hp storage

march 2003

invent

implementation blueprint

hp StorageWorks mezzanine backup-restore solution

table of contents

executive summary

This blueprint describes how to build a mezzanine backup-restore solution. The HP StorageWorks modular SAN array 1000 (msa1000) is a 2-Gb Fibre Channel storage system for the entry-level to midrange storage area network (SAN). The msa1000 provides large-capacity, low-cost storage. While the msa1000 is typically used for primary storage, it can also be used as a mezzanine solution for backup and restore, also known as disk-to-disk backups, along with a tape or library device for a full data protection solution. This feature, known as two-stage backup, uses the array as a middle-tier backup and recovery device supported with industry-standard backup and recovery software. With this solution, customers can take advantage of backing up and restoring over the SAN.

In this solution, the msa1000 storage is used by a data protection application (HP OpenView Data Protector (DP), VERITAS NetBackup (NBU) or Computer Associates BrightStor ARCserve Backup (AB) for mezzanine (near online) storage.

The intended audience consists of experienced Windows 2000 administrators who can install and configure backup applications. Administrators should also be experienced users of the data protection applications. The information in this guide will enable administrators to do the following:

- Back up data to the msa1000
- Copy backup files to tape for offline storage
- Restore from the backup files

Figure 1 presents a logical view of the mezzanine backup-restore solution.

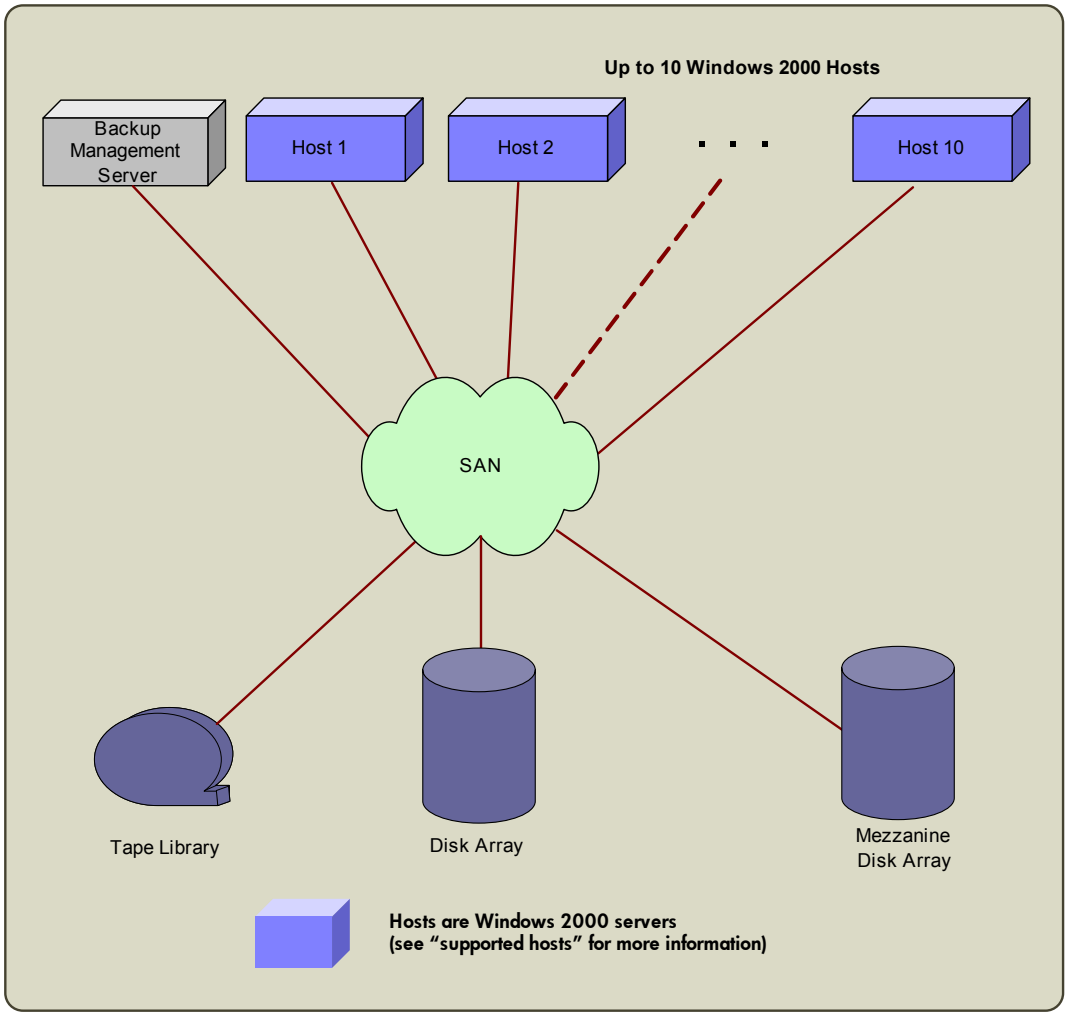

figure 1. mezzanine backup-restore solution: logical view

solution benefits

Two-stage backup using the msa1000 and tape storage addresses customers' shrinking backup windows, by using SCSI disk technology that allows for higher I/O performance and offline backup and restore. This increases overall system performance by adding high-speed targets to the backup environment. Mezzanine storage provides faster single file recovery, a reduced backup window, and increased reliability.

This mezzanine backup-restore solution blueprint provides customers with the following advantages:

- Improved backup and recovery system performance that can reduce the overall time required.
- Faster single file recovery from inexpensive, near online storage.
- Decreased backup window by distributing file backups to near online storage and tape. Disk files are then copied to tape for offline storage.
- Increased data reliability by capturing file backups to RAID-protected near online storage, where failure does not mean data loss.
- As required, offline or offsite backup files can be efficiently copied to tape.

Table 1describes three scenarios that can help you meet data protection requirements when using mezzanine storage.

table 1. scenarios for using mezzanine backup-restore solution

scenario description	backup window impact	restore time impact	best used for	notes
1. Full and incremental backups to msa1000; offline backup to tape	• Backup window reduced as additional backup resources are available • Improved reliability from RAID-protected storage	• Single file restore in milliseconds	• Operations with a fixed backup window requiring all applications to be backed up at one time • Business critical data with zero tolerance for tape error handling	• More efficient use of backup window • Tape resources can be used more hours per day
2. Weekly full backup to tape, daily incremental backups to msa1000	• Backup window reduced as additional backup resources are available • More frequent backup for frequently changing data, without changing media	• Instant access for single file restores • Improved reliability from RAID protected storage	• Large sets of data requiring frequent file restores	• Less administration required for frequent incremental backups • A large backup window is needed for weekly full backups to tape
3. Full and incremental backups to msa1000 (not recommended for a full data protection solution)	• Multi-stream host backups to disk reduce the backup window	• Instant access for full or file restores • Improved reliability from RAID protected storage	• Business requires high data reliability and instant data recovery over short periods of time	• This method requires additional processes for disaster recovery and any required data archiving or retention

solution overview

The msa1000 is a qualified mezzanine backup and restore solution that uses disk-to-disk backup technology. In the first stage of the solution, the msa1000 storage is used by a data protection application such as HP OpenView Data Protector (DP), VERITAS NetBackup (NBU) or Computer Associates BrightStor ARCserve Backup (AB) for mezzanine storage.

In the second stage of the solution, you can work offline and copy the backup files to tape resources. You create offline storage tapes without interrupting end users.

For example, an HP StorageWorks Enterprise Virtual Array (EVA) can backup data to tape resources through an HP Storage Works Network Storage Router (NSR) or to the msa1000. Using zoning and Selective Storage Presentation (SSP) in the msa1000 and the NSR, multiple hosts can be configured to use the msa1000 and NSR storage devices. While multiple hosts can share a single tape device, each Logical Unit Number (LUN) must be presented to one and only one host.

Three backup applications have been configured and verified for this solution:

- If you choose to use Data Protector, you can create a virtual jukebox. This blueprint describes how to configure Data Protector to back up to a virtual file jukebox in the msa1000 array.
- If you choose to use VERITAS NetBackup V4.5, you can create a disk storage unit.
- If you choose to use Computer Associates BrightStor ARCserve Backup (AB), you can create a File System Device.

Each of these backups points to the newly created/presented msa1000 LUN. This allows the msa1000 to act as a backup target. For example, data can be read from the source EVA and packaged and backed up to the msa1000 LUN using the logical backup device created for the msa1000 LUN.

Figure 2 displays a physical view of the mezzanine solution.

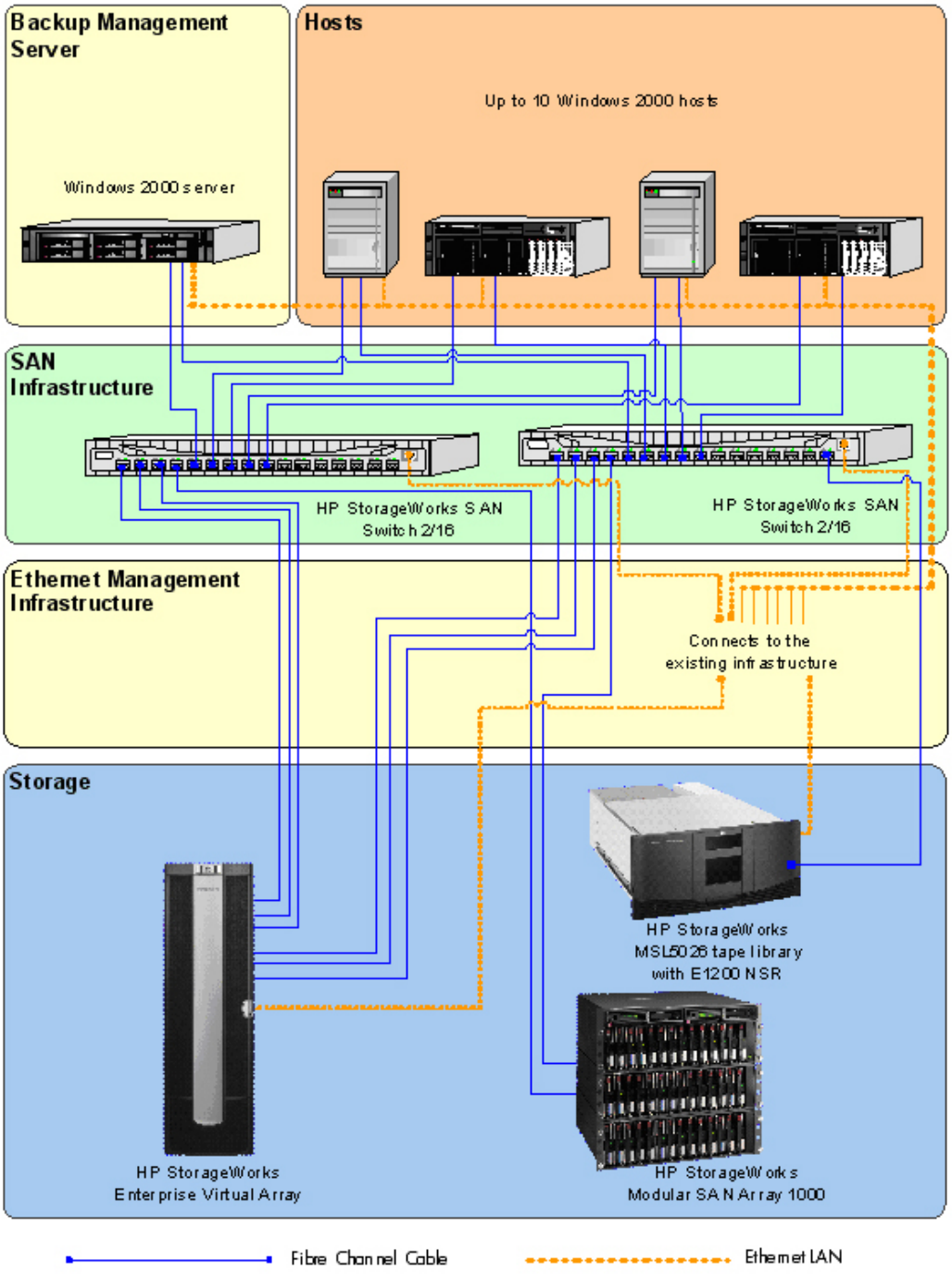

figure 2. mezzanine backup-restore solution: physical view

Ethernet connectivity provides out-of-band management for the solution components. The msa1000 is a dedicated mezzanine storage device.

how the solution works

These components work together to create the mezzanine solution.

msa1000

- Uses Selective Storage Presentation (SSP). SSP lets you assign LUNs on a storage system to one or more servers, which provides an extra level of security.
- Stores data with RAID. When using RAID ADG (Advanced Data Guarding) data is protected if two disk drives fail.
- Uses the latest industry-standard 2-Gb/s interconnects and Fibre Channel technology
- Scales to 6.0 TB, using (42) 146-GB, 1-inch Universal hard drives
- Throughput up to 200 MB/s

tape library

- An Enterprise Backup Solution (EBS)-supported MSL or ESL model tape library.

backup process

- All backups are LAN-free over the Fibre Channel fabric.

recovery process

- The primary backup copy is kept on disk. Copies made to tape are secondary copies, used for archival purposes. When the disk copy expires, the copy on tape becomes the primary backup file.

Fibre Channel infrastructure

- The SAN is operating correctly and is a known good environment before mezzanine storage is implemented.

software applications

- HP OpenView Data Protector V5, CA BrightStor ARCserve Backup V9.0, or VERITAS NetBackup V4.5

design rules

- When using multiple hosts on the msa1000, use SSP to protect LUNs. LUNs may not be shared, as shared LUNs may result in data corruption.
- Although you can configure the msa1000 with 32 LUNs, best practice advises that no more than 16 servers should access a single msa1000.
- If you use NSR, be sure to zone the NSR on the fabric. HP recommends implementing initiator-based hard zoning. Assign one host per LUN.
- A backup management server must be in place to support the solution. This server must meet the configuration requirements of the data protection application being used.

For more information on HP storage products, visit:
www.hp.com/country/us/eng/prodserv/storage.html

Figure 3 shows a sample solution racked in HP Rack 10000 Series 22U rack. The 10000 Series also includes 36U, 42U, and 47U racks. The e1200 NSR is embedded in the tape library.

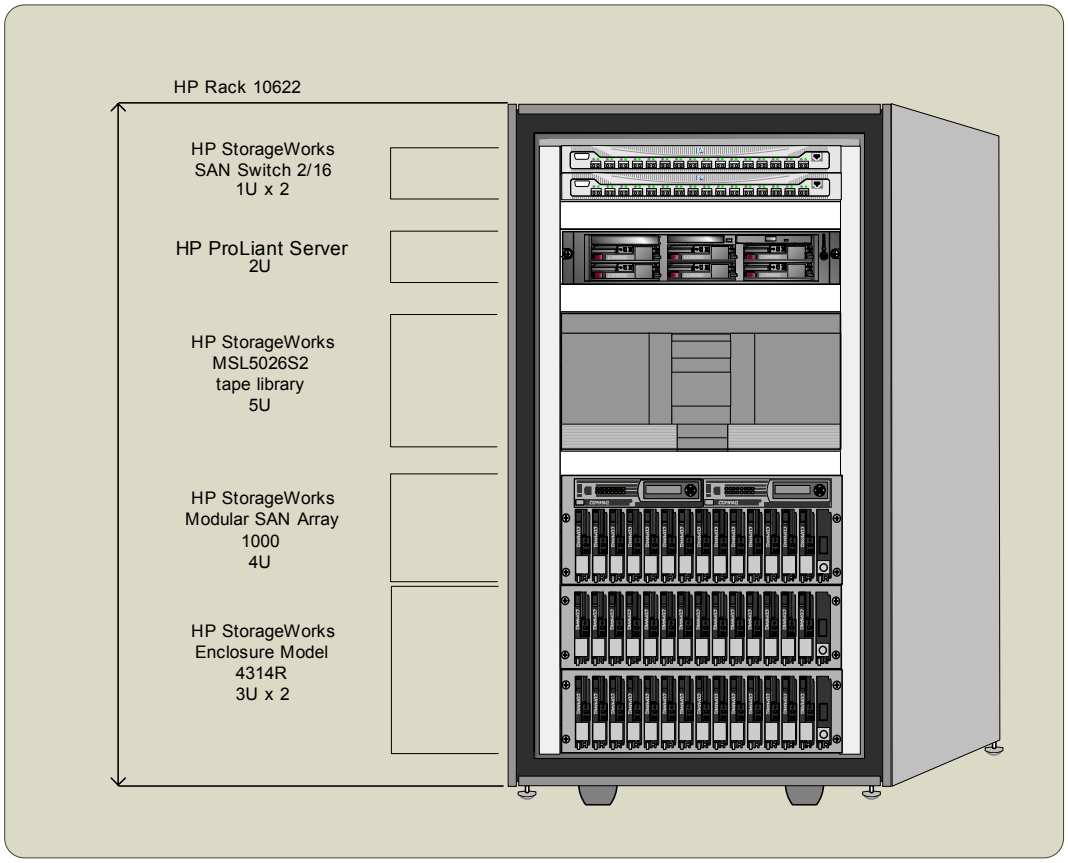

figure 3. example mezzanine backup-restore solution rack

Customers with an existing SAN and a supported ESL or MSL tape library may only need to add the msa1000 and the two 4314R enclosures.

supported hosts

supported hosts and Fibre Channel host bus adapters (HBA's)

link speed	any Windows 2000 server	any Windows 2000 advanced server
1 Gb/s or 2 Gb/s	FCA-2101 (245299-B21)	FCA-2101 (245299-B21)

interconnect

SAN Fibre Channel infrastructure

features	HP StorageWorks SAN Switch 2/8	HP StorageWorks SAN Switch 2/16
number of ports	8	16
per-port line speed	1.0625/2.125 Gb/s, Full Duplex	1.0625/2.125 Gb/s, Full Duplex
Note 1: An external FC switch must be used. The MSA Fabric Switch 6 is not supported.		
Note 2: Shaded areas represent hardware used in example technical blueprint configuration.		

storage

disk storage

features	msa1000 w/72-GB drives plus two 4200/4300 disk enclosures	msa1000 w/146-GB drives plus two 4200/4300 disk enclosures
number of msa1000 drives	14	14
number of 4200/4300 drives	28	28
total raw capacity	3.3 TB	6.6 TB
Note 1: Shaded areas represent hardware used in example technical blueprint configuration.		
Note 2: One msa1000 can support a total of two single-bus 4200/4300 disk enclosures.		

tape storage

features	HP StorageWorks MSL5026s2 tape library		HP StorageWorks MSL5030 tape library	
drive type	SDLT		LTO Ultrium	
number of drives	1	2	1	2
number of slots	26		30	
max native storage capacity	4.2 TB		3.6 TB	
max native data transfer rate	16 MB/s 57.6 GB/hr	32 MB/s 115.2 GB/hr	15 MB/s 54 GB/hr	30 MB/s 108 GB/hr
Note 1: An EBS-supported MSL or ESL model tape library is used.				
Note 2: Shaded areas represent hardware used in the example technical blueprint configuration.				

software

data protection software	**backup management server**	**host**	**description**
HP OpenView Storage Data Protector 5.0	Cell Manager	Media Agent Disk Agent	Data Protector is the only tool that integrates disk-based and tape-based recovery in a single product across multiple applications, operating systems and storage architectures.
VERITAS NetBackup Data Center 4.5 NetBackup Vault	Master Server Vault	Media Server Client	Intuitive user interfaces enable organizations to manage all aspects of backup and recovery and allow consistent backup policies to be set across the enterprise. Simplifies the management and creation of tape duplicates for offsite vaulting.
Computer Associates BrightStor ARCserve Backup for Windows 9.0 SP1	Primary Server	Distributed Server	Provides an easy-to-use interface for backup, restore, and device management. Delivers reliable recovery and backup for distributed environments.

management

msa1000 management software

management software	a SAN host	description/notes
Array Configuration Utility XE	√	Provides a graphical view of drive array configurations. Web-based ACU-XE supports online, remote Web-based, and offline configuration.
Insight Manager XE	√	Serves as a powerful storage, server, and server option management tool. Browser-based Insight Manager XE provides full access from anywhere on the intranet, eliminating the need for a dedicated Insight Manager management console.

working with HP OpenView Data Protector

This section describes how to configure Data Protector to back up data to a virtual file jukebox in an msa1000.

Data Protector supports backups to file devices in jukeboxes. The file device can be up to 2TB on Windows. The file devices used in the virtual file jukebox are the virtual tape media. A real jukebox typically has several drives. The virtual jukebox in MSA1000 uses the same concept, except that the drives are virtual.

In a virtual jukebox, a slot is actually a filename located in a specific directory or folder. The media (virtual tape) inserted into the slot has a media label that is assigned automatically by Data Protector. New media must be formatted before it can be used.

When a backup starts, Data Protector picks the free file "media" out of the available slots and fills up the file until it reaches its capacity. When the file reaches the limit and the backup requires more media, Data Protector picks the next media out of the next slot. This process continues until all the files are filled.

Before you create a virtual jukebox, you must create a dedicated media pool. In this Data Protector example, the media pool is named FileMedia.

This section includes the following instructions:

- Preparing to install
- Creating the media pool
- Creating the virtual tape library device in the msa1000
- Backing up to the virtual file jukebox in the msa1000
- Restoring from the virtual jukebox

configuring HP OpenView Data Protector

Before you begin, check the following:

- Be sure the backup management server is set up.
- Be sure LUNs are assigned on the msa1000.

This section describes how to define the following items:

- FileMediumCapacity parameter
- File devices
- Segment size
- Block size

FileMediumCapacity parameter

The default capacity is 100MB. Depending on your Data Protector setup, you may want to change this parameter to meet your requirements. For example, if you need to store more data in a file device, you could increase the capacity. The largest capacity you can specifiy is 2TB on a Windows operating system. In this example, the value for FileMediumCapacity is set to 8GB.

This parameter is defined in the global configuration file
`C:\Program Files\Omniback\Config\Options\Global`

File Devices

Data Protector does not support compressed files for file devices. Before you configure a file device on a Windows operating system, check that the file compression option is disabled. Here are the steps:

1. Using **Windows Explorer**, right-click the slot filename.
2. Select **Properties**.
3. Select **Attributes > Advanced**.
4. Click to clear **compress contents to save disk space**. If **compress** is selected, Data Protector cannot write to the file device.

Segment Size

Be sure to specify the proper segment size for a file device. Data Protector can run out of space on a file device even if there is still free space available.

1. Using Data Protector, choose **Devices and Media** from the **Context** drop-down menu.
2. Double-click **Devices**.
3. Select a drive and right-click.
4. Select **Properties**.
5. Choose the **Settings tab.**
6. Click **Advanced.**
7. Select the **Sizes tab**.

The default value of the segment size is 30MB. If the file device is bigger than 7GB, be sure to change the segment size to 100MB.

Here is a table with recommended segment sizes for some file device sizes.

File size (GB)	Segment size (MB)
< 7	30
< 16	100

Refer to the Data Protector Administrator's Guide for more information.

Block Size

You can specify the block size for a file device.

1. Using Data Protector, choose **Devices and Media** from the **Context** drop-down menu.
2. Double-click **Devices**.
3. Select a drive and right-click.
4. Select **Properties**.
5. Choose the **Settings tab.**
6. Click **Advanced.**
7. Select the **Sizes** tab**.**

Be sure to configure virtual drives with the same block size to ensure that virtual media (file device) is compatible.

creating the media pool

In this example, the following steps describe how to create the media pool.

1. Launch Data Protector. The following screen is displayed.

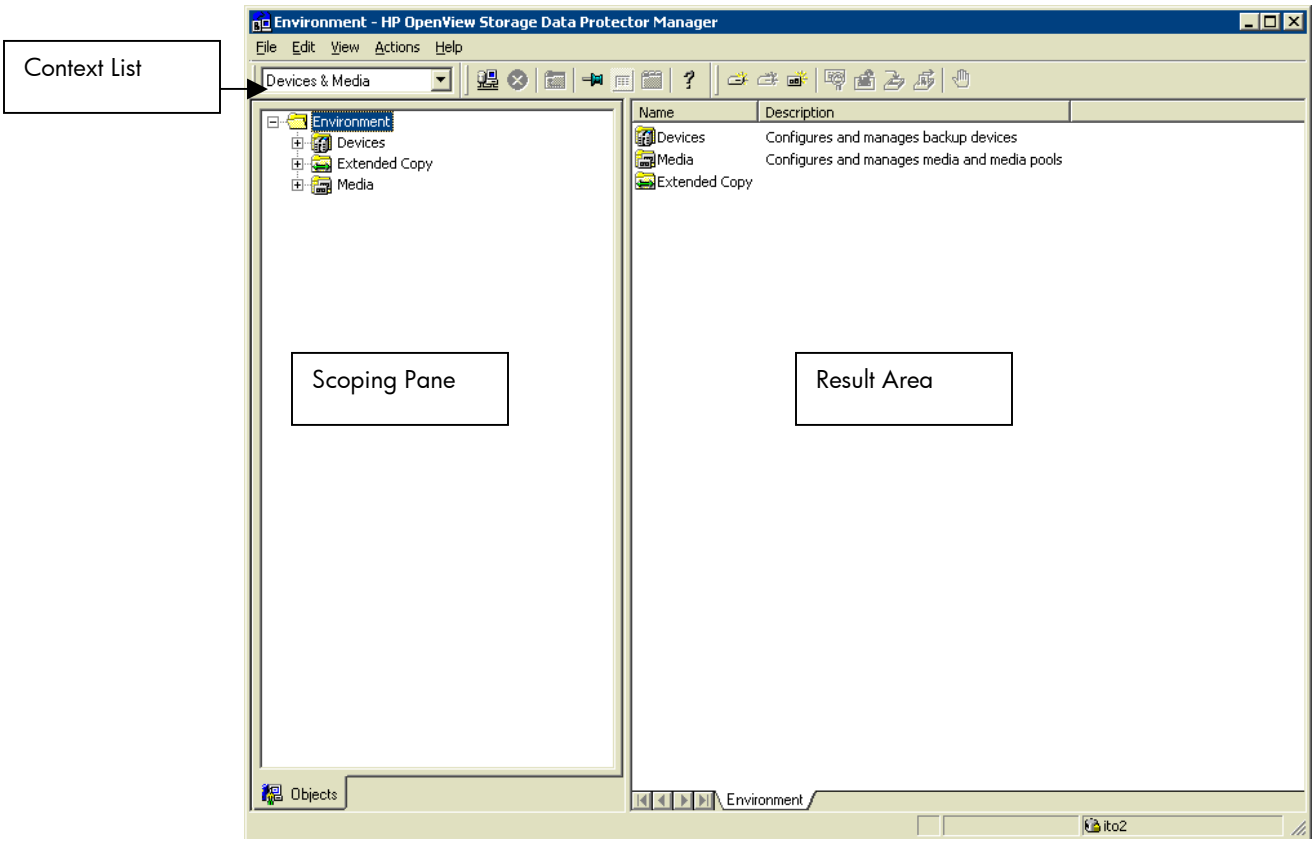

figure 4. HP Data Protector main screen

.

2. Choose **Devices and Media** from the **Context** drop-down menu. The **Environment** folder is displayed.
3. Right-click **Media** in the **Scoping Pane**.
4. Click **Add Media Pool**.
5. Enter **FileMedia** in the **Pool Name** field.
6. Select **File** from the drop-down menu in the **Media Type** box.
7. Click **Next**.
8. Use the default settings for the **Allocation Policies** dialog box. Refer to the Data Protector Administrator Guide if you want to choose different settings.
9. Click **Next**.
10. Use the default settings for the **Media Condition Factors** dialog box. Refer to the Data Protector Administrator Guide if you want to choose different settings.
11. Click **Finish**. The screen looks similar to figure 5. Notice the new media pool called **FileMedia**.

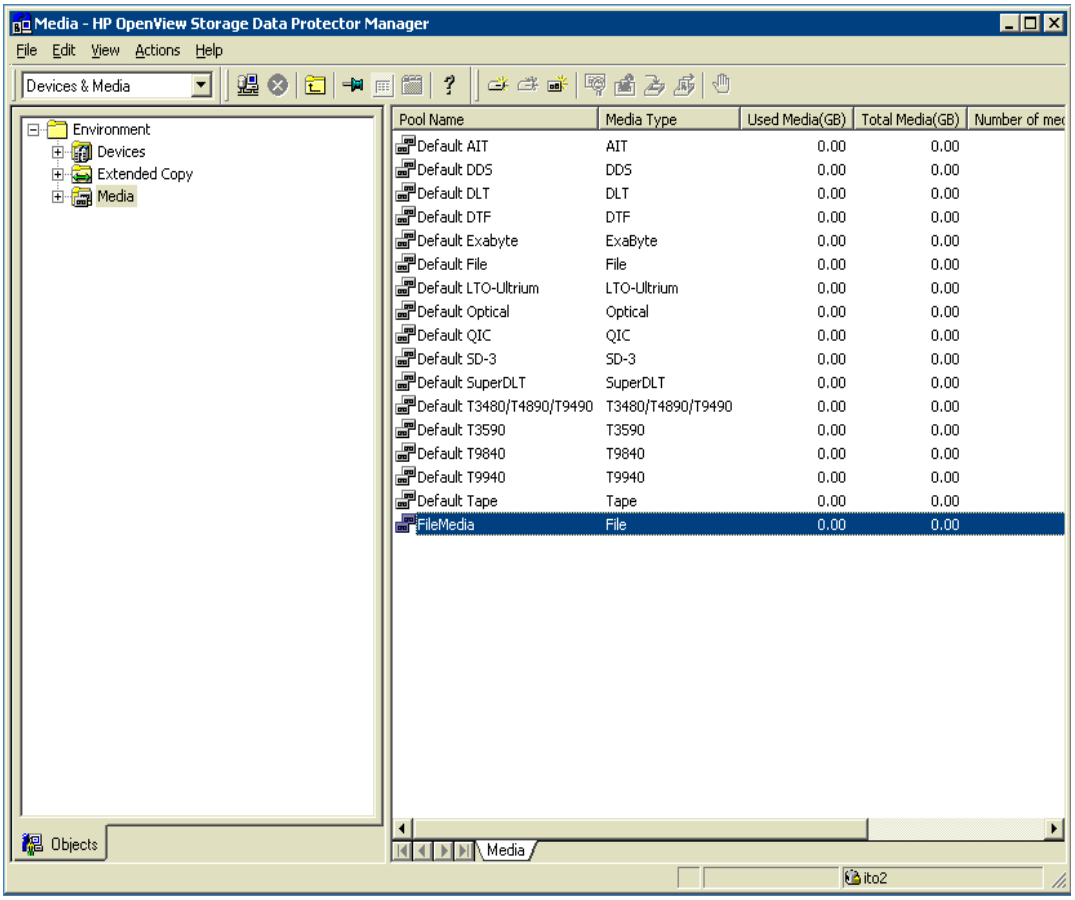

figure 5. FileMedia is the new media pool

creating the virtual tape library device in the msa1000

Here is an overview of the steps you need to follow to create a virtual file jukebox:

- Create a new device in the **MediaDevice Management** screen.
- Select **Jukebox** as the device type.
- Select **File** as the media type.
- Enter the number of slots for the jukebox.
- Select **Yes** when asked to create a drive for the jukebox.
- Configure the drive.
- Change the Default Pool of the drives to **FileMedia**.

The number of slots available in this virtual jukebox depends on the license key product you purchased. HP recommends that you always create at least ten extra free slots in the jukebox. If you need to restore data from a tape, you might have to restore the data to a temporary staging directory. Then the filename in the staging area will be moved into the free empty slots. If all slots are occupied, you must “eject” some media out of the slots. When you have free slots, some media management process is eliminated.

1. Choose **Devices and Media** from the **Context** drop-down menu.
2. Right-click **Device** in the **Scoping Pane**.
3. Click **Add Device**.
4. In the example, enter MSA1k_jukebox in the **Device Name** field. Make sure the selected device type is **Jukebox**.
5. Click **Next**.
6. Enter the path for the slotnames. See Figure 6.

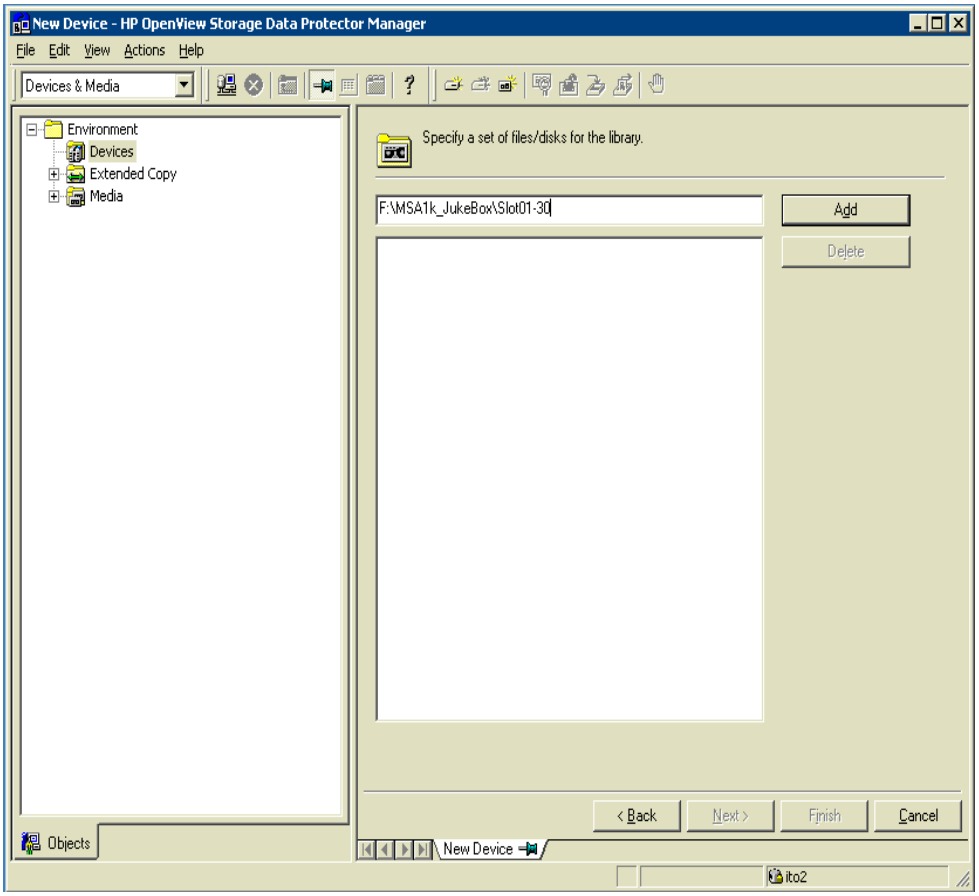

figure 6

In this example, the folder called MSA1K_Jukebox was created in the F: drive. The MSA1k_Jukebox contains the slots for the Virtual Tape Drive. Thirty slots were created in the Virtual Jukebox. The filename slot01-30 instructs Data Protector to create the files named slot01 through slot30.

Enter the complete path in the **Slotname** field that specifies the location of the filesystem where you are storing the Virtual Tape Media. For example, specify a fully qualified path such as c:\HTH\File_Device\slot01-20. Files slot01 till slot20 will be created in the specified directory after the "media" in the slots are initialized

Initializing the slots writes media headers to the files and associates media names with each slot. Even though the file name is slot01, the media name tracked in the database is different. (You can identify the media label by looking at the description column on the Data Protector screen.) After the initialization process, the files have a size of 24 KB.

If you do not specify the path in the slot name, the files are created in the OMNITMP directory. HP does not recommend that you use the OMNITMP directory as it contains all process files and debug files. You can change the path by adding the OmniTmp key to the registry entry HKLM/Software/Hewlett-Packard/Open View/OmniBack II/Common.)

Note: Do not use the "-" character in the filename.

7. Click **Add**.

8. Review the slotnames and determine if they were added successfully. If the information in the screen (figure 7 below) is correct, click **Next**.

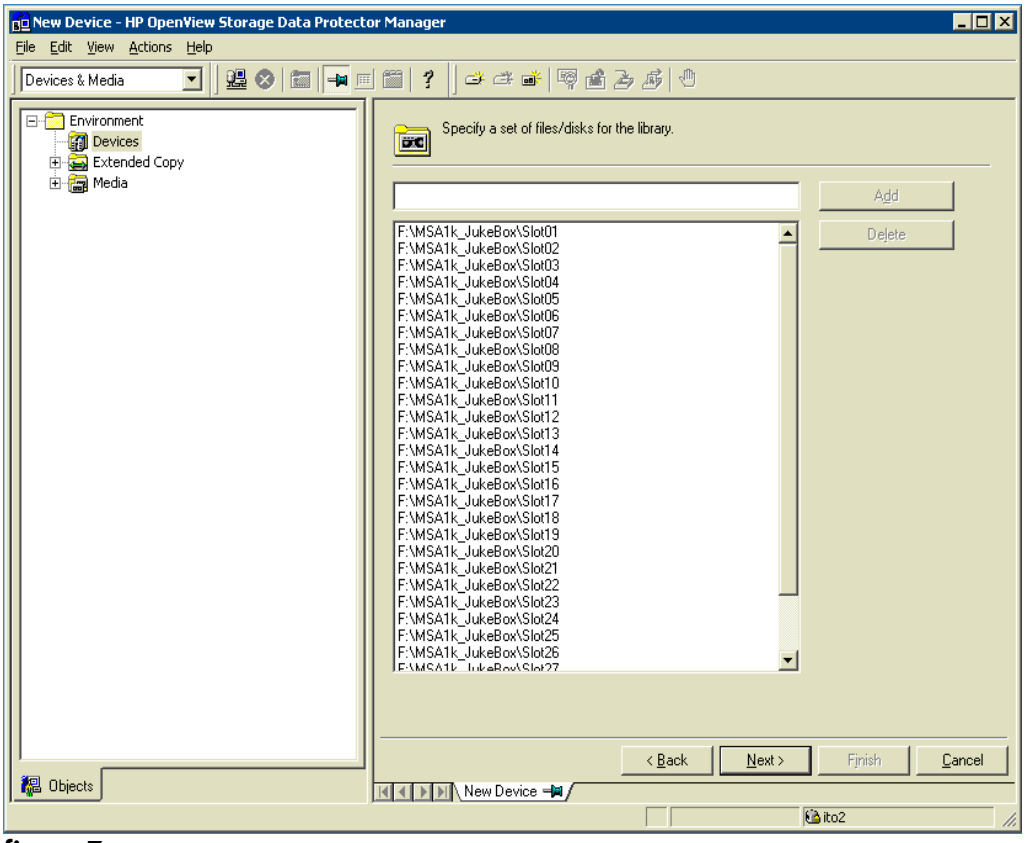

figure 7

9. Ensure that the media type is set to **File**. Click **Finish**.

10. Start adding drives. Click **Yes** to the message that asks if you want to configure drives for the jukebox you just created.

11. Enter the drive name in the **Device Name** field.

12. Enter the description. Click **Next**

13. Check that **FileMedia** is selected as the **Default Media Pool**. If you want to change any parameters, click **Advanced**. Figure 8 is displayed.

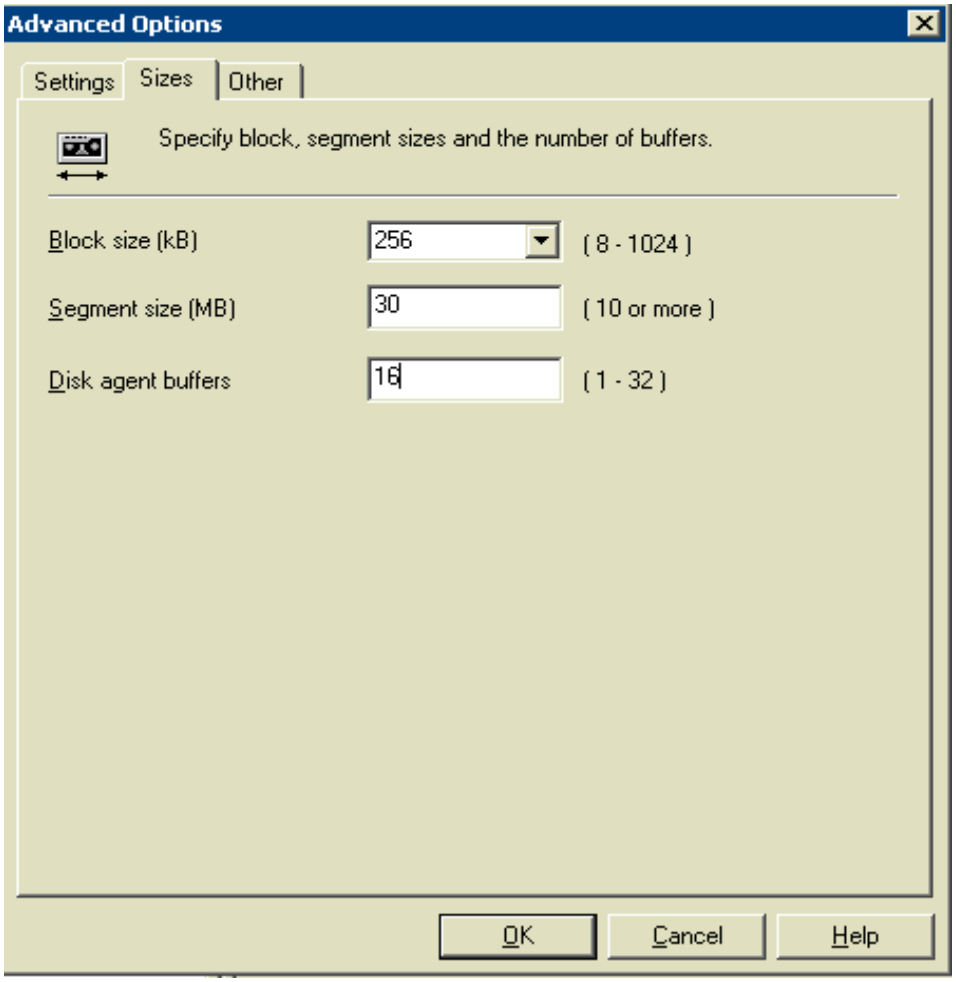

figure 8

14. Make your changes.
    Be sure to calculate the segment size against the size of the file device. Otherwise you will run out of filemarks. (The default value of the segment size is 30MB. If the file device is bigger than 7GB (single file size), be sure to change the segment size to 100MB.)

    Click **OK**.

15. Click **Finish**.

16. A dialog box is displayed. Click **Yes** if you want to continue adding drives or click **No** if you are done.

17. When you are done adding drives to the jukebox, the screen should look similar to Figure 9.

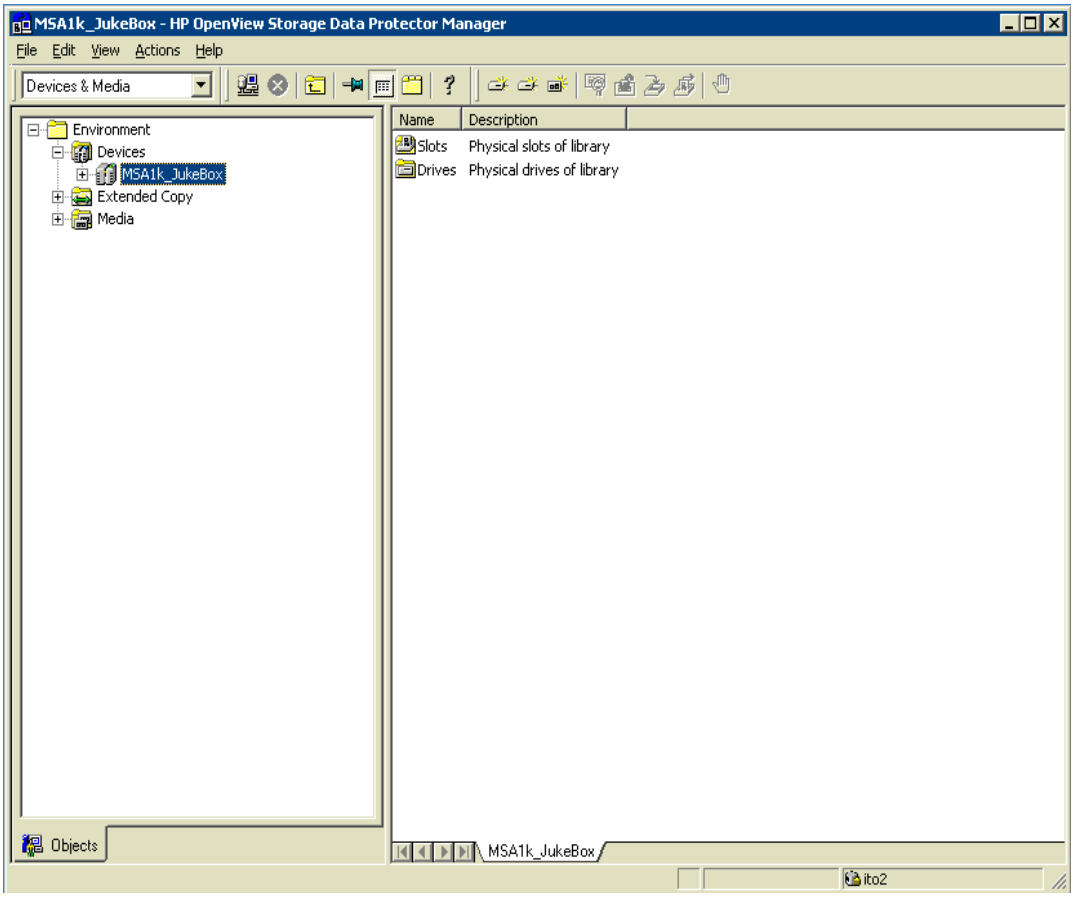

figure 9

formatting the virtual tape media

1. Expand the MSA1K_Jukebox folder in the **Scoping Pane**. The **Drives and Slots** folder in the MSA1K_Jukebox is displayed.

2. Click **Slots**.

3. Select the number of slots you want to format. See figure 10.
   Although there are 30 slots in this virtual jukebox, only 20 slots are being formatted. Formatting slots is analogous to putting a physical tape into the slot of a physical jukebox library.

4. Select **Format**. Before the format begins you are prompted to select the drive. Since the format is not performing on physical media, the process should complete quickly.

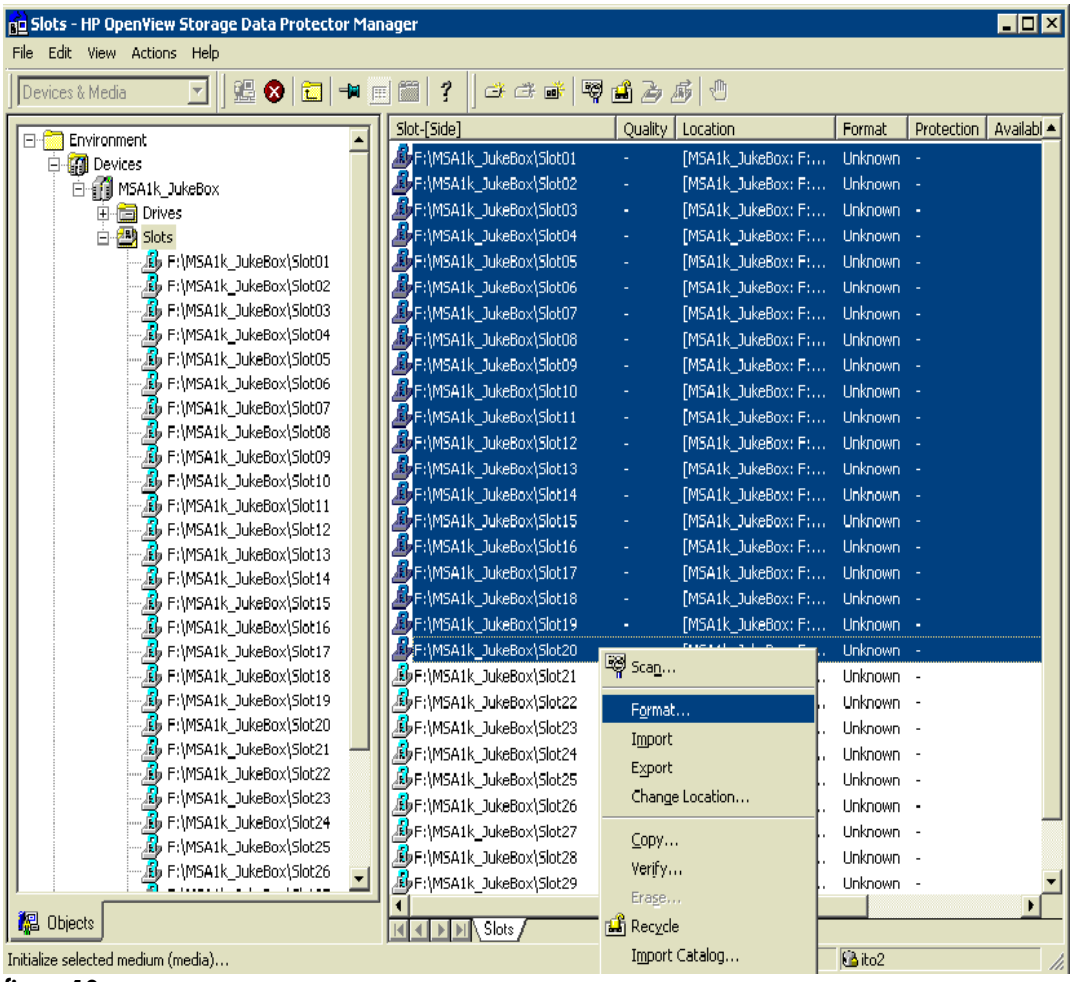

figure 10

5. Select the drive and click **Next**.

6. Check that **MediaFile** is selected as the **Media Pool**. Click **Next**.

7. You can assign a label to the virtual tape or you can select the default, **Automatically generate**. Click **Next**.

8. You can specify a specific size for the media or accept the default size, which is the size defined in the Data Protector configuration file. Click **Finish**.

When the format is complete, the results should look similar to figure 11.

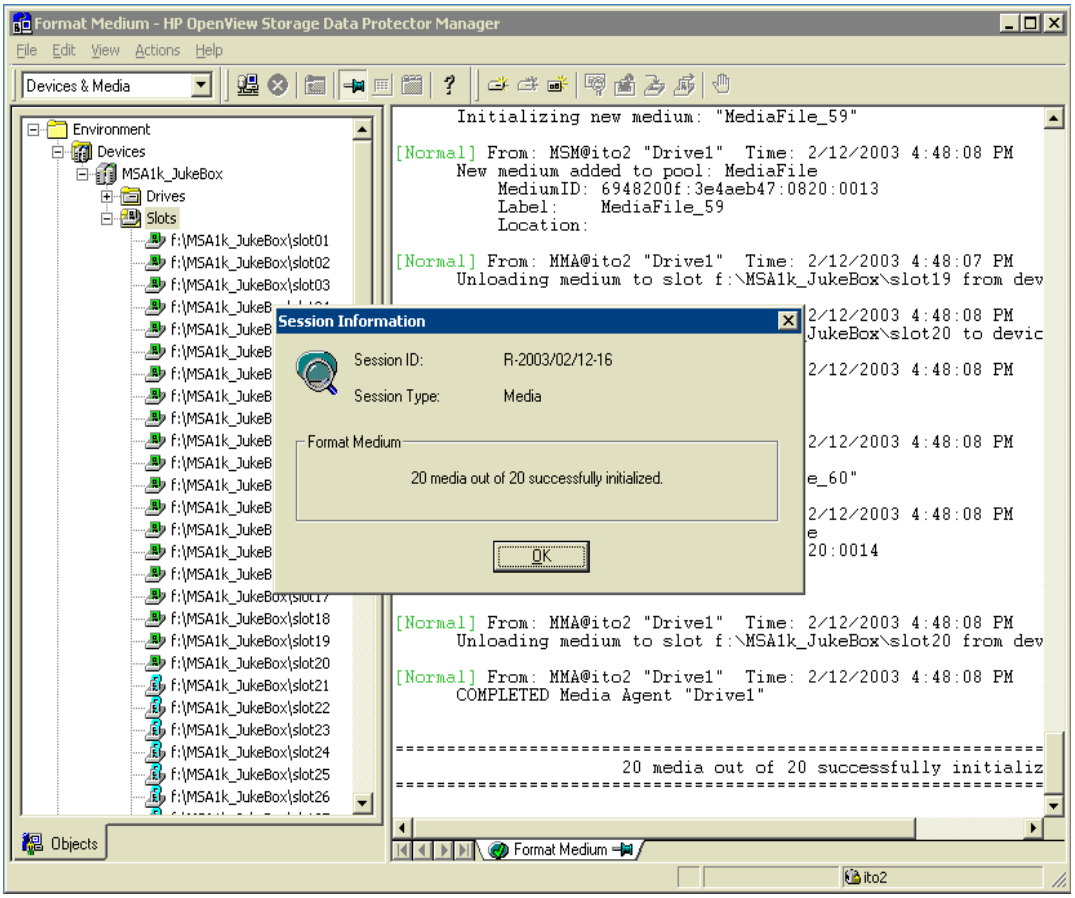

figure 11

backing up to the virtual jukebox

1. Select **Backup** from the **Context** dropdown menu.
2. Right-click **Filesystem**.
3. Select **Add Backup**.
4. Click **OK** to accept all the default options on the **Create New Backup** window. In this example, the default options are always selected although you may have to make different selections depending upon your environment.
5. Click **Next**. In this example, the C: drive is backed up to the F: drive, which is the msa1000 filesystem for disk-to-disk backup.
6. Select the virtual jukebox (MSA1k_jukebox) that you previously created as the device to be used for the backup. Click **Next**.
7. Select the defaults on the **Backup Specifications** window. Or you can specify different parameters to suit your environment. Click **Next**.
8. Select the defaults on the window that lets you specify dates and times. Or you can specify different parameters to suit your environment. Click **Next**.
9. Select the defaults on the **Review Summaries** window. Or you can specify

different parameters to suit your environment. Click **Nex**t.

10. Choose **Save As**, **Start Backup,** or **Start Preview**.
    If you would like to save the setting, select **Save As**. To begin the backup, click **Start Backup**. Or for a preview of the backup, click on **Start Preview**.

11. Specify the type of backup you want and the **Network Load**. Click **OK** to start the backup.

backing up to tape

You may want to back up to tape if the msa1000 is running out of space. You can back up data to tape to free up space for new backups. Or you can back up to tape when you want to archive data and store it offline. You can back up data to tape or optical media for offline storage.

Data Protector tracks backup data files stored in the msa1000 with their media names or media labels, which were written to the file during initialization. Here is the procedure to follow to back up data from the msa1000 to tape or to any offline media:

1. Using Windows Explorer, identify the device file (slot filename) size in the Virtual Jukebox directory. In this example, the device file is found at:

   `F:\MSA1K_Jukebox\`

2. Using Windows Explorer, create a folder in a drive that has enough capacity to store the data that you want to offload to tape. Name this folder “export to tape”.

3. In the Data Protector screen, identify the media label (under the description column) that corresponds to the slot that you want to backup.

4. Using Windows Explorer, move the “slot” filenames to the new “export to tape” folder. Rename the slotname with the media label that you identified in step 2.

5. Repeat steps 2 and 3 for all the slots that you want to backup.

6. After you have renamed the filenames, you need to scan the library using Data Protector. Select all the slots. Right-click and choose **Scan**. See Figure 12.

   When the scan is complete, the slots are recreated in the msa1000 folder but the slots are empty. You can fill the jukebox with media by reformatting the slots that were just recreated. See formatting the virtual tape media. New virtual media is now in the slots and you are ready for the next backup. In Windows Explorer, you can see the slot filenames again. See Figure 12.

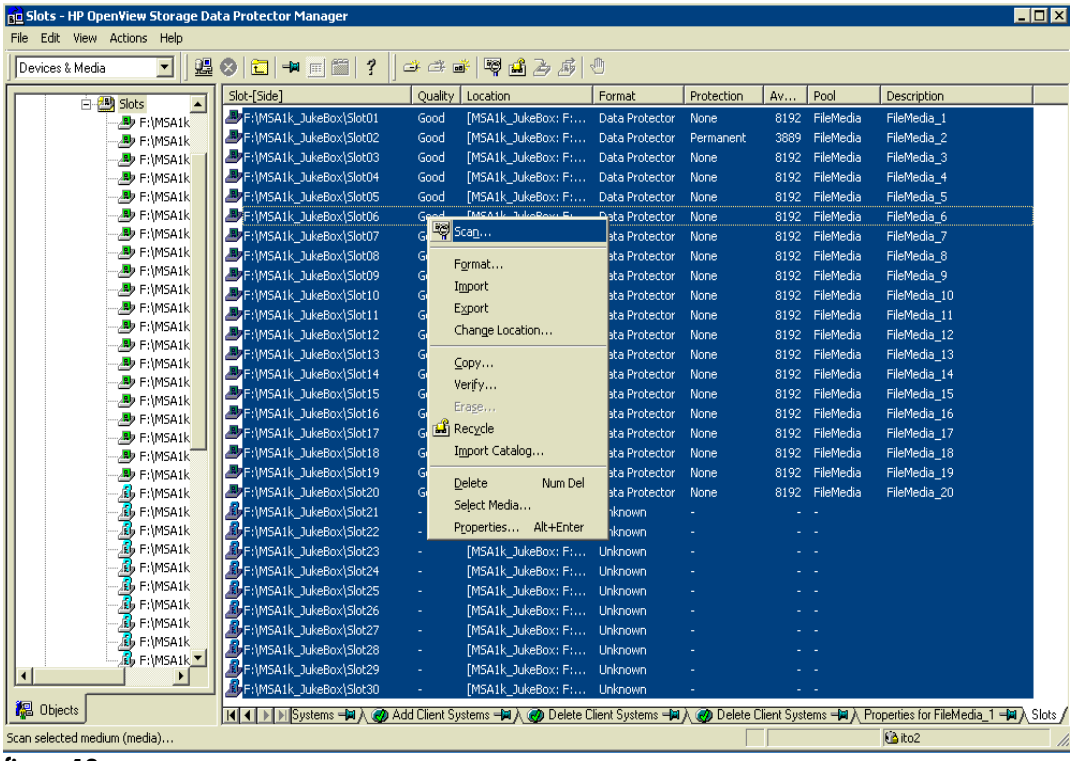

figure 12

7. Back up the files in the “export to tape” folder to the tape media. (Follow standard Data Protector procedures for backing up to tape.)

8. Delete the files from the “export to tape” folder.

restoring data from the virtual jukebox

1. Choose Restore from the Context dropdown menu. See Figure 4.
2. Identify the client that you want to restore in the Scoping Pane. Double-click the client to expand the drive list.
3. On the Source tab in the Results area, click the drive letters and select the files and folders that you want to restore.
4. Click Restore.

   If the data is still in the file jukebox, then the data is accessed directly from the MSA1000 and restored automatically from the virtual media. This type of restore is much quicker than restoring from tape.

   If the data is not in the file jukebox because it has been backed up to tape, Data Protector displays a **Mount Request Information** window and asks you to insert the required media into a specific slot in the jukebox. You should write down the name of the media label and the slots number. Close the window and follow the procedure for restoring from tape. See restoring from tape.

restoring from tape

Here is the procedure to follow for restoring data from tape.

1. Using Windows Explorer, create a folder in a drive that has enough capacity to hold the restore data. Create a folder and name it “import from tape”.
2. In the Data Protector screen, select Restore from the Context dropdown menu.
3. Restore the required media label file from the tape drive to the “import from tape” folder.
4. Using Windows Explorer, rename the media label file name in the “import from tape” folder with the specified slot name from the **Mount Request Information** window.
5. Move the slotname in the “import from tape” folder into the file jukebox folder.
6. Scan the library using Data Protector.
7. Confirm the Mount Request in Data Protector to continue the restore process.

troubleshooting notes

- You can specify the capacity of a file device when you first format the medium. When you reformat the medium, you can specify a new size but the originally specified size is still used. You can only change the capacity of a file device by deleting the file from the system and recreating the file with the new size.

- Data Protector cannot monitor disk space usage and prevent other Media Agents or processes from writing on the same file system. Therefore, a disk could run out of space when Data Protector tries to backup to the disk.

working with VERITAS NetBackup V4.5

With VERITAS NetBackup 4.5, you can perform backups to high-speed, low-cost inline storage, the MSA1000. In addition, with VERITAS NetBackup Vault, you can easily duplicate the msa1000's backup data to tape.

Vault handles the media and catalog management, which lets you perform a restore without knowing exactly where the backup image is located. Vault also automatically "expires" the primary images that were duplicated from the msa1000 to tape. In this way, disk space for online backups is efficiently managed without administrator intervention.

configuring VERITAS NetBackup

Before you begin, check the following:

- The backup management server is set up using NetBackup's default values.
- LUNs are assigned on the msa1000
- VERITAS NetBackup V4.5 and VERITAS NetBackup V4.5 Vault are installed in a normal NetBackup environment.
- Enterprise Virtual Array is installed.

Here is an overview of the procedures required to create backups and duplicate them to tape. In this example, NetBackup is configured to use an MSL5026 SL.

1. Create a new storage unit.
2. Assign the path to the msa1000.
3. Create a policy that lets you backup data to the msa1000.
4. Create a vault robot. This is the robot or jukebox that you use for duplicating the data to the tape medium. (A robot is identical to a jukebox.)
5. Create a profile that you can use for the duplication.
6. Determine the source of the backups.
7. Define the target.

creating a new storage unit

You can start this procedure from the Vault Management – NetBackup Administration Console, Figure 13.

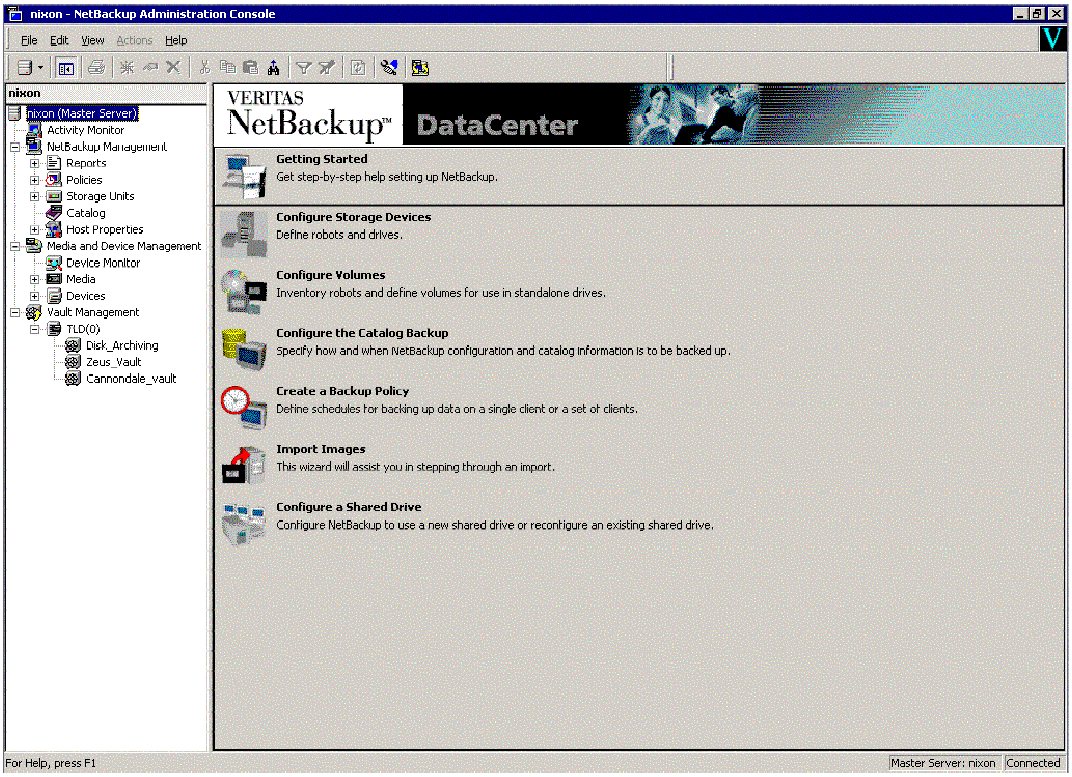

figure 13

1. Right-click **Storage Units.** Choose **New**.
2. Choose **Disk** from the **Storage unit type** drop-down menu. Click **OK**.
3. Enter the name of the storage unit in the **NetBackup media server** field.
4. Enter the path to the MSA1000 in the **Absolute pathname to directory** field.
5. Enter "**1**" for the **Maximum concurrent jobs**. You can enter a maximum of 8, which is the number of concurrent backups that can go to this new storage unit.
6. Enter the **Maximum fragment size**, which is the size of each individual fragment of data.

creating a policy to backup data to the msa1000

In this step, you create the policy that lets you backup data to the msa1000. (A policy is a backup job.)

1. On the **Attributes** tab, enter the **Policy type**. In this example, enter MS Windows NT.
2. In the **Destination** box, enter the **Policy storage unit**. (Disk Storage unit created previously.)
3. Click the **Schedules**, **Clients**, and **Files** tabs and enter the information that suits your environment.

creating a vault robot and profile

n this step, you create a logical robot for vault to use. This is the robot that exists on the host and that can be used for vaulting (duplicating the data). The robot must exist in the configuration and the host must have a valid storage unit for that robot. Vaults are assigned to a particular robot. Each vault will have one or more profiles.

Note: Only one profile in a vault can run at a time.

1. Go to the Vault Management — NetBackup Administration Console.
2. Right-click **Vault Management**
3. Choose **New Vault Robot**.
4. Choose the robot that you want to use for vaulting. Enter the **Robot number**.
5. Double-click **Vault Management**.
6. Right-click on the newly created "Vault robot" and select **New Vault.**
7. Enter a **Vault name** and the appropriate **Robotic volume group** (if needed) to use for media in this Vault.
8. Select the newly created vault under the Vault robot.
9. Right-click on the **Vault** and select **New Profile**.
10. Enter the name of the new profile and select **Duplication** only. Click **OK**.
11. Select the **Choose Backups** tab. Select the criteria to use for the source of the backups. For example in the **Backups started** box, enter the number of days and hours that you want to use as criteria.
12. Select the target for the duplication. In the **Source** box, select **Disk only**.
13. Choose **Expire original disk backup images after** and enter the number of hours. For example, if you select 0 hours, as soon as the duplication is complete, the original copies are deleted.

creating the policy that schedules the time for the vault to run.

1. On the **Attributes** tab, enter the **Policy type**. In this example, enter **Vault**.
2. On the **Schedules** tab, select the times that you want the vault to run. Click **OK**.
3. On the **Files** tab, enter the vault profile name. In this example, enter vltrun <profile name>.

restoring the data

Depending on the release of NetBackup that you have installed, review the following document for restore procedures.

- *VERITAS NetBackup 4.5 Feature Pack 3 User's Guide for Microsoft Windows*
- *VERITAS NetBackup 4.5 User's Guide for Microsoft Windows*

Complete documentation is available on the http://support.veritas.com website.

working with CA BrightStor ARCserve V9.0

CA BrightStor ARCserve supports backup-to-disk functionality along with media copy capabilities, which allows disk-based backup media to be transferred to tape media. This section provides instructions that describe how to do the following:

- Create a disk backup device.
- Copy data from the disk medium device to a tape medium device.

configuring CA BrightStor ARCserve Backup

Before you begin, check the following:

- BrightStor ARCserve Backup for Windows with Tape Library Option and Storage Area Network Option has been installed on all servers.
- The Primary and Distributed servers have been designated and the Device Configuration and SAN Configuration has taken place.
- msa1000 LUNs have been presented to the hosts that will be using CA backup-to-disk functionality.

setting up a disk backup volume

1. Using the BrightStor ARCserve Manager user interface, expand the Wizard menu and select **Device Configuration**.
2. Select **Windows Server** and click **Next**.
3. Select **File System Devices** and click **Next**.
4. Click **Add** and then click the **FSName** text that is displayed.
5. Enter a name of your choice for the disk backup device that you are creating.
6. Enter a description for the device under the **Description** column. Select the path where you want the backup volumes to reside under the **Location** column. Click **Finish** when the disk devices have been created.

transferring backups from disk to tape

You can transfer backups from disk to tape using the tapecopy command. You can run the tapecopy command as follows:

- From the MS-DOS command prompt.
- Using the backup post option from the BrightStor ARCserve interface.

You can use the tapecopy command to do the following:

- Copy a session or produce a mirror media.
- Make logical media-to-media copies of like or unlike media types.
- Make an identical copy of the source media.
- Copy from a range of sessions in the source media and append to the contents of the destination media.

Keep in mind that after the copy from disk to tape is complete, the ARCserve database is unaware of the contents of the tape. You need to perform a merge operation of the tape media before you can actually restore from the tape.

running the tapecopy command

If you choose to run the command as a post operation to a backup job from the BrightStor ARCserve interface, here is the procedure to follow:

1. Using the ARCserve Manager interface, open a Backup window.
2. Enter all the parameters for the backup job.
3. Click **Options** and select the **Pre/Post** tab.
4. In the **Pre/Post** dialog box, enter the tapecopy command in the **Run Command After Job** field.
5. Click **OK**.

tapecopy syntax

Here is the syntax to use when you are transferring backups from disk to tape:

```
<BAB Install Path>/tapecopy -s[source group] -d[destination
group] -t[source tape name] {[source options] [destination
options]}
```

Source Options:

- -n <Beginning Session >
  Specify the session number where copy from the source tape begins
- -ntotal <Number of Sessions>
  Used with -n only. With this switch, you can specify the number of sessions to copy, beginning with -n.
- -rs <Remote Server Name>
  When the source tape is located on a remote machine, use this switch to specify the remote hostname.
- -entire (Copy All Non-Blank in Group)
  This switch copies all tapes in a group to another group. This switch is valid only within a changer.
- -t <Source Tape Name >
  Specifies the name of the tape you want to copy. If there are multiple tapes with the same name, specify -m and/or -q.
- -q <Source Sequence No.>
  Specifies the source tape sequence number if there is ambiguity about which tape to choose. This will be necessary when source tapes have the same name.
- -s <Source Group Name>
  Specifies the source device/changer group name of the source tape.
- -m <Source Random ID>
  Specifies the source tape random ID if there is ambiguity about which tape to choose. This will be necessary when source tapes have the same name and sequence number.

- -date<{MM-DD-YYYY,MM-DD-YYYY}>
  This switch copies tapes modified within the specified date range.

Destination Options:

- -rd <Remote Server Name>
  When the destination tape is located on a remote machine, use this switch to specify the remote hostname.

- -d <Destination Group Name>
  Specifies the destination device/changer group name of the destination tapes.

- -c <Destination Tape Name>
  Specifies the name of the destination tape.

- -off (Offline)
  Offlines target tapes at the end of the copy routine. This switch is valid for changers only.

- -ex (Export)
  Exports target tapes at the end of the copy routine. This switch is valid for changers only.

- -a (Append)
  Causes the target tape to be appended. The default is overwrite.

- -b (Blanks Only)
  Uses blanks only as target tapes.

tapecopy syntax examples

Here are samples of common commands.

To copy all sessions from the source tape and export target tapes after completion, enter:

```
tapecopy -sGROUP0 -dGROUP1 -tTAPE1 -ex
```

To copy all sessions from the source tape and offline target tapes after completion, enter:

```
tapecopy -sGROUP0 -dGROUP1 -tTAPE1 -off
```

To copy all sessions starting on session 3 of the source tape, enter:

```
tapecopy -sGROUP0 -dGROUP1 -tTAPE1 -n3
```

To copy all sessions from source tape to a blank target tape, enter:

```
tapecopy -sGROUP0 -dGROUP1 -tTAPE1 -b
```

To copy all sessions from source TAPE 1 to target TAPE 2, enter:

```
tapecopy -sGROUP0 -dGROUP1 -t"TAPE 1" -c"TAPE 2"
```

To copy all sessions from source[TAPE 1] and append to target[TAPE 2], enter:

```
tapecopy -sGROUP0 -dGROUP1 -t"TAPE 1" -c"TAPE 2" -a
```

To copy all non-blank tapes from source group and export target tapes after completion, enter:

```
tapecopy -sGROUP0 -dGROUP1 -entire -ex
```

To copy from local source tapes to remote tapes, enter:

```
tapecopy -sGROUP0 -dGROUP0 -tTAPE1 -rdSERVERNAME(or IP address)
```

To copy from remote source tapes to local tapes, enter:

```
tapecopy -sGROUP0 -dGROUP0 -tTAPE1 -rsSERVERNAME(or IP address)
```

automating the two stage backup

table 1. scenarios for using mezzanine backup-restore solution, page 5, describes several scenarios. The following example describes how to automate scenario 2 in Table 1.

The process includes performing daily incremental backups to disk and weekly full backups to tape. Using the tapecopy command, the incremental disk backups are also copied weekly. The required merge operation follows the tapecopy command.

After the contents of the weekly incremental backups have been copied to tape, and the tape is merged into the database, the disk media is erased using the `ca_devmgr` command.

You can schedule and run the jobs using the ARCserve Manager user interface or with a batch file script that calls the “cabatch.exe” utility. With either approach, you use the post job functionality to run the “tapecopy”, “ca_merge”, and “ca_devmgr” operations. This section describes how to automate the process.

Here is a list of parameters used for the job definition in this example:

- Group name for disk device: DISK
- Media name in group DISK (used to store incrementals): DISKMEDIA
- Group name for the tape media that is storing the Full Backups: TAPEFULL
- Media name that is used to store Full Backups: FALCFULL
- Group name for tape media that is archiving the incrementals: TAPEINCS
- Media name that is archiving the incrementals: FALCINC
- Host server name where the jobs are run: FALCON
- Path of objects that are being archived: f:\temp

scheduling a daily incremental backup to disk

From the ARCserve Backup Manager window, you can schedule a daily incremental backup to disk.

1. Choose **QUICK START** and click **Backup**.
2. Select the **Source** tab and select the objects to be backed up. In this example, f:\temp is selected.
3. Select the **Destination** tab and then select the groups and media that you want to use. In this example, group "DISK" and tape "DISKMEDIA" are selected.
4. Select the **Schedule** tab and then select **Custom in the Repeat Method** field.
5. In the **Repeat Interval** column, enter "1" in the **Days** field.
6. In the **Exclude Days** column, check **Sunday**.
7. In the **Backup Method**, select **Incremental**.
8. Start the job and set the time to start. For this example, the job is scheduled to start at 10:00 pm on the same day the job is submitted, so long as that day is not Sunday.

scheduling a weekly full backup to tape

You can schedule a weekly full backup to tape and set the post operation to run a script file, which contains the tapecopy (copy of disk incrementals to tape). The script file merges and catalogues the tape that contains the copy of disk incrementals and then erases the disk contents after the tapecopy is complete.

Here is how to schedule a weekly full backup to tape and run a post operation batch file that contains the tapecopy, merge, and disk media erase operations.

1. Choose **QUICK START** and click **Backup**.
2. Select the **Source** tab and select the objects to be backed up. In this example, f:\temp is selected.
3. Select the **Destination** tab and then select the groups and media that you want to use. In this example, group TAPEFULL and tape FALCFULL are selected.
4. Select the **Schedule** tab. Select **Every** in the **Repeat Method** field, and enter **7 Days** in the **Every** field.
5. In the **Backup Method**, select **Full (Clear Archive Bit)**.
6. Click **Options** at the top of the window and select the **Pre/Post** tab.

In the **Enter the name of the file/application to execute after the job** field, enter the name and path of the batch file that contains the tapecopy, merge, and erase operations.

In this example, the "tpcpymrg.bat" script file was created and stored in the root of f:\. Enter the following syntax in this field:

```
cmd /c "f:\tpcpymrg.bat"
```

The cmd /c must precede the file path and the path must be in quotes. The cmd /c opens the Windows 2000 command prompt, runs the command in quotes, and terminates when the batch commands are complete.

The contents of the tpcpymrg.bat batch file for this example are as follows:

```
cd c:\program files\ca\brightstor arcserve backup
tapecopy –sdisk –dtapeincs –tdiskmedia –cfalcinc
ca_merge –group tapeincs –tape falcinc –allsessions
ca_devmgr –erase <adapter #><scsi id><tape name>
```

In this example, the ca_devmgr command should be as follows:

```
ca_devmgr –erase 4 0 diskmedia
```

Note: The ca_devmgr command renames the tape with its original name but with a different ID. Since this command creates a new media object in the database, you must manually delete the old object.

7. Select the **Job fails** in the **Do not run Command if** field. Click **OK**.

creating a script

You can use the cabatch.exe utility to run a script file. You can define a job using the ARCserve Manager interface and save it as an .asx extension script file. You can save the .asx file as follows:

- In the **Backup Job** dialog box, choose **File > Save As**.

The saved files have an .asx extension such as incs.asx and full.asx. You can only execute script files using the ARCserve Manager interface or as an argument using the cabatch.exe utility. To run these .asx scripts, use the following syntax at the command prompt:

```
cabatch /MODE=execute|Submit /H=ServerName /S=<path>ScriptName
```

In this example, a batch file with the following two lines was created to include two jobs:

```
cabatch /MODE=execute /H=falcon /s=C:\Program Files\CA\BrightStor
ARCserve Backup\incs.asx
cabatch /MODE=execute /H=falcon /s=C:\Program Files\CA\BrightStor
ARCserve Backup\fulls.asx
```

restoring the data

See the *BrightStor ARCserve Backup for Windows Administrator Guide V9.0* for specific information about restores. You can use the Backup Restore wizard or the Restore Manager. See the following website for the list of documentation:

http://support.ca.com/techbases/basb9/basb9-manuals.

for more information

additional solutions

For more information on two-stage backup and the msa1000, visit:
http://h18006.www1.hp.com/products/storageworks/msa1000/index.html

HP offers solutions that simplify and streamline your infrastructure. Other available solutions provide business continuity and tape-based disaster recovery. See the URL's below for more information.

- Consolidation Solutions:
  http://h18006.www1.hp.com/storage/solutions/itconsolidation.html
-
- Business Continuity Solutions:
  http://h18006.www1.hp.com/storage/continuity
- Tape-based Disaster Recovery Solutions:
  http://h18000.www1.hp.com/products/storageworks/drtape/

For additional HP Solution technical blueprints, visit:
www.hp.com/go/hpstorage_blueprints

To get answers to further solution implementation questions, contact your HP sales representative, who will consult our regularly updated interoperability matrices and provide

guidance on additional operating system, fabric topology, and third-party/legacy device interoperability.

hp components

To get further information on the individual components in an HP SAN, visit:

http://www.hp.com/go/storage

hp services

A full range of storage services are available including design, integration, data migration, support, and services to help you evolve your solution as needs change. For full details, contact your HP sales representative or visit:

www.hp.com

related documents

For HP OpenView Data Protector documents, see
http://ovweb.external.hp.com/lpe/doc_serv/

For VERITAS NetBackup documents, see
http://support.veritas.com

For BrightStor ARCserve Backup documents, see
http://support.ca.com/techbases/basb9/basb9-manuals.

You can also use the CAbatch.wri and template.txt files in the BrightStor ARCserve Backup home directory, which includes the template for building the job definition text file.

03/2003