (such as a system crash, or abnormal termination of the backup), the frozen image may not be removed.

▼ To identify and remove a left over frozen image

1. When no backups are running, enter the following:

   `df -k`

   This displays all mounted file systems, including any frozen images of a mounted file system.

Note It is important to enter `df -k` when no backups are running. If a frozen image backup is currently running, the frozen image should not be deleted. NetBackup will delete it when the backup completes.

Here are two frozen images from a `df -k` listing:

```
/dev/dsk/c1t3d2s4   1048800   73076   914742   8%   /tmp/_vrts_frzn_img__wil_vxfs_1299000
/dev/vx/dsk/clone_qes_clone/ufs 38383 21678   12867   63%   /tmp/_vrts_frzn_img__mix_ufs_1299000
```

The frozen image appears in the following form:

`/tmp/_vrts_frzn_img__`*filesystemname_pid*

2. Unmount the unneeded frozen image file system(s).

3. The next step depends on the type of frozen image.

   For nbu_snap:

   a. Enter the following to display leftover snapshots:

      `/usr/openv/netbackup/bin/driver/snaplist`

b. To remove a leftover snapshot, enter

`/usr/openv/netbackup/bin/driver/snapoff` *snap1* `...` *snapn*

For more information on the snap driver commands, refer to the "ServerFree Agent Commands" appendix of this guide.

For vxvm:

a. Enter the following to display unsynchronized mirror disks:

`vxprint -g` *diskgroup*

b. Enter the following to resynchronize the mirror disks:

`vxassist -g` *diskgroup* `-v` *volume* `snapback`

For fsclone:

a. Enter the following VxFS command to display the name of the clone (checkpoint):

`/usr/lib/fs/vxfs/fsckptadm list /`*file_system*

where *file_system* is the name of the file system where the clone is mounted (the mount point of the file system that was backed up).

b. Remove the clone by entering the following:

`/usr/lib/fs/vxfs/fsckptadm remove` *name_of_clone* */file_system*

c. If the clone cannot be removed, unmount the clone (`umount` command) and retry step b.

For more detail on removing VxFS clones, refer to the recommended actions for NetBackup status code 11 in the *NetBackup Troubleshooting Guide*.

For TimeFinder, ShadowImage, BusinessCopy:

a. To discover and remove any VxVM clones, follow the steps under "Removing a VxVM Volume Clone."

b. Enter the following to resynchronize the mirror disks:

For EMC arrays (TimeFinder):

`symmir -g` *device_group* `establish` *LdevName*

where *LdevName* is the logical device name of the standard device.

For Hitachi and HP arrays (ShadowImage, BusinessCopy):

```
pairresync -g groupname -d dev_name
```

For more information about EMC, Hitachi, and HP arrays and about resynchronizing disks, refer to the chapter "Extended Frozen Image Services (Array Integration Option)."

Removing a VxVM Volume Clone

A form of frozen image that might need manual deletion is a VxVM volume clone. See "Disk Group Clones" on page 113 for a description of disk clones.

Major system interruptions, such as a system crash or unexpected reboot, may prevent NetBackup from removing the clone. If the clone is not removed, subsequent backups of the client's data will fail with a status code 11. Examine the `/usr/openv/netbackup/logs/online_util` log for text such as the following:

```
19:13:07.686 [14981] <2> onlfi_vfms_logf: INF - do_cmd: Command failed with status=20:
/usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -f /var/tmp/HDSTFCAAs7aOqD
</dev/null >/var/tmp/VfMSAAAq7aOqD 2>/var/tmp/VfMSBAAr7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file /var/tmp/VfMSAAAq7aOqD (stdout):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- End of file /var/tmp/VfMSAAAq7aOqD
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF - --- Dumping file /var/tmp/VfMSBAAr7aOqD (stderr):
19:13:07.687 [14981] <2> onlfi_vfms_logf: INF -     clone group and volume already exists
19:13:07.688 [14981] <2> onlfi_vfms_logf: INF - --- End of file /var/tmp/VfMSBAAr7aOqD
```

In this case, you must use the `bpdgclone` command with the `-c` option to remove the clone, and then resynchronize the mirror disk with the primary disk.

▼ How to remove the clone

1. When no backups are running, use the following VxVM command to list any clones.

   ```
   vxdg list
   ```

Note If a backup configured with Extended Frozen Image Services is currently running, a clone for that backup will appear in the `vxdg` output. Do not delete the clone; NetBackup will delete it when the backup completes.

Example `vxdg` output:

```
NAME          STATE           ID
rootdg        enabled  983299491.1025.turnip
VolMgr        enabled  995995264.8366.turnip
clone_wil_test_clone enabled  1010532924.21462.turnip
wil_test      enabled  983815798.1417.turnip
```

In this example, `clone_wil_test_clone` was created for a frozen image backup that was configured with Extended Frozen Image Services. If a backup failed with log entries similar to those included above, the clone must be manually deleted.

2. To remove the clone, enter the following:

   `/usr/openv/netbackup/bin/bpdgclone -g` *disk_group* `-n` *volume* `-c`

   For the above example, you would enter:

   ```
   /usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -c
   ```

   where `wil_test` is the name of the disk group and `volo1` is the name of the VxVM volume. (Use the Volume Manager `vxprint` command to display volume names and other volume information).

   The `bpdgclone` command is described in more detail in the "ServerFree Agent Commands" appendix of this manual. For assistance with `vxprint` and other Volume Manager commands, refer to the *VERITAS Volume Manager Administrator's Guide*.

3. To verify that the clone has been removed, re-enter `vxdg list`.

   Sample output:

   ```
   NAME         STATE           ID
   rootdg       enabled  983299491.1025.turnip
   VolMgr       enabled  995995264.8366.turnip
   wil_test     enabled  983815798.1417.turnip
   ```

   The clone no longer appears in the list.

VfMS Error Conditions

Note For explanations of NetBackup error codes, refer to the "NetBackup Status Codes and Messages" chapter in the *NetBackup Troubleshooting Guide*.

For VfMS errors in the `/usr/openv/netbackup/logs/online_util` log, refer to the following for an explanation of the VfMS error codes.

VfMS Error Codes:

0 - successful

1 - vfm_init() not called

2 - feature not supported

3 - invalid file path

5 - file open failed

6 - invalid method handle

7 - file does not exist

8 - memory allocation failure

9 - miscellaneous OS error (see errno)

10 - non-fatal method error

11 - fatal method error

12 - error in dynamic library system call

13 - invalid argument

14 - one or more open file handles

15 - invalid file handle

16 - volume open failure

17 - frozen image does not exist

18 - invalid frozen image configuration parameter

19 - invalid volume path

20 - invalid method name

VfMS Method Errors

Frozen Image Method: nbu_snap

0 - no error

1 - memory allocation error

2 - error in parsing string

3 - system error

4 - cannot open snap driver

5 - cannot turn snapshot on

6 - cannot turn snapshot off

7 - invalid argument

Frozen Image Method: vxvm

0 - no error

1 - memory allocation error

2 - error in parsing string

3 - system error

4 - error opening a file

7 - invalid argument

8 - no available mirror to use as a frozen image

9 - file system resides on non-VxVM volume

10 - internal data or logic error

Frozen Image Method: fsclone

0 - no error

1 - memory allocation error

2 - invalid argument

3 - system error

Frozen Image Method: TimeFinder, ShadowImage, BusinessCopy

0 - no error

1 - memory allocation error

2 - error in parsing string

3 - system error

4 - error opening a file

5 - cannot split device

6 - cannot synchronize device

7 - invalid argument

8 - Illegal operation; invalid device

9 - Illegal operation; device is not a primary

10 - no BCV device for the standard device

11 - state of mirrored device is invalid for attempted operation

12 - General software API error

13 - Internal data or logic error

14 - Entry point not found

File Mapping Method: dsk

1 - failed to open fs_open

2 - invalid argument

3 - memory allocation error

4 - system call error

5 - read error when partitioning table

File Mapping Method: nbu_snap

1 - invalid argument

2 - map ioctl error

3 - memory allocation error

4 - system call error

5 - cannot find snapshot devices

File Mapping Method: ufs

1 - failed to open fs_open

2 - failed on fset_get

3 - invalid argument

4 - memory allocation error

5 - system call error

6 - cannot get inode information from special file

7 - file type does not match file system type

8 - map offset must be a multiple of 512

9 - file is too big

File Mapping Method: vxfs

1 - failed to open fs_open

2 - failed on fset_get

3 - invalid argument

4 - memory allocation error

5 - system call error

6 - cannot get dnode information from special file

7 - file type does not match

8 - map offset must be multiple of 512

9 - file is too big

10 - unable to open /etc/mnttab

100 - library not loadable

101 - Entry point not found

102 - library not initialized

103 - O/S call failed

104 - VxFS not installed

105 - unsupported VxFS version

File Mapping Method: vxvm

1 - memory allocation error

2 - cannot load volume database

3 - volume layout is not supported

4 - no volume for device

6 - volume not active

7 - no plex for the volume

8 - invalid argument

9 - system call error

10 - no vxvm notify received

11 - vxvm configuration call failed

12 - RAID5 in degraded mode

100 - library not loadable

101 - Entry point not found

102 - library not initialized

103 - O / S call failed

104 - VxVM not installed

105 - unsupported VxVM version

Online Services Error Codes

0 - the requested operation was successfully completed

6 - the backup failed to back up the requested files

9 - an extension package is needed, but was not installed

10 - allocation failed

11 - system call failed

12 - file open failed

13 - file read failed

14 - file write failed

20 - invalid command parameter

27 - child process killed by signal

28 - failed trying to fork a process

29 - failed trying to exec a command

35 - cannot make required directory

36 - failed trying to allocate memory

69 - invalid filelist specification

77 - execution of the specified system command returned a nonzero status

158 - failed accessing daemon lock file

227 - no entity was found

Offhost Backup and Data Movement Error Codes

9 - an extension package is needed, but was not installed

20 - invalid command parameter

21 - socket open failed

23 - socket read failed

24 - socket write failed

25 - cannot connect on socket

26 - client / server handshaking failed

43 - unexpected message received

83 - media open error

84 - media write error

154 - storage unit characteristics mismatched to request

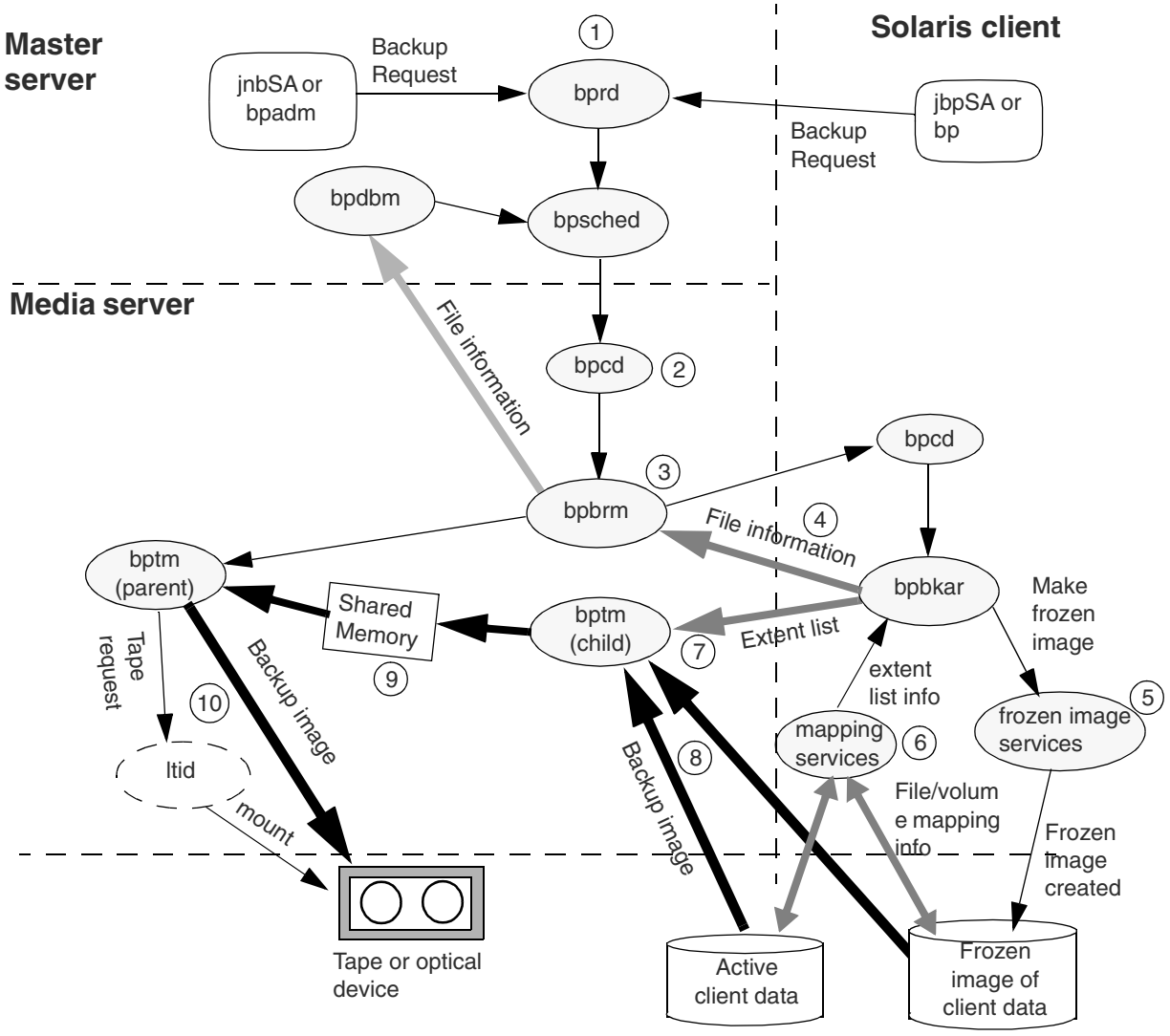
170 - third party copy backup failure

Process Diagrams for Offhost Backup

NetBackup Media Server: Copy-On-Write Process

The following diagram shows the major components for making a backup using the NetBackup Media Server method with a copy-on-write snapshot frozen image. Numbers refer to descriptions on the next page.

Overview of NetBackup Media Server Process: Copy-On-Write



1. The NetBackup master server or client initiates the backup, causing the NetBackup request daemon `bprd` to start the scheduler, `bpsched`. `bpsched` processes the policy configurations depending on the initiator of the backup (scheduled, immediate manual, or user directed). Refer to Appendix A of the *NetBackup Troubleshooting Guide* for more information on this stage of the backup operation.

2. `bpsched` uses `bpcd` (client daemon) to start the backup / restore manager (`bpbrm`) on the media server.

3. `bpbrm` starts the Media Manager process `bptm` (parent) and also starts the actual backup by using `bpcd` on the client to start the client's backup and archive program `bpbkar`.

4. `bpbkar` sends information about files within the image to the backup / restore manager `bpbrm`, which directs the file information to `bpdbm` for the NetBackup file database on the master server.

5. `bpbkar` requests creation of a frozen image of the client's active data. `bpbkar` uses the frozen image method that was configured for the frozen image source.

6. `bpbkar` requests file / volume mapping information about the client data. `bpbkar` uses one or more mapping services to decompose the client's data into physical disk addresses (also referred to as disk *extents*). The file / volume mapping information (list of extents) comes from one of two places: the client's active (primary) data, and from the frozen image of the client data (cached).

7. On the media server, `bptm` creates a child process, which reads the mapping information (extent list) from `bpbkar`.

8. Based on the extent list received from `bpbkar`, `bptm` reads the client data (backup image) from two places: from the client's active data (for those blocks that have *not* changed since the backup was initiated), and from the frozen image cache (to obtain the original contents of the blocks that *have* changed since the backup was initiated).

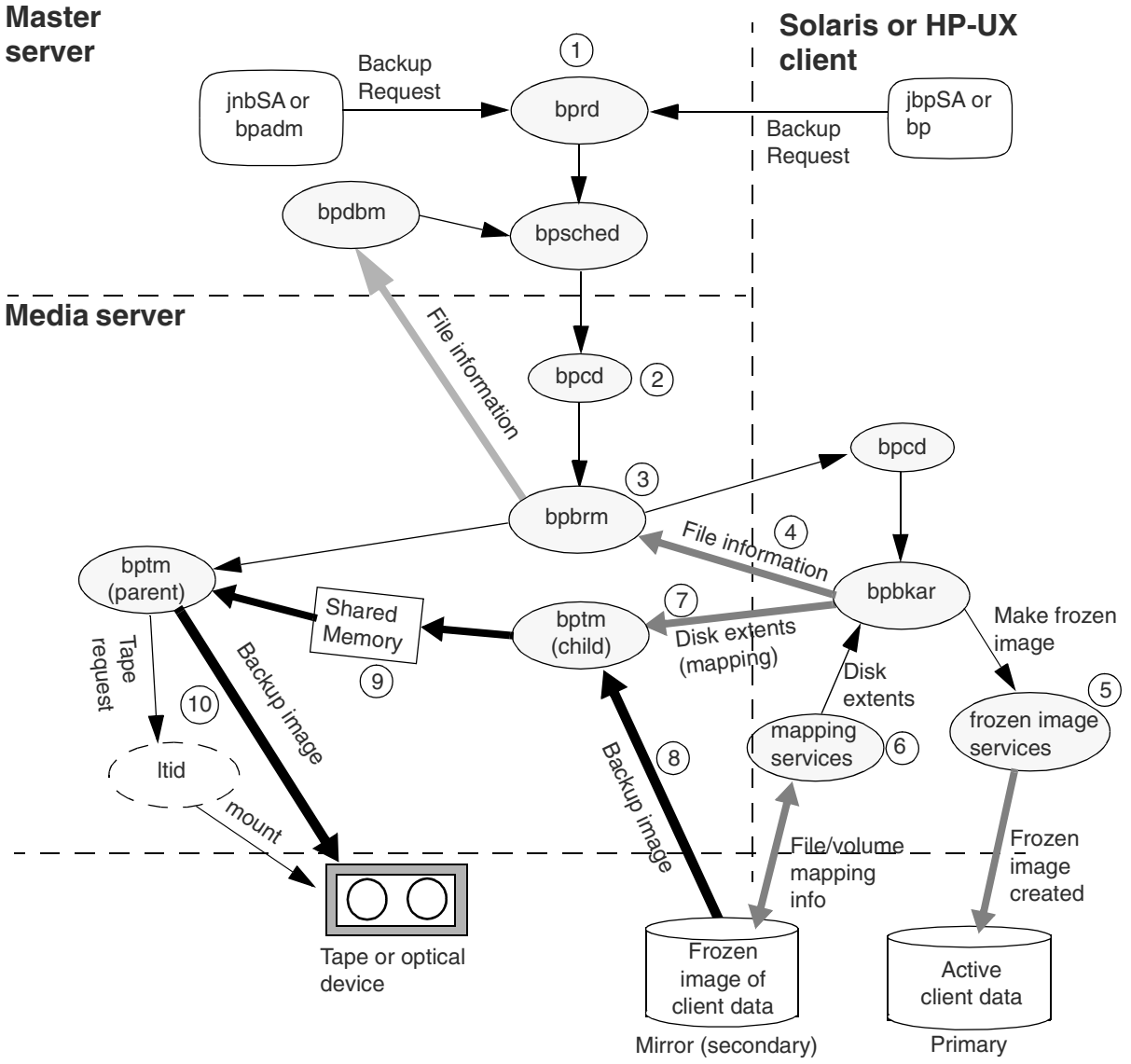
9. The `bptm` child stores the client data block-by-block in shared memory.

10. The parent `bptm` process then takes the backup image from shared memory and sends it to the storage device. For information on how the tape request is issued, refer to Appendix A of the *NetBackup Troubleshooting Guide.*

NetBackup Media Server: Mirror Process

The following diagram shows the major components for making a backup using the NetBackup Media Server method with a mirror frozen image. Numbers refer to descriptions on the next page.

Overview of NetBackup Media Server Process: Mirror



1. The NetBackup master server or client initiates the backup, causing the NetBackup request daemon bprd to start the scheduler, bpsched. bpsched processes the policy configurations depending on the initiator of the backup (scheduled, immediate manual, or user directed). Refer to Appendix A of the *NetBackup Troubleshooting Guide* for more information on this stage of the backup operation.

2. bpsched uses bpcd (client daemon) to start the backup / restore manager (bpbrm) on the media server.

3. bpbrm starts the Media Manager process bptm (parent) and also starts the actual backup by using bpcd on the client to start the client's backup and archive program bpbkar.

4. bpbkar sends information about files within the image to the backup / restore manager bpbrm, which directs the file information to bpdbm for the NetBackup file database on the master server.

5. bpbkar requests creation of a frozen image of the client's active data. bpbkar uses the frozen image method that was configured for the frozen image source.

6. bpbkar requests file / volume mapping information about the client data. bpbkar uses one or more mapping services to decompose the client's data into physical disk addresses (also referred to as disk *extents*). The file / volume mapping information (list of disk extents) comes from the frozen image of the client data.

7. On the media server, bptm creates a child process, which reads the mapping information (disk extent list) from bpbkar.

8. Based on the extent list received from bpbkar, bptm reads the client data (backup image) from the frozen image on the mirror (secondary) disk.

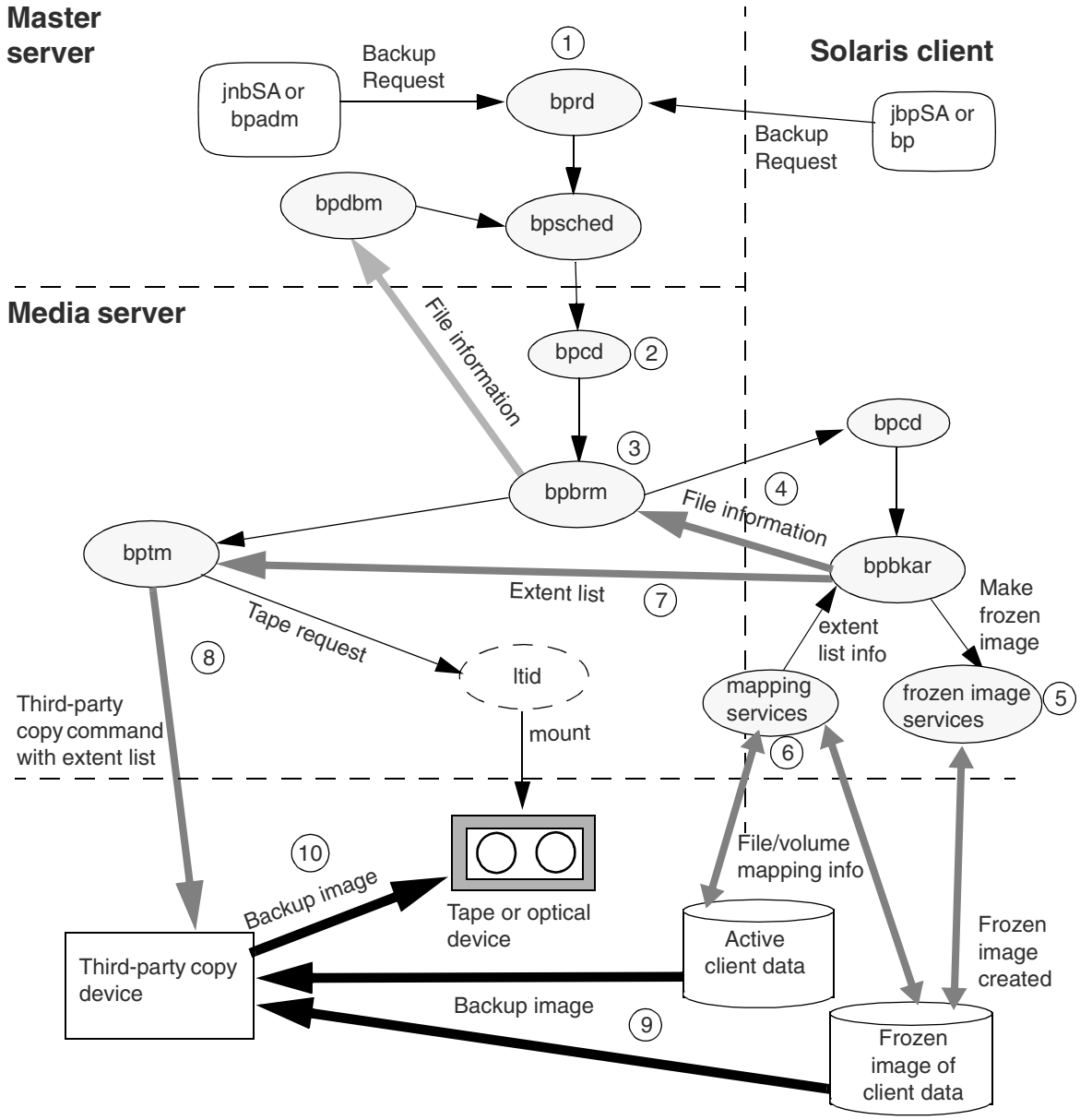
9. The bptm child stores the client data block-by-block in shared memory.

10. The parent bptm process then takes the backup image from shared memory and sends it to the storage device. For information on how the tape request is issued, refer to Appendix A of the *NetBackup Troubleshooting Guide*.

Third-Party Copy Device: Copy-On-Write Process

The following diagram shows the major components for making a backup using the NetBackup Third-Party Copy Device method with a copy-on-write snapshot frozen image. Numbers refer to descriptions on the next page.

Overview of Third-Party Copy Device Process: Copy-On-Write



1. The NetBackup server or client initiates the backup, causing the NetBackup request daemon `bprd` to start the scheduler, `bpsched`. `bpsched` processes the policy configurations depending on the initiator of the backup (scheduled, immediate manual, or user directed). Refer to Appendix A of the *NetBackup Troubleshooting Guide* for more information on this stage of the backup operation.

2. `bpsched` uses `bpcd` (client daemon) to start the backup / restore manager (`bpbrm`) on the media server.

3. `bpbrm` starts the Media Manager process `bptm` and also starts the actual backup by using `bpcd` on the client to start the client's backup and archive program `bpbkar`.

4. `bpbkar` sends information about files within the image to the backup / restore manager `bpbrm`, which directs the file information to the NetBackup file database on the master server.

5. `bpbkar` requests creation of a frozen image of the client's active data, by means of a frozen image method. `bpbkar` uses the frozen image method that was configured for the frozen image source.

6. `bpbkar` requests file / volume mapping information about the client data. `bpbkar` uses one or more mapping services to decompose the client's data into physical disk addresses (also referred to as disk *extents*). This file / volume mapping information (list of extents) comes from one of two sources: the client's active (primary) data, or from the frozen image of the client data (cached).

7. `bptm` reads the mapping information (extent list) from `bpbkar`.

8. `bptm` sends the third-party copy command with the extent list to the third-party copy device. For information on how the tape request is issued, refer to Appendix A of the *NetBackup Troubleshooting Guide*.

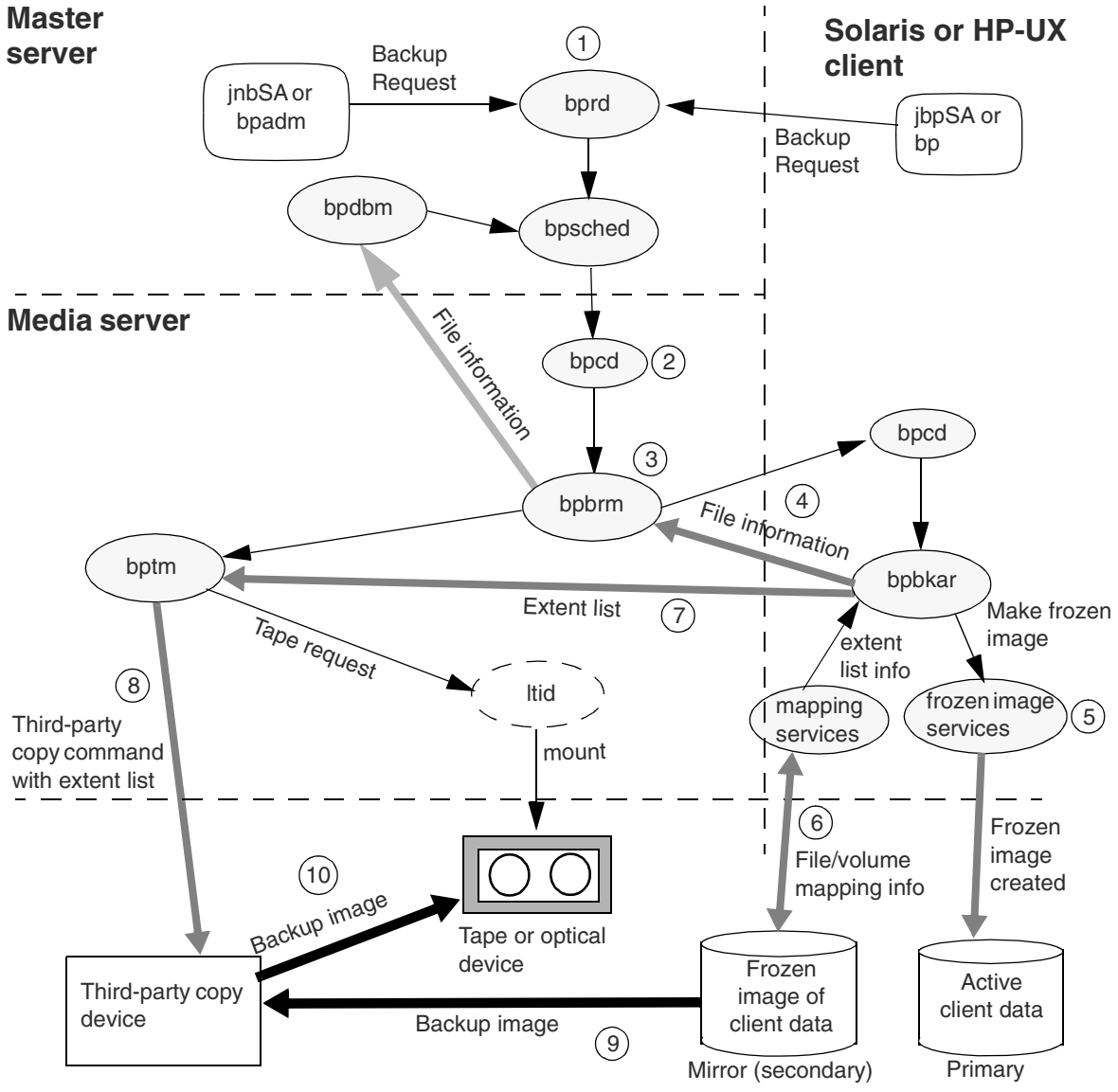
9. The third-party copy device reads the backup image (client data) from two places: from the client's active data (for those blocks that have *not* changed since the backup was initiated), and from the frozen image cache (for the original contents of the blocks that *have* changed since the backup was initiated).

10. The third-party copy device sends the backup image to the storage device.

Third-Party Copy Device: Mirror Process

The following diagram shows the major components for making a backup using the NetBackup Third-Party Copy Device method with a mirror frozen image. Numbers refer to descriptions on the next page.

Overview of NetBackup Third-Party Copy Process: Mirror



1. The NetBackup server or client initiates the backup, causing the NetBackup request daemon `bprd` to start the scheduler, `bpsched`. `bpsched` processes the policy configurations depending on the initiator of the backup (scheduled, immediate manual, or user directed). Refer to Appendix A of the *NetBackup Troubleshooting Guide* for more information on this stage of the backup operation.

2. `bpsched` uses `bpcd` (client daemon) to start the backup / restore manager (`bpbrm`) on the media server.

3. `bpbrm` starts the Media Manager process `bptm` and also starts the actual backup by using `bpcd` on the client to start the client's backup and archive program `bpbkar`.

4. `bpbkar` sends information about files within the image to the backup / restore manager `bpbrm`, which directs the file information to the NetBackup file database on the master server.

5. `bpbkar` requests creation of a frozen image of the client's active data, by means of a frozen image method. `bpbkar` uses the frozen image method that was configured for the frozen image source.

6. `bpbkar` requests file / volume mapping information about the client data. `bpbkar` uses one or more mapping services to decompose the client's data into physical disk addresses (also referred to as disk *extents*). This file / volume mapping information (list of extents) comes from the frozen image of the client data on the mirror (secondary) disk.

7. `bptm` reads the mapping information (extent list) from `bpbkar`.

8. `bptm` sends the third-party copy command with the extent list to the third-party copy device. For information on how the tape request is issued, refer to Appendix A of the *NetBackup Troubleshooting Guide*.

9. The third-party copy device reads the backup image (client data) from the frozen image on the mirror (secondary) disk.

10. The third-party copy device sends the backup image to the storage device.

ServerFree Agent Commands A

This appendix describes commands used with NetBackup ServerFree Agent.

The following are special conventions used in the command descriptions.

- Brackets [ ] mean that the enclosed command line component is optional. For example, assume that a command has the following format:

  `command [arg1]`

  The user can either choose `arg1` or omit it.

- A vertical bar (or pipe) symbol | separates optional arguments. For example:

  `command [arg1 | arg2]`

  The user can choose `arg1` or `arg2` (not both), or can omit both.

- Italics indicate that the information is user supplied. For example, the user supplies a value for *directory* in the following command:

  `-client_libraries` *directory*

bptpcinfo(1M)

NAME

bptpcinfo - discovers SAN devices and creates a `3pc.conf` file.

SYNOPSIS

```
/usr/openv/netbackup/bin/bptpcinfo [-a] [-c] [-h] [-u] [-v]
          [-x client_name] [-d disk_device_directory]
          [-t tape_device_directory] [-p physical_device]
          [-o output_file_name] [-o -]
```

DESCRIPTION

The `bptpcinfo` command lists all source and destination devices on the SAN, such as disk and tape drives and third-party copy devices, and provides information about each device (one line per device). By default, this command writes the information to the following file:

```
/usr/openv/volmgr/database/3pc.conf
```

Note For offhost backup (Third-Party Copy Device or NetBackup Media Server backup methods), a `3pc.conf` file must exist at `/usr/openv/volmgr/database`.

See the *NetBackup ServerFree Agent System Administrator's Guide* for further instructions and related information on creating the `3pc.conf` file.

OPTIONS

`-a` Discovers all devices on the fibre channel and SCSI connections. This option lists all devices in `/dev/rdsk` and `/dev/rmt`.

`-c` Checks for syntax errors in an already existing `3pc.conf` file (in `/usr/openv/volmgr/database`). If the `3pc.conf` file does not exist, a message states "cannot open file." In that case, use other options on this command to create the file. Note that if -c is specified, any other options are ignored.

The `-c` option checks for syntax errors such as missing keywords (for instance, a missing "w="), missing spaces between entries, or a world-wide name that is not 8 digits in length. Any such errors can cause the backup to fail.

`-h` Displays the `bptpcinfo` usage statement.

`-u` Discovers all devices on the fibre channel and SCSI connections, and updates the existing`3pc.conf` file. If the `3pc.conf` file does not exist, the -u option will fail (use -a instead).

`-v` Specifies verbose mode, causing `bptpcinfo` to list information on its discovery progress. The information is written to the screen, not to the `3pc.conf` file.

Note You should select the `-v` option only to track problems in device discovery and then delete that information from the `3pc.conf` file. If left in the `3pc.conf` file, the verbose information will cause the backup to fail.

`-x` *client_name*
Discovers fibre channel and SCSI devices visible to this client but not visible to the media server, and adds entries for those devices to the `3pc.conf` file on the media server. Note that you must edit the new entries in the `3pc.conf` file by adding the world-wide name (wwn=) of each device. For assistance, refer to "Create the 3pc.conf File" in the "SAN Configuration for ServerFree Agent"chapter of the *NetBackup ServerFree Agent System Administrator's Guide*.

`-d` *disk_device_directory*
Discovers all disks in the specified directory (usually `/dev/rdsk`) and fills in the values for each device (such as world-wide name and target values) depending on the options specified on this command.

`-t` *tape_device _directory*
Discovers all tape drives in the specified directory (usually `/dev/rmt`) and fills in the values for each device (such as world-wide name and target values) depending on the options specified on this command.

`-p` *physical_device*
For the specified device, this option discovers values depending on the options specified on this command (such as world-wide name and target values).

`-o` *output_file_name*
`-o` specifies an alternate (usually temporary) path for the `bptpcinfo` command output. If this option is not specified, the default is `/usr/openv/volmgr/database/3pc.conf`.

`-o -` Sends output to the screen. Note the space before the second hyphen.

EXAMPLES

Example 1

Discover all source and destination devices on the SAN and create the required `3pc.conf` file in `/usr/openv/volmgr/database`.

```
/usr/openv/netbackup/bin/bptpcinfo -a
```


Example 2

Discover all source and destination devices on the SAN, and send the output to the screen.

```
/usr/openv/netbackup/bin/bptpcinfo -a -o -
```

Sample output:

```
devid [p=devpath]      [s=sn]   [n=npid]         [l=lun]  [w=wwn]  [i=iddesc]
 0     p=/dev/rdsk/c1t4d1s2    s=SEAGATE:ST39175LW:3AL02EV300001936JL7R
l=1i=1031000005013E000D3313933364A4C3752
 1     p=/dev/rdsk/c1t11d2s2   s=IBM:DDYS-T18350N:VEY06933
l=2i=1035005076706C01B15
 2     p=/dev/rdsk/c1t11d3s2   s=SEAGATE:ST19171N:LAE82305                      l=3
 3     p=/dev/rdsk/c1t13d4s2   s=SEAGATE:ST19101W:NH022724                      l=4
 4     p=/dev/rdsk/c1t18d0s2   s=SEAGATE:ST336605FC:3FP001Z000008122HWSD
l=0i=103200000203742595A
 5     p=/dev/rdsk/c1t19d0s2   s=SEAGATE:ST336605FC:3FP003KC00008122HWD1
l=0i=1032000020374259B5
 6     p=/dev/rdsk/c1t20d0s2   s=HITACHI:OPEN-9:60159003900                     l=0
 7     p=/dev/rdsk/c1t20d1s2   s=HITACHI:OPEN-9:60159000000                     l=1
 8     p=/dev/rdsk/c1t20d2s2   s=HITACHI:OPEN-9:60159000100                     l=2
 9     p=/dev/rdsk/c1t20d3s2   s=HITACHI:OPEN-9-CM:60159001C00                  l=3
 10    p=/dev/rdsk/c1t20d4s2   s=HITACHI:OPEN-9:60159002B00                     l=4
 11    p=/dev/rdsk/c1t20d5s2   s=HITACHI:OPEN-9:60159002C00                     l=5
 12    p=/dev/rmt/0cbn s=QUANTUM:DLT8000:CX949P0164                    l=1
i=10200E09E6000000868
 13    p=/dev/rmt/1cbn s=QUANTUM:DLT8000:CX949P1208                    l=2
i=10200E09E6000001381
```

Example 3

Discover the devices in the `/dev/rmt` directory and send the output to the screen:

```
/usr/openv/netbackup/bin/bptpcinfo -t /dev/rmt -o -
```

Sample output:

```
 devid [p=devpath]      [s=sn]   [n=npid]         [l=lun]  [w=wwn]  [i=iddesc]
 0     p=/dev/rmt/0cbn s=QUANTUM:DLT8000:CX949P0164                    l=1
i=10200E09E6000000868
 1     p=/dev/rmt/1cbn s=QUANTUM:DLT8000:CX949P1208                    l=2
i=10200E09E6000001381
 2     p=/dev/rmt/4cbn s=QUANTUM:DLT8000:CX940P2790                    l=2
i=1031000005013E000D33934305032373930
 3     p=/dev/rmt/7cbn s=QUANTUM:DLT7000:TNA48S0267                    l=1
 4     p=/dev/rmt/19cbn        s=QUANTUM:DLT8000:PKB02P0989                     l=1
i=10200E09E6000030C36
 5     p=/dev/rmt/20cbn        s=QUANTUM:DLT8000:PKB02P0841                     l=2
i=10200E09E6000030DC5
```

Example 4

Create a `3pc.conf` file that describes all devices on the SAN, and send the output to an alternate file:

```
/usr/openv/netbackup/bin/bptpcinfo -a -o /usr/openv/volmgr/database/3pc_alt1.conf
```

NOTES

- The `bptpcinfo` command should be run when no backups are in progress. If a device is being used (or is reserved) by a backup, the `bptpcinfo` command may not be able to obtain information on the device, thus omitting the device from the output.
- If you do not want to overwrite the existing `3pc.conf` file, include the -o option and specify the desired location.

FILES

`/usr/openv/volmgr/database/3pc.conf`

bpmoverinfo(1M)

NAME

bpmoverinfo - discovers the third-party copy devices available on the SAN and creates a `mover.conf` file.

SYNOPSIS

```
/usr/openv/netbackup/bin/admincmd/bpmoverinfo [-u] [-h]
          [- output_file_name] [-o -]
```

DESCRIPTION

The `bpmoverinfo` command discovers the devices on the SAN that can operate as third-party copy devices (data movers), and by default writes the information to file `/usr/openv/volmgr/database/mover.conf`.

Note For offhost backup (Third-Party Copy Device backup method), a `mover.conf` file must exist at `/usr/openv/volmgr/database`.

See the *NetBackup ServerFree Agent System Administrator's Guide* for instructions on this command and for creating the `mover.conf` file.

OPTIONS

`-u` Discovers all third-party copy devices on the SAN, and updates the existing `mover.conf` file. If the `mover.conf` file does not exist, the `-u` option will fail.

`-h` Displays the `bpmoverinfo` usage statement.

`-o output_file_name`
Specifies an alternate path for the `bpmoverinfo` command output. If this option is not specified, the default is `/usr/openv/volmgr/database/mover.conf`.

`-o -` Sends output to the screen. Note the space before the second hyphen.

FILES

`mover.conf`

bpdgclone(1M)

NAME

bpdgclone - creates or removes clones of Volume Manager (VxVM) volumes.

SYNOPSIS

```
/usr/openv/netbackup/bin/bpdgclone [-h] [-v] [-c]
          -g disk_group -n volume
          [-d primary_disk,secondary_disk:primary_disk_2,secondary_disk_2:
          primary_disk_n,secondary_disk_n]
          [-f output_location]
```

DESCRIPTION

For backups using Extended Frozen Image Services, where client data is configured over a Volume Manager volume, NetBackup ServerFree Agent uses the `bpdgclone` command to create a temporary disk group or *clone* of the disk(s) containing the mirror image of the volume. To avoid a naming conflict in the Volume Manager, `bpdgclone` names the temporary disk group as follows: `clone_`*diskgroup_name*`_clone`. When the backup completes, NetBackup removes the disk group clone.

During normal operation, NetBackup calls the `bpdgclone` command as needed: no administrator use of this command is required. But if a system failure prevents NetBackup from removing the clone, you must use the `bpdgclone` command with the `-c` option to remove the clone. Then you must resynchronize the mirror disk with the primary disk.

Note If the backup has completed but the clone is not removed, subsequent backups of the client's data will fail. For assistance removing a clone, see the example below.

OPTIONS

`-g`	Specifies the name of the target disk group.
`-n`	Specifies the name of the target volume.
`-d`	Lists the primary and secondary disks. The list consists of disk pairs (primary,secondary), where the primary is separated from the secondary by a comma. If there is more than one primary disk in the target volume, the additional device pairs are separated by colons (:).
`-c`	Deletes the cloned disk group and volume. Note that the primary and secondary disks must be resynchronzied once the clone is deleted.
`-h`	Prints command usage.
`-v`	Sets verbose mode.

`-f` Specifies an output file. This file contains a list of pathnames of the primary disks over which the target volume is configured. Use this option to discover the primary disks that make up the target volume.

NOTES

- A clone should not be removed while the frozen image backup using that clone is still in progress. Barring any system failures, NetBackup will remove the clone when the backup completes.
- If you use the `bpdgclone` command to remove a left over disk clone, you must resynchronize the mirror disk with the primary disk.
- Before NetBackup executes `bpdgclone` to create the clone, NetBackup splits the secondary disk from the primary disk.

EXAMPLES

The following example removes a clone.

```
/usr/openv/netbackup/bin/bpdgclone -g wil_test -n vol01 -c
```

where `wil_test` is the name of the disk group after which the clone was named (in this example, the actual clone would be named `clone_wil_test_clone`).

For detailed assistance, refer to "Removing a VxVM Volume Clone" in the Troubleshooting chapter of the *NetBackup ServerFree Agent System Administrator's Guide*.

Solaris snapctl Driver

The snap driver is invoked by NetBackup under either of the following circumstances (Solaris systems only):

- If the **nbu_snap** frozen image method is configured for the frozen image source that is being backed up.
- If the client is in a FlashBackup policy and no frozen image method is configured (**Allow frozen image clients** on the New / Change Policy display is not checked).

A cache partition must be specified for the cache parameter in the Frozen Image Client Configuration dialog (described in the "NetBackup Configuration" chapter). The same cache can be used by any number of concurrent nbu_snap backups, as long as it is big enough.

The cache size should be approximately 10% to 15% of the total of all frozen image sources that are associated with the specific cache. This assumes no more than a moderate level of write activity during backups.

If a cache overflows, all snapshots that are using the cache will become unreadable and the backups that are reading the snapshots will fail.

snapoff

`snapoff` terminates a snapshot that was previously initiated by a backup that failed abnormally. `snapoff` must be invoked as:

`/usr/openv/netbackup/bin/driver/snapoff snap1 ... snap`*`n`*

If `snapoff` is successful, a message of the following form will be displayed:

```
snap 1 disabled
snap 2 disabled
...
snap n disabled
```

If `snapoff` fails, an explanatory message is displayed. Error codes are identified in `/usr/include/sys/errno.h`.

snaplist

This command must be invoked as:

`/usr/openv/netbackup/bin/driver/snaplist`

`snaplist` displays information about all active snapshots in the following form:

```
id  device             size   cached  cache              err time
1   /dev/rdsk/c0t3d0s0 72560  16450   /dev/rdsk/c0t4d0s0 0   12/19/99 13:23:48
```

Where:

- `size` is the size of the snapped frozen image source in 512-byte blocks.
- `cached` is the number of 512-byte blocks that have been cached (written to) for this snapshot since it was initiated.
- `err` is an error code; 0 indicates no error.

  If a snapshot has encountered an error, then `err` will be non-zero and the snapshot will be inaccessible. It can be terminated using `snapoff`. Error codes are identified in `/usr/include/sys/errno.h`. Also, error messages may be found in `/var/adm/messages`.

snapcachelist

This command must be invoked as:

`/usr/openv/netbackup/bin/driver/snapcachelist`

`snapcachelist` displays information about all partitions currently in use as snapshot caches. It is useful for monitoring the extent to which caches are full. Displayed output is of the form:

```
device               free      busy
/dev/rdsk/c0t4d0s0   238528    264472
```

Where:

- `free` is the number of 512-byte blocks available.
- `busy` is the number of 512-byte blocks that have been written to.

When a cache is full, any write to a snapped partition or snapped file system associated with that cache will cause the snapshot to fail and the snapshot will no longer be readable or writable. Reads or writes to the snapped partition will remain unaffected. The failed snapshot will not be terminated automatically and must be terminated using `snapoff` in the usual way.

Note Snapshots are initiated and terminated by NetBackup. While a backup is in progress, `snaplist` and `snapcachelist` can be used to monitor the snapshot.

Caution Do not terminate a NetBackup snapshot using `snapoff` while the backup is active because corruption of the backup image may result.

snapstat

The snapstat command must be invoked as:

```
/usr/openv/netbackup/bin/driver/snapstat
```

`snapstat` displays diagnostic information about the snap driver.

Index