



# HP Data Protector Operations Guide

About this document .....	3
Data Protector architectural overview .....	3
Data Protector Cell .....	3
Cell Manager services .....	5
The Session Manager .....	6
User management .....	6
Default user accounts .....	6
Using a service account .....	8
Wild-card user .....	8
About user management .....	9
Device management .....	11
Poor media .....	11
Resolving mount requests .....	13
Using a free pool .....	14
Using media preallocation list .....	15
Backup management .....	17
Viewing the backup specifications .....	17
Adding a new backup specification .....	18
Using drive concurrency .....	19
Order of Disk Agents started .....	20
Defining drive-based concurrency .....	20
Defining backup specification-based drive concurrency .....	21
About multiplexing .....	22
Object copy .....	24
Copy session start time .....	25
Emailing backup session reports .....	26
Setting up webbased reporting .....	26
Monitoring offsite procedures .....	27
Performance monitoring using a nul device .....	28
Restarting failed sessions .....	30
Resuming sessions .....	30
Editing the backup schedules .....	31
Restore management .....	32
File version restore .....	32
Restore query .....	33
Performing a restore when a library configuration has been deleted .....	33
IDB maintenance activities .....	34
Short-term IDB maintenance .....	34
Daily notifications .....	34
Long-term IDB maintenance .....	35
IDB Purge preview .....	35
IDB Purge .....	36

DCBF .....	37
Tablespaces .....	39
IDB notifications and reporting .....	41
Recovering the IDB .....	41
Data Protector cell and client tuning .....	43
global variables .....	43
omnirc variables .....	44
scsitab file .....	45
cell_info .....	45
Variables currently undocumented .....	46
Treewalk .....	46
Event management .....	46
Setting up SNMP trap forwarding .....	46
Running omnismmp .....	47
Setting OVdests trap destination .....	47
Adding a community name registry key other than public .....	48
Configuring the SNMP service destination host .....	48
Frequently used commands .....	50
omnidbutil .....	50
omnidb .....	50
omnimm .....	53
devbra .....	54
Log files and troubleshooting .....	54
Data required for support calls .....	54
The session log .....	54
Support files .....	56
Database copy .....	56
Debugging Data Protector .....	57
Inet connection .....	59
Patch upgrade and versioning .....	60
Security .....	60
Secure cell/client .....	60
Firewall configuration .....	61
Operation audit checklist .....	62
Backing-up data .....	62
Restoring data .....	63
Short-term maintenance checklist .....	64
Long term maintenance checklist .....	64
Off-site vaulting .....	64
References .....	65

## About this document

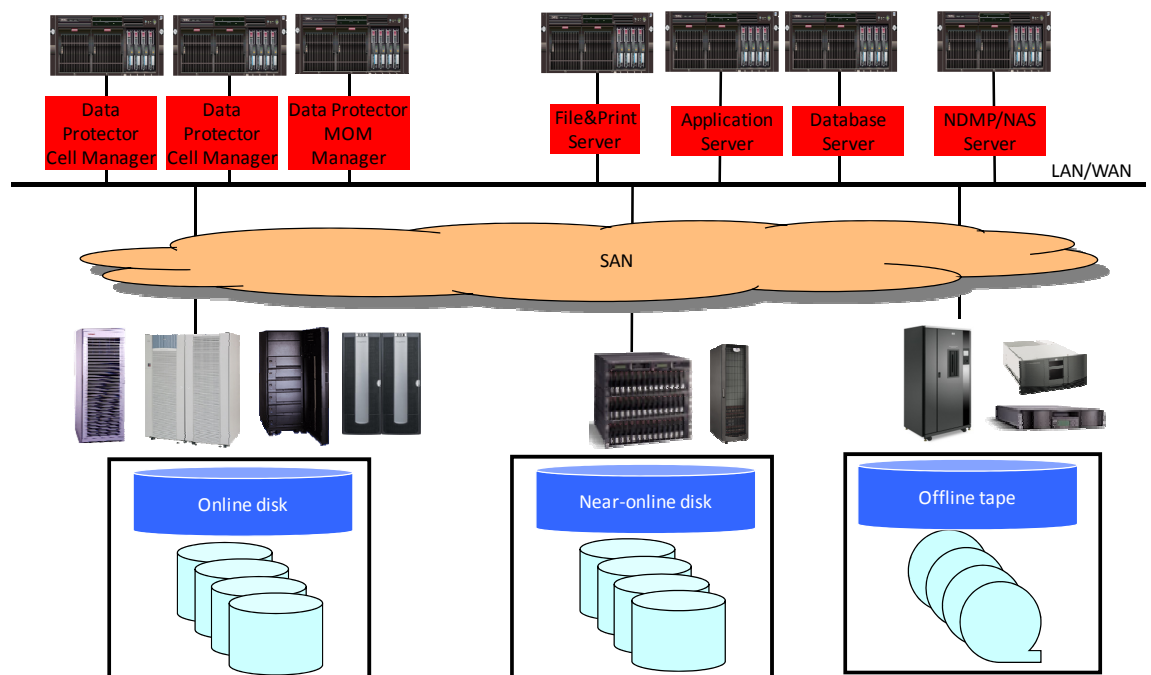
This document is intended for backup, system or storage operators and administrators, who are new to Data Protector and are performing common backup tasks. It covers frequently performed maintenance tasks, and provides some configuration recommendations and best practices on how to set up an effective and efficient backup environment. This is not intended to replace any existing documentation. For other Data Protector documentation, please refer to [www.hp.com/support/manuals](http://www.hp.com/support/manuals).

The role of a backup operator is to be in charge of daily tasks such as making sure backups complete successfully, tapes are ejected and scratch tapes are entered, and so on. Backup environments present many challenges that are often overlooked simply because we are too occupied with operations. There are many areas where a backup administrator can bring value to an organization beyond being the keeper of the data.

## Data Protector architectural overview

This chapter explains the HP Data Protector cell manager, client and Manager-of-Managers (MOM) server architecture, and the main processes which are running on the cell manager.

### Data Protector Cell



A Data Protector Cell consists of a Cell Manager system the systems that are to have their backup and restored tasks managed by it.

The basic HP Data Protector implementation utilizes only two architecture layers, the Cell Manager, and the Cell Client layers. The Cell Console (GUI) is installed on the Cell Manager but it may be distributed on multiple client systems as well.

The architecture is highly scalable and lends itself to the simplest single-system configuration, right up to the most complex multi-system, multi-site enterprise-wide solution. With centralized administration capabilities (managed locally or remotely) and a client/server-based architecture, Data Protector provides the ability to globally support automated backup and restore for up to tens of thousands of enterprise-wide network systems.

The Data Protector client/server architecture provides multiple manager layers, which offer tremendous flexibility and adjust easily to organizational needs and changes.

### **Cell Manager and clients**

The Cell Manager is the heart of the Data Protector backup environment. The clients are controlled from the Cell Manager system.

### **Enterprise Console**

The Data Protector integration with HP Operations Manager provides the concept of the Enterprise Console. HP Operations Manager allows remote administration and monitoring of one or more Data Protector cells from a single Enterprise Console.

### **Manager of Managers—MoM**

An existing Data Protector Cell Manager can be configured as the Manager of Managers (M.o.M.) which allows remote administration and monitoring of many cells from a single consolidated GUI. A centralized media management database (CMMDB), cross-cell device sharing as well as central license management may also be configured with MoM.

There is no enforced limit to the number of systems per Data Protector Cell, but the cell size may be limited by a number of factors:

- the number of supported systems (a maximum of 1000, although 100 is recommended)
- the size of the Data Protector internal database
- the number of backups that can be effectively managed (a maximum of 2000 per day)

The Data Protector internal database (IDB) can grow to be many GB. An estimate is to allocate enough disk space to allow the internal database to be approximately 2% of the quantity of data that is backed up. You may find that if you are backing up many large files (50 MB–100 MB each), the size of the database can be as little as 0.25% of the size of the data; this is especially true when backing up large database files. Backing up many small files means more records in the database, which means more space is required for the database.

Which Factors Should Be Considered when Defining Cells?

- Systems that have a common backup policy
- Systems that are to be backed up on the same LAN
- Systems administered by the same team of administrators
- Systems within the same time zone
- Systems should use time synchronization
- Systems in the same Windows Domain (for simpler administration)

Cells are generally independent parts of the enterprise network. They are administered and operate independently of each other.

Data Protector has the capability to monitor and administer all the cells from a central administration point utilizing the Cell Console, the Enterprise Console or the Manager of Managers console.

The agent processes are used for accessing disk and tape devices for backup, restore and media management tasks. The two fundamental agents are:

- Disk Agent – responsible for read/write actions from disk drives for backup and restore
- Media Agent – responsible for read/write actions to backup media (which may be tape or disk)

The basis of the client/server model is that the Data Protector software consists of client modules and a server module. These modules can all be installed on a single system (a single client cell) or distributed across many systems.

Communication between modules is accomplished via TCP/IP sockets, initiated on port 5555.

**Notes:**

- See the *HP Data Protector concepts guide (B6960-90151)* for further information on cell architecture.
- See the *Cell Manager Planning and Sizing Guide (4AA2-5036ENW)* and *Capacity Planning Spreadsheet* for further details on cell sizing.

## Cell Manager services

A UNIX Cell Manager system always has three daemon processes running to provide Data Protector services:

crs     Cell Request Server  
rds     Raima Database Server  
mmd     Media Management Daemon

A Windows Cell Manager system always has three service processes running to provide Data Protector services:

Data Protector CRS     Cell Request Server  
Data Protector RDS     Raima Database Server  
Data Protector Inet     Remote Connection Server

The manager programs resides in:

- *UNIX:* /opt/omni/lbin
- *Windows:* C:\Program Files\Omniback\bin

The three services or daemons normally start when the system boots up. Data Protector provides a program `omnisv` that can stop, start, and check on the status of these services. `omnisv` has three options: `-stop`, `-start`, `-status`. The “-” in front of the option flags is not required.

Default program locations:

- *UNIX:* /opt/omni/sbin/omnisv
- *Windows:* C:\Program Files\Omniback\bin\omnisv

Restart the Data Protector services via the command line to stop and start all services at the same time:

```
C:\Program Files\OmniBack\bin>omnisv -stop
HP Data Protector services successfully stopped.

C:\Program Files\OmniBack\bin>omnisv -start
HP Data Protector services successfully started.

C:\Program Files\OmniBack\bin>omnisv
usage: omnisv [-start | -stop | -status | -start_mon | -version | -help]
```

Or use the Windows services window to restart the Data Protector CRS, EDS and Inet services:

Name	Description	Status	Startup Type
Alerter	Notifies selected users and computers of administrative alerts...	Stopped	Disabled
Altiris Deployment Agent	Provides functionality for Altiris Deployment Solution	Started	Automatic
Application Layer Gateway	Process application compatibility lookup requests for applicati...	Started	Automatic
Application Management	Processes installation, removal, and enumeration requests fo...	Started	Manual
AppStorWin32Agent	AppStorWin32Agent Service	Started	Automatic
Automatic Updates	Enables the download and installation of Windows updates. If...	Started	Automatic
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwid...	Started	Manual
ClipBook	Enables ClipBook Viewer to store information and share it with...	Stopped	Disabled
COM+ Event System	Supports System Event Notification Service (SENS), which pro...	Started	Automatic
COM+ System Application	Manages the configuration and tracking of Component Object...	Started	Manual
Computer Browser	Maintains an updated list of computers on the network and su...	Started	Automatic
Cryptographic Services	Provides three management services: Catalog Database Serv...	Started	Automatic
Data Protector CRS	[HP Data Protector] - Cell Manager service	Started	Automatic
Data Protector Inet	[HP Data Protector] - Backup client service	Started	Automatic
Data Protector RDS	[HP Data Protector] - Cell Manager database service	Started	Automatic
Data Protector UIProxy	[HP Data Protector] - User Interface proxy service	Started	Automatic
DCOM Server Process...	Provides launch functionality for DCOM services.	Started	Automatic

Verify the services status by running the following command line option:

```
C:\Program Files\OmniBack\bin>omnisv -status
ProcName  Status  [PID]
=====
rds       : Active [5412]
crs       : Active [5536]
mmd       : Active [3720]
kms       : Active [4700]
uiproxy  : Active [4880]
omniinet : Active [4060]
Sending of traps enabled for the following hosts:
10.50.3.38
=====
Status: All Data Protector relevant processes/services up and running.
```

## The Session Manager

The Cell Manager listens for session requests and starts the appropriate Session Manager, which in turn starts the required clients. A dedicated Session Manager controls the clients for each operation. If a new session is started, an additional Session Manager is generated.

- bsm Backup Session Manager
- rsm Restore Session Manager
- csm Copy Session Manager (used for object copy)
- dbasm Database Session Manager
- msm Media Session Manager
- asm Administration Session Manager

When they are installed with the cell manager, these session manager programs reside in:

- UNIX: /opt/omni/lbin directory
- Windows: C:\Program Files\OmniBack\bin

## User management

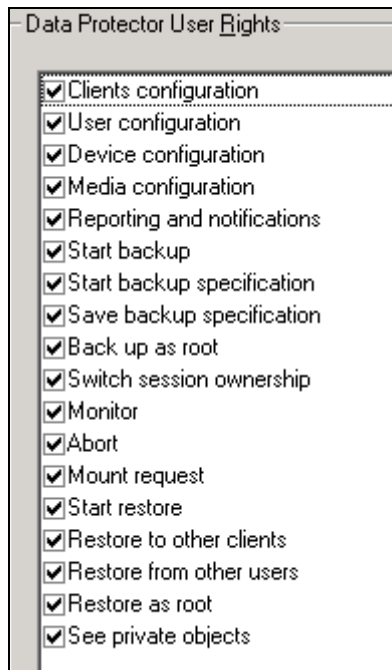
This chapter explains the user accounts created by default on the cell manager, and provides hints and tips about undocumented user management configuration.

### Default user accounts

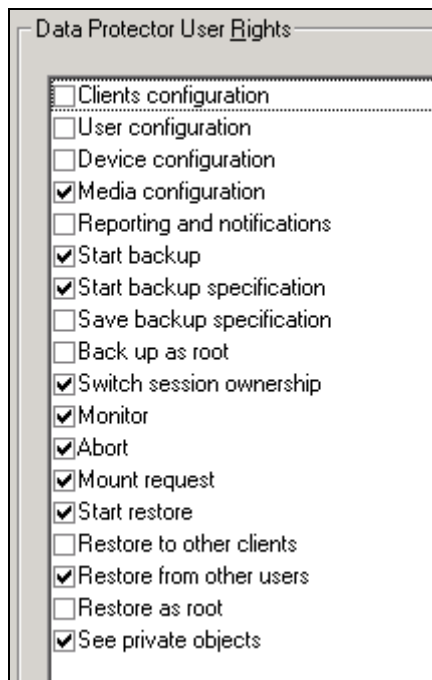
By default, Data Protector adds the local or domain administrator account that installed the software into the administrative user group. The administrator will be called the Initial cell administrator, and the CRS service account. A third user that is added is the Java WebReporting account.

These 3 default accounts can be removed if required, as long as another account has been defined with access to all Data Protector clients and user rights.

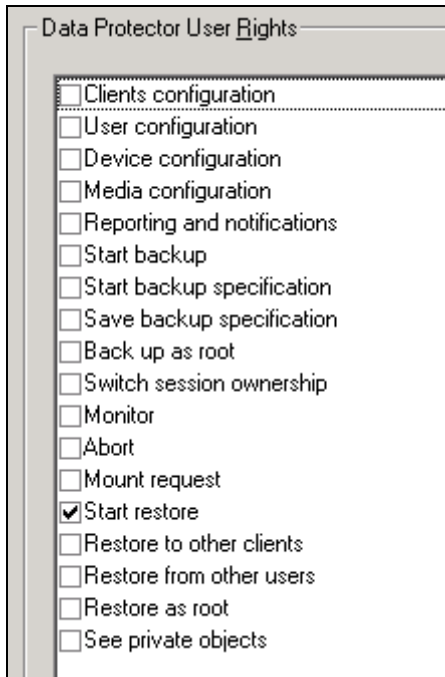
The Administrator has the following default user rights:



The Operator has the following default user rights:



The User has the following default user rights:



New user groups can be created with custom user rights.

## Using a service account

The CRS service on windows has an owner assigned with certain permissions and a password, which needs to be updated if the user password changes. Use a dedicated service account if you do not want to change the passwords.

## Wild-card user

Caution: For security reasons, it is not recommended to add a wild-card user. It is only recommended for use in test environments.

Adding an `any` user with access to `any` client in Data Protector will give any local or domain administrator access to all clients on the network with all Data Protector related user rights. This opens up Data Protector access to any user for any client on the network.

**Note:** Instead of `any`, you can use an asterix (\*).



To add the any user, click on **Add User**, then fill in **Any** under **Name, Domain** and/or **Client**:

Name	Group/Domain	Client System	Description
ADMINISTRATOR	MUGGY	muggy.xst.rose.hp.com	CRS service account
ADMINISTRATOR	MUGGY	<Any>	Initial cell administrator
java	applet	webreporting	WebReporting
SYSTEM	NT AUTHORITY	muggy.xst.rose.hp.com	Local System account on t...

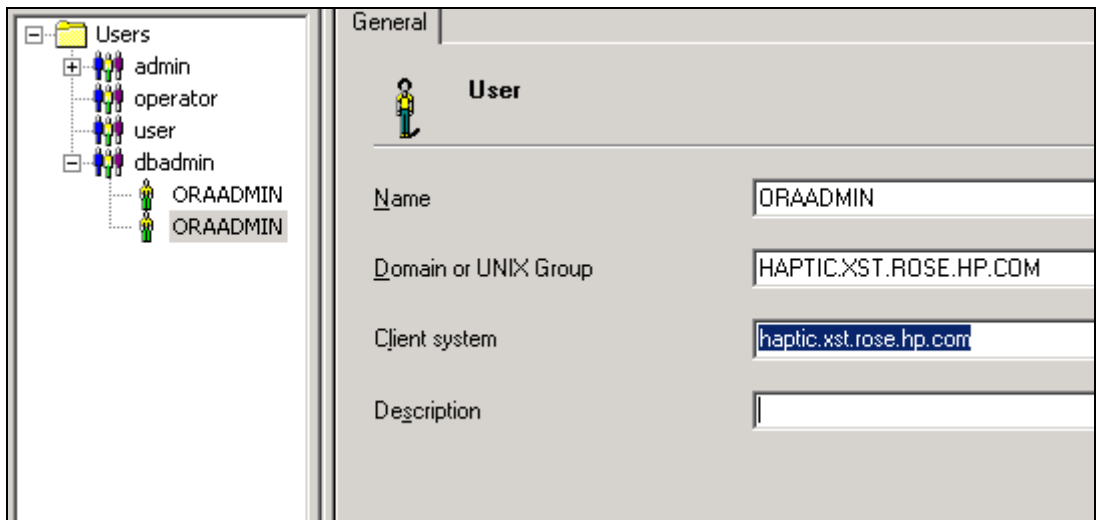
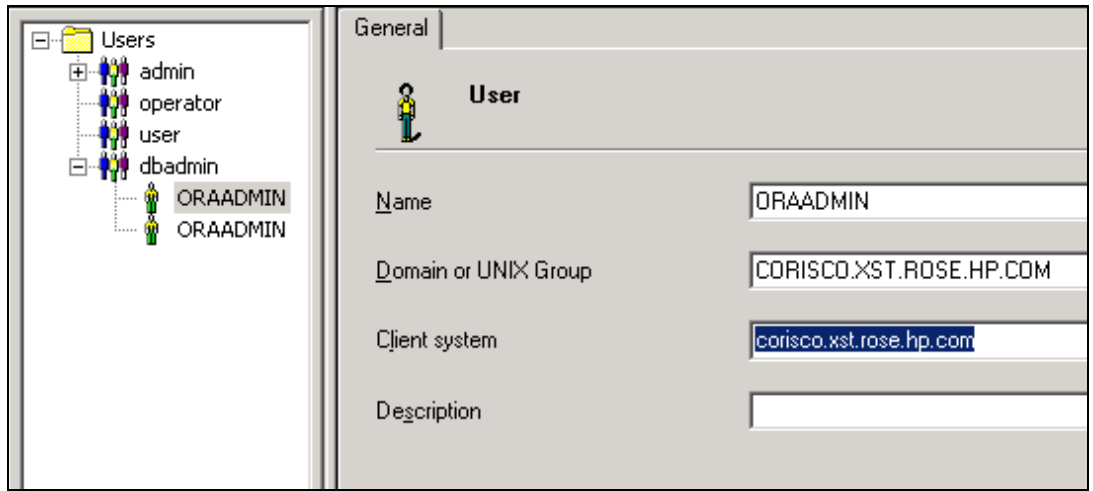
## About user management

Data Protector users are based on the operating system user.

Data Protector backup session ownership is based on a session level. This means that if there are multiple clients in a session or backup spec, it is not possible to split the ownership. Backup specifications need to be organized so there are never two clients with different owners in the same backup spec.

The user responsible for filesystem backups (fsadmin) is able to see and restore the Oracle DB on the same server, because all Data Protector database integrations have the option **public** set by default, which allows all users to see the data. Once the public option is unchecked in the Oracle backup specification, only the correct owner (dbadmin) is allowed to see and restore the data.

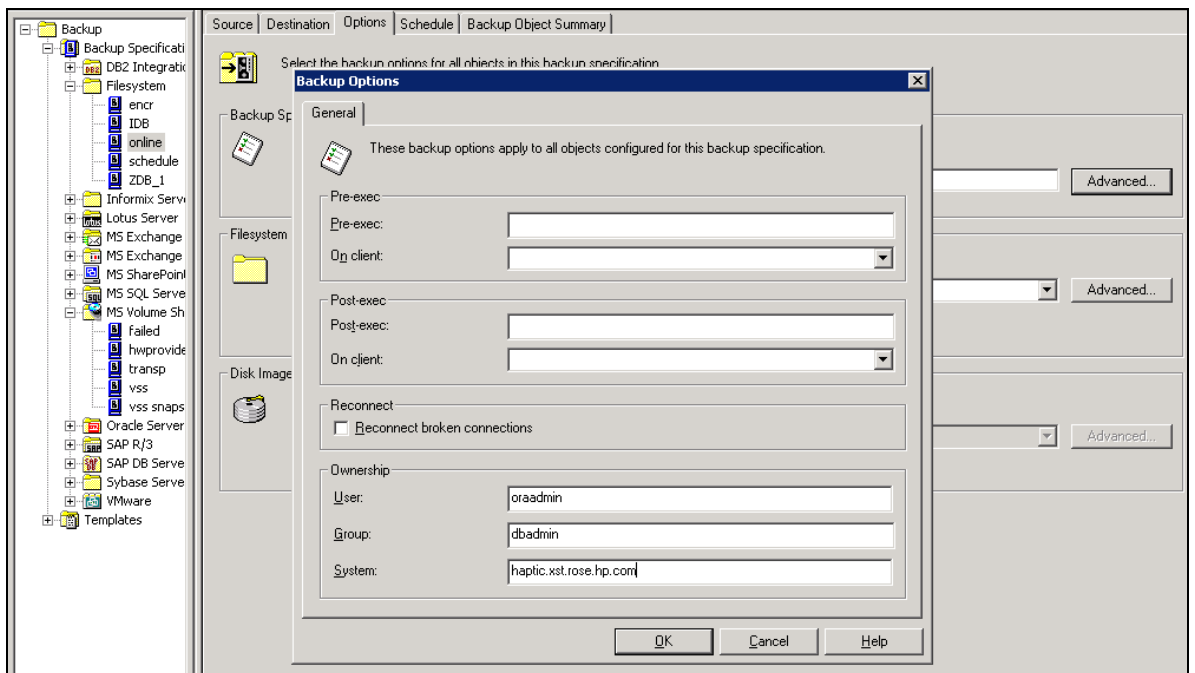
You cannot specify more than one client system for a user. If a user needs to access several client systems, add the same user multiple times. In the example below, the user has rights to access the client system Corisco, as well as the client system Haptic.



**Note:** It is probably easier to directly modify the

C:\ProgramData\OmniBack\Config\Server\users\userlist file to add batches of users than to do it through the GUI.

**Note:** You cannot enter more than one System for the **Ownership** of a backup specification:



RMAN, in conjunction with the Data Protector oracle integration, can perform backups and restores. In order for RMAN initiated backups and restores to be successful, you need to add certain other users to Data Protector:

- For Data Protector 6.1 on UNIX systems, add the users root and the oradba account. For Oracle, you need to add the RAC root and oracle dba account.
- For Data Protector 6.11 on UNIX systems, you only need to add the oradba account. The root account is no longer needed by the Oracle integration in Data Protector 6.11.
- For Data Protector 6.1 and Data Protector 6.11 on Windows systems, add the account used to install the Oracle software as a Data Protector user.

The **Group** field in the ownership part of the backup specification does not correspond to a user group; it corresponds to a UNIX user's group or to a Windows domain name. In Data Protector, a Data Protector user always corresponds to an Operating System user. For example, you can see the ownership of a backup when you look at the session list for the last day using the command `omnidb -session -last 1`:

```
C:\Program Files\OmniBack\bin>omnidb -session -last 1
SessionID      Type          Status        User.Group@Host
-----
2009/09/22-1   Backup       Aborted       HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-2   Backup       Failed        HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-3   Backup       Aborted       HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-4   Backup       Completed     HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-5   Backup       Completed     HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-6   Backup       Failed        HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-7   Backup       Aborted       HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-8   Backup       Completed     HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/22-9   Backup       Completed     XST\MOMADMIN@haptic.xst.rose.hp.com
```

Notice the column [User.Group@Host](#).

You can see that there are 2 different users: local Haptic administrator and domain XST momadmin. The domain name is what you need to enter in the Group field in the ownership part of the backup specification.

Data Protector does not have the functionality to add groups of users to the ownership part of a backup specification. The current Data Protector functionality does not allow a Data Protector user to be added for groups of systems. It is possible to separate users and what they see and are allowed to do, using templates.

If you have selected the user right "See Private Objects", the user can see and restore private objects, but can only restore files that the user backed up. If the user needs to be able to restore from one of the scheduled backups, define the user as the owner of the backup specification. This will allow the user to browse and restore the data. Refer to the on-line help index "ownership" for details.

It is possible to backup other clients with "Start Backup" being the only user right selected. According to the help for the "Start Backup" user right, you should only be able to backup your own client. I thought maybe Data Protector was getting some rights from the operating system, since this ID had admin rights on the operating system, so I moved this ID from administrator to user and I can still backup/restore other clients data.

## Device management

This chapter describes common media management tasks, and hints and tips for media management.

### Poor media

*When are media marked poor?*

Data Protector media management automatically selects the most appropriate media for backup. Basic media selection criteria:

- If available, media in good condition are used first.
- Media in fair condition are used only if no media in good condition are available.
- Media in poor condition are not selected for backup.
- Media are always selected from the specified pool. If the pool does not contain unprotected media, Data Protector accesses a free pool (if configured).

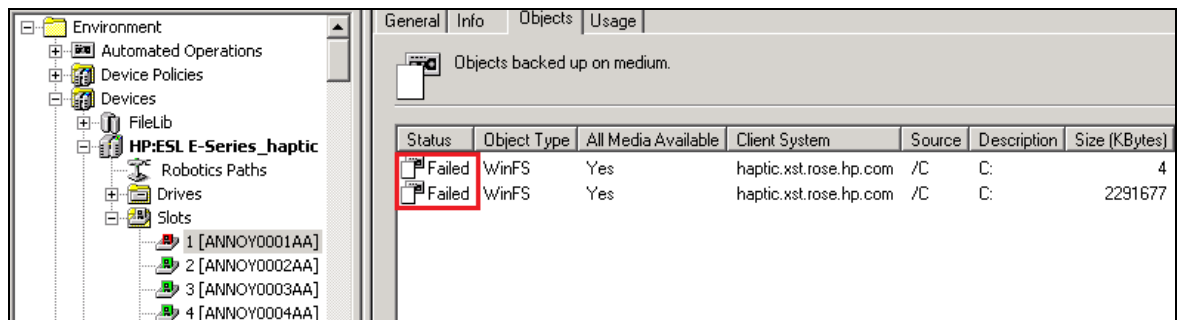
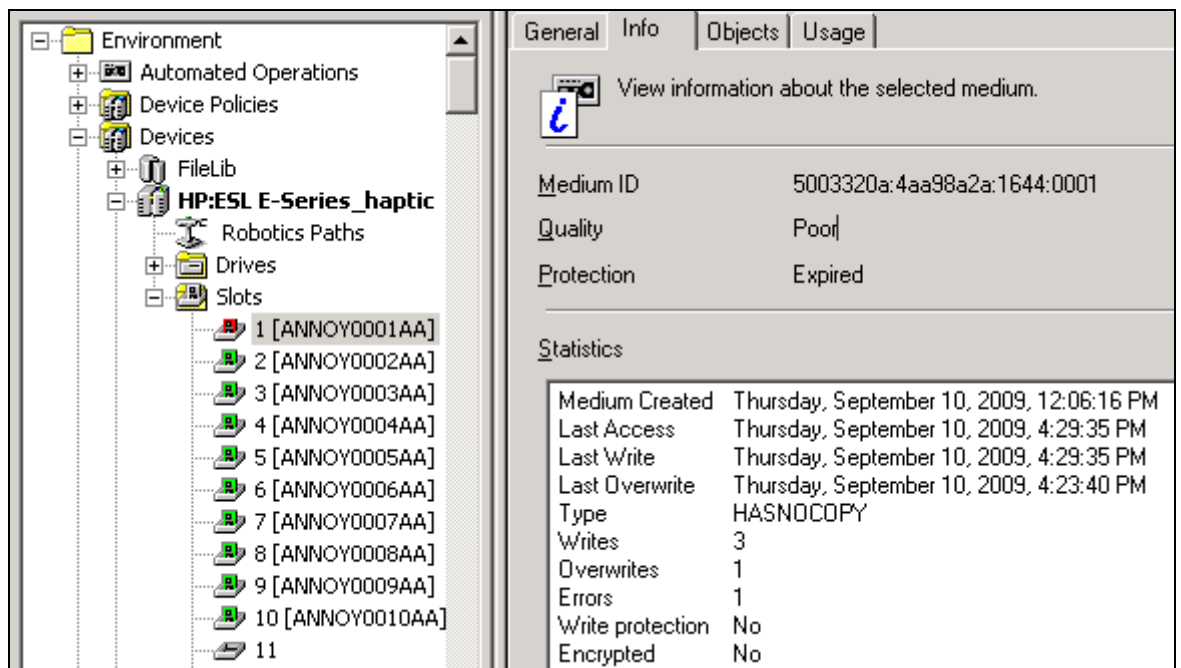
Heavy usage and age result in an increased number of read and write errors with tape media. You need to replace media marked as POOR. This media status means that the threshold for age or usage has been exceeded, or read/write errors have occurred on the tape.

*What to do with media marked poor?*

It is recommended that you investigate why media are marked poor. If a tape is marked as poor due to a device error, you can verify the tape to check and change its condition. If the error was due to a dirty drive, clean the drive and verify the tape to reset its condition. You can use Verify to get more information on each tape's condition. It is not recommended to simply recycle the tape. Rerun the failed backup session to a different tape.

Tapes that are accidentally poor (because of SAN or drive issues) can be switched back to normal using the command `omnimmm -reset_poor_medium id`.

The following screenshots show an example of a tape that is marked poor:



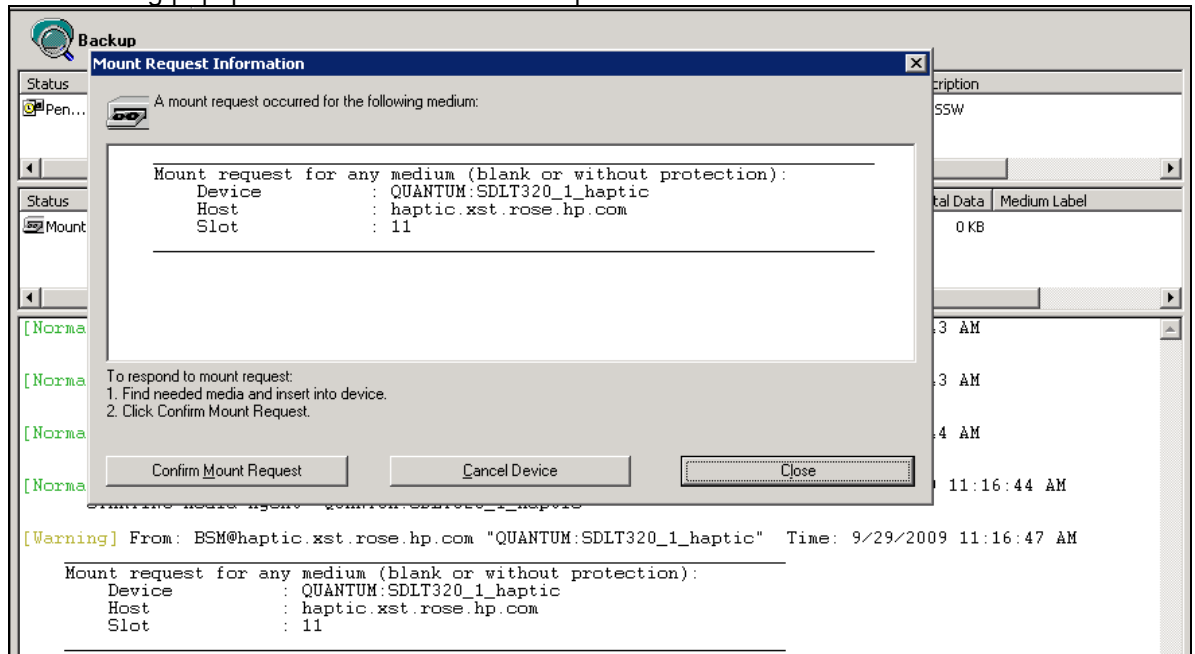
## Resolving mount requests

Data Protector issues a mount request if either it requires a specific medium to read data from, or it needs more media but none are available in the device.

To resolve the mount request, add additional media or cancel the device:

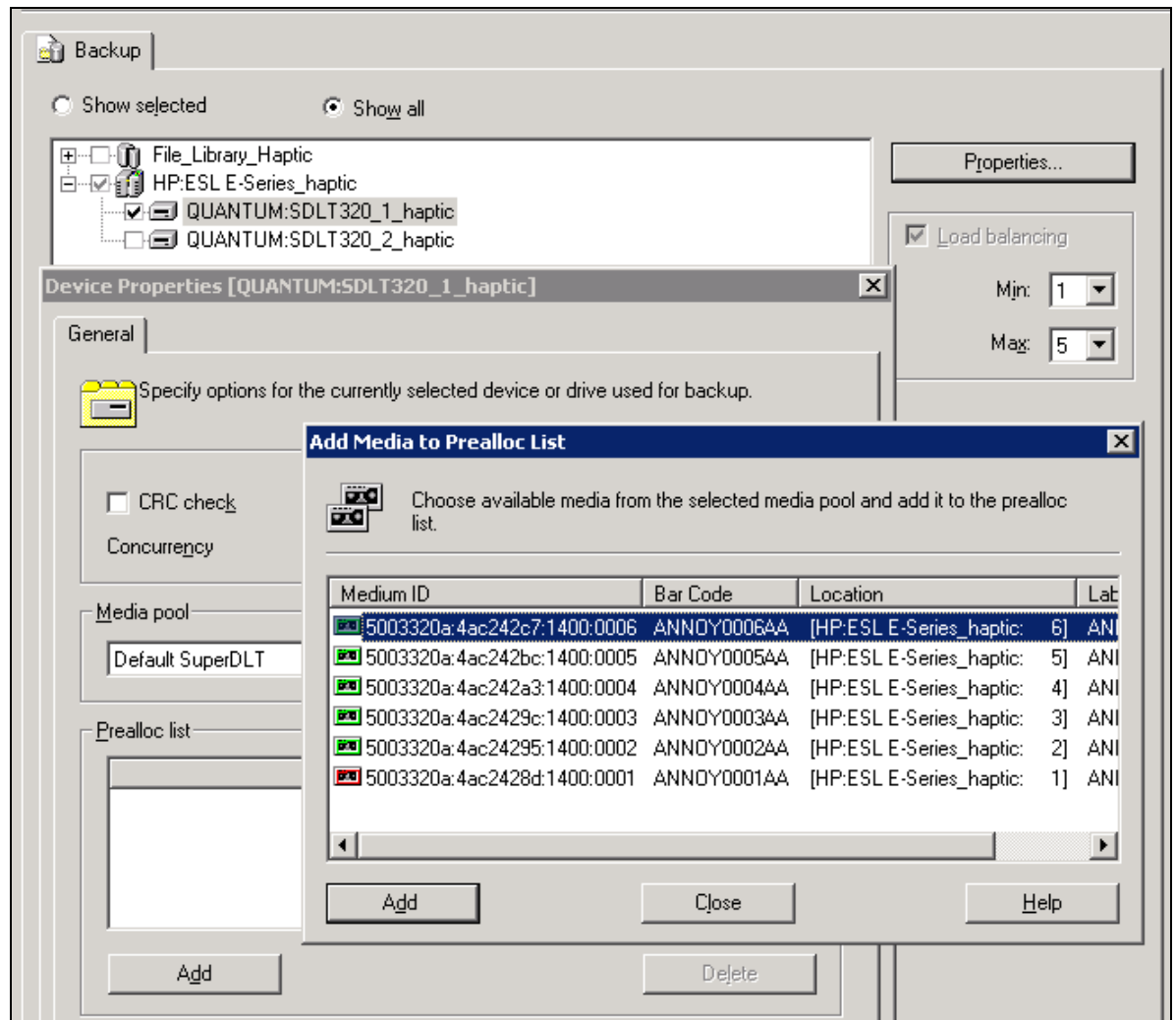
- To confirm the mount request, insert the required medium into the device and click **Confirm Mount Request**. Alternatively, use `omnimnt` on the Data Protector CLI to confirm the mount request.
- To cancel the device with the mount request, click **Cancel Device**. The data specified for that device will not be backed up, restored, or copied.

The following popup will show when a mount request is issued:



When a pool has poor media in it, and a mount request is issued, use the media pre-allocation list to specify which media to use. Click on the device properties, and add the media that needs to be allocated.

The following screenshot shows the media that is added to the pre-allocation list:



## Using a free pool

A free pool is a media pool that you can configure to allow free media to be shared across media pools, which may reduce operator intervention due to mount requests. The use of a free pool is optional.

A free pool:

- cannot be deleted if it is linked with a media pool or if it is not empty.
- is different from a regular pool as it cannot be used for allocation because it cannot hold protected media. Consequently, allocation policy options (Strict / Loose, Appendable/Non-Appendable) are not available.
- contains only free Data Protector media (no unknown or blank media).

Media are moved between the regular pool and the free pool on two occasions:

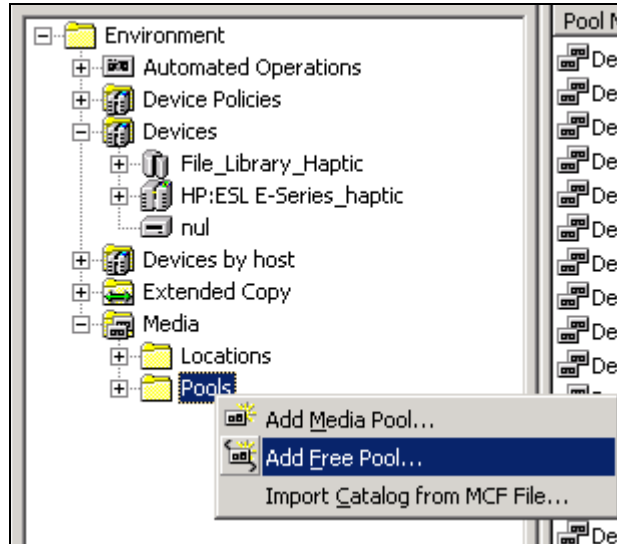
- If there is no free media in the regular pool anymore, Data Protector allocates media from the free pool. This automatically moves the media to the regular pool.
- When all the data on the media expires (and the media is in a regular pool), media can be moved to the free pool automatically.

*Limitations:*

- You cannot move protected media to a free pool.
- You cannot use some operations on media, such as Import, Copy, and Recycle, because they may operate on protected media.
- Pools with the Magazine support option selected cannot use a free pool.

- You may experience some temporary inconsistencies (1 day) in pools when using free pools (for example when there is an unprotected medium in a regular pool waiting for de-allocation to the free pool).
- If a free pool contains media with different data format types, Data Protector automatically reformats allocated media if necessary. For example, NDMP media may be reformatted to normal media.

To create a free pool, right-click on **Media, Pools** and select **Free Pool**. Follow the wizard to define the pool properties.



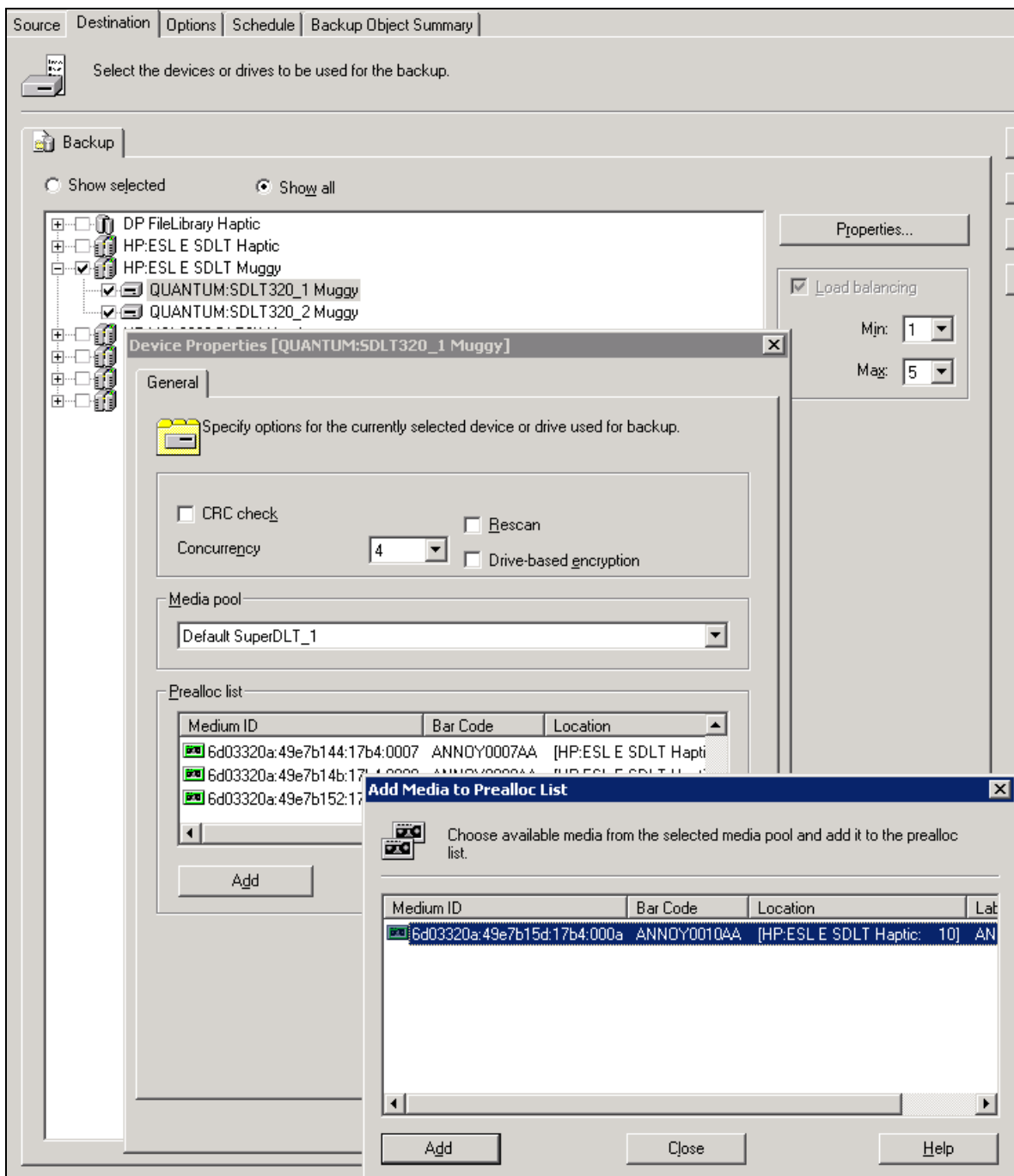
**Note:** Each media type (such as SDLT or LTO) needs to have its own free pool.

On the tape pool, append the free pool with the same media type:



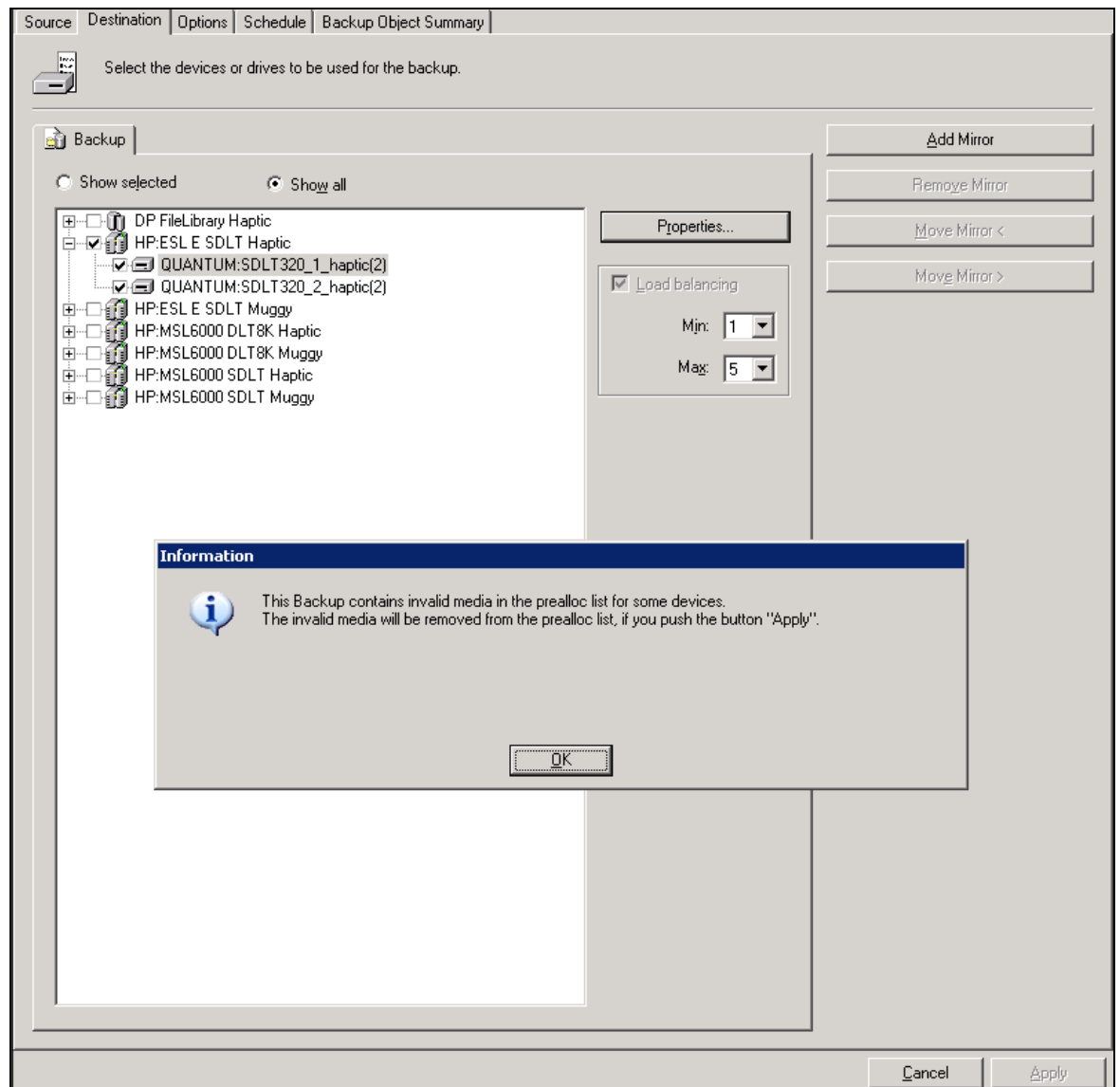
## Using media preallocation list

In the backup specification, under the tape drive properties, select media from the list and add it to the pre-allocation list:





**Note:** Invalid media will be removed by Data Protector:



## Backup management

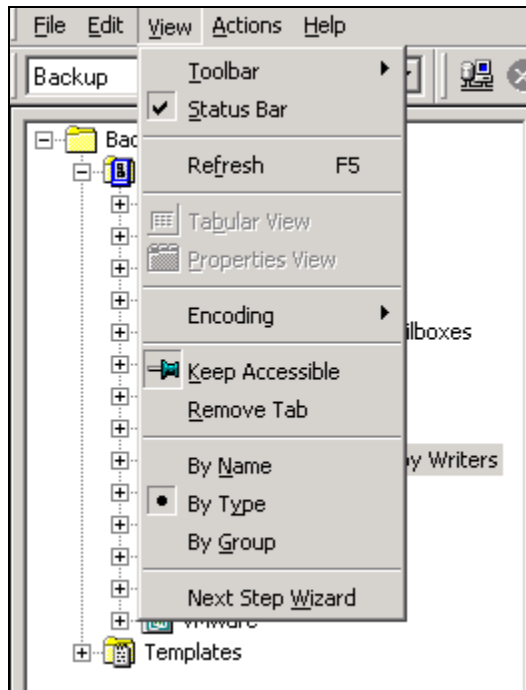
This chapter covers hints and tips about common backup management tasks, for instance creating and viewing a backup specification, and soon. It explains a few HP Data Protector internals, such as using drive concurrency and multiplexing. It describes how to configure and run reports, how to monitor backup sessions, and how to resolve failed sessions.

### Viewing the backup specifications

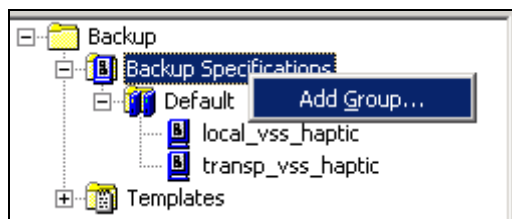
Backup specifications can be viewed in three different ways:

- By Name
- By Type
- By Group

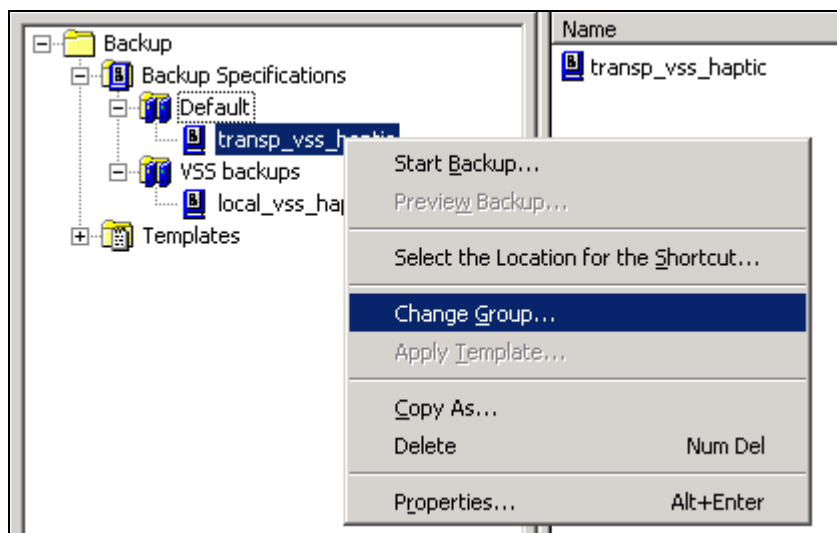
Click on the **View** menu to select what criteria to use for viewing the backup specifications:



Right-click to add a group, and specify the name of the new group:



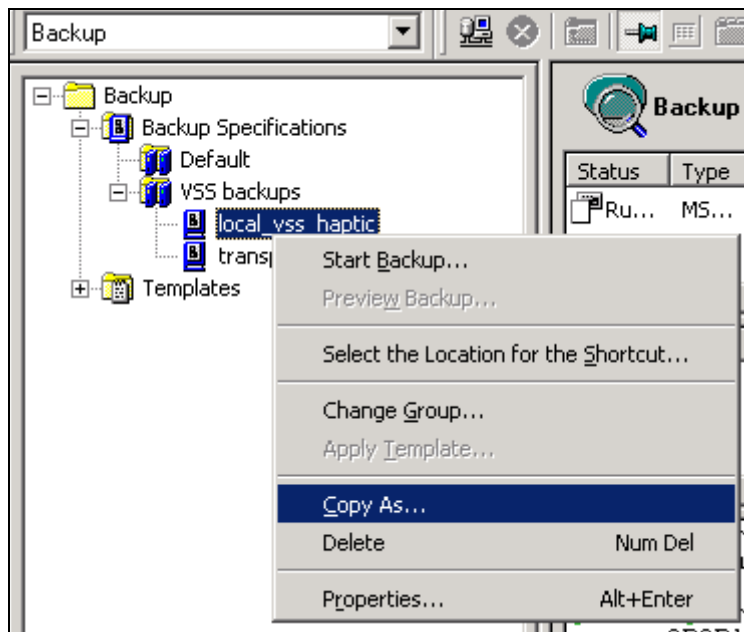
Click **Change-Group...** to move backup specifications into their dedicated groups:



## Adding a new backup specification

An existing backup specification can be quickly copied and edited through the Data Protector GUI. Edit the parameters that you want to change after copying the backup specification, for example, changing full to incremental backup, altering the backup schedule, and so on.

To copy a backup specification, right-click and chose **Copy As...**:



## Using drive concurrency

The number of Disk Agents started for each Media Agent is called Disk Agent (backup) concurrency and can be modified using the Advanced options for the device or when configuring a backup.

Note: The concurrency set in the backup specification takes precedence over the concurrency set in the device definition.

Data Protector provides a default number of Disk Agents that are sufficient for most cases. For example, on a standard DDS device, two Disk Agents send enough data for the device to stream. For library devices with multiple drives where each drive is controlled by one Media Agent, you can set the concurrency for each drive independently.

If properly set, backup concurrency increases backup performance. For example, if you have a library device with four drives, each controlled by a Media Agent and each Media Agent receives data from two Disk Agents concurrently, data from eight disks is backed up simultaneously.

You can concurrently back up parts of a disk to multiple devices. This method speeds up the backup and is useful for backing up very large and fast disks to relatively slow devices. Multiple Disk Agents read data from the disk in parallel and send the data to multiple Media Agents.

Note that concurrency can correspondingly *decrease* restore performance. If one mount point is backed up through many Disk Agents, the data will be contained in multiple objects. To restore the whole mount point you have to define all parts of the mount point in a single backup specification and then restore the entire session.

When you back up large objects, you can speed up your backup by using multiple Disk Agents. In the backup specification, you have to manually define which directories/files will be backed up using a new Disk Agent. You should take care to avoid overlapping the same data. If more than one Disk Agent is concurrently accessing the same disk, the performance of retrieving data from the disk will drop. This can be different when using disk arrays.

## Order of Disk Agents started

Data Protector has 2 backup modes: SAN Backup mode, and LAN Backup mode.

1. If you do a SAN backup, Data Protector always tries to run local backups. It will fill up all slots of a running local Media Agents with available Disk Agent slots.

Example:

- Server A – FS1, FS2, FS3 Local (SAN attached) Device D1 with concurrency 4
- Server B – FS4, FS5, FS6 Local (SAN attached) Device D2 with concurrency 4

So Device D1 with concurrency 4 backs up FS1 to FS4, which means for FS4, Data Protector runs a Network (LAN) backup. Then Data Protector starts D2 to backup FS5 and FS6 for a SAN backup.

2. In case of a LAN backup, Data Protector always tries to reduce the load of a Server. So it starts only 1 Disk Agent per server, and picks up the next one until all slots are all filled up.

Example:

Server A – FS1, FS2, FS3

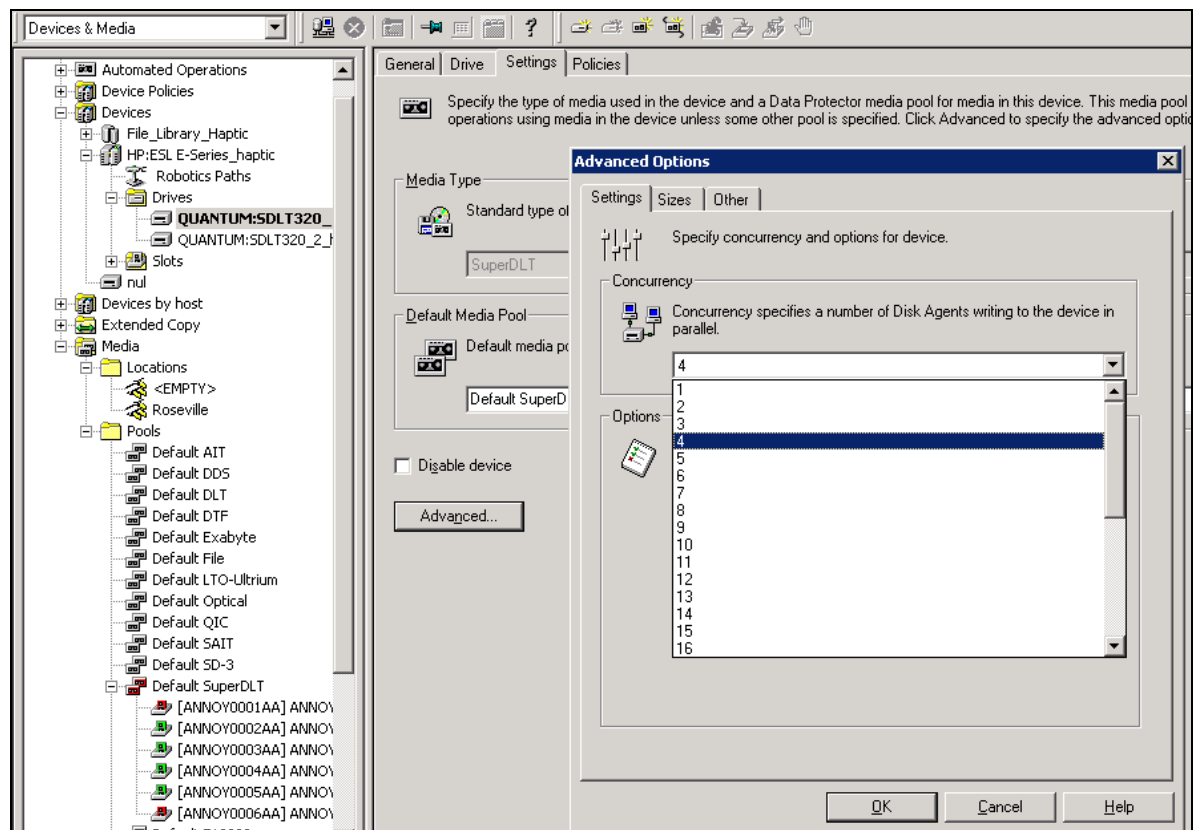
Server B – FS4, FS5, FS6

Server C – Media Agent host with D1 and D2 concurrency 2

D1 will start and backup FS1 and FS4. Then D2 will start (together with D1) and backup FS2 and FS4. The first free slot will backup FS3 and FS6.

## Defining drive-based concurrency

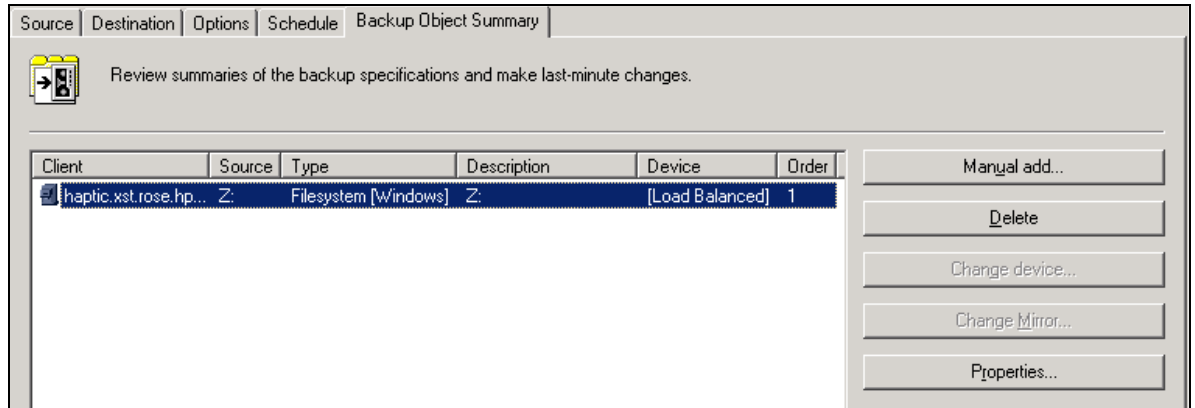
Go to the drive **Advanced Options, Settings**, and specify the number of Disk Agents to be used by default for the drive. The Data Protector default value is 4.



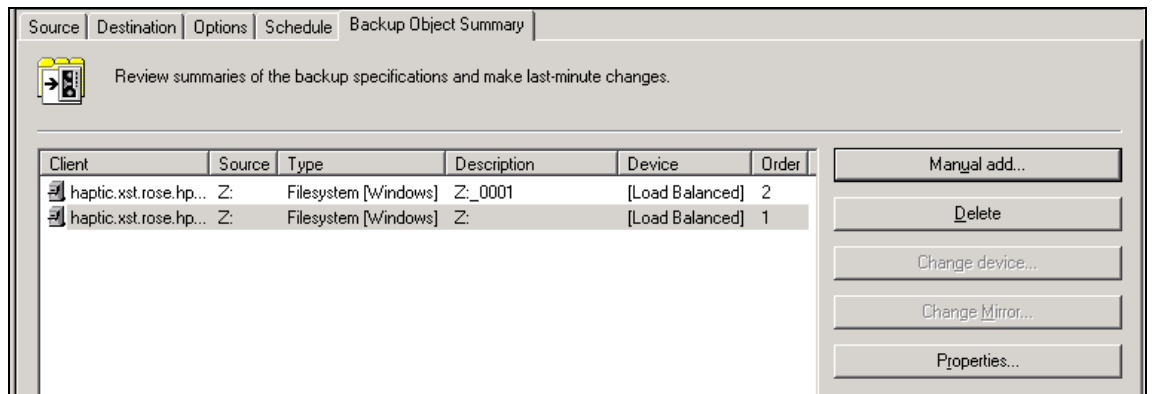
## Defining backup specification-based drive concurrency

The backup object summary shows the number of Disk Agents configured for a filesystem backup specification.

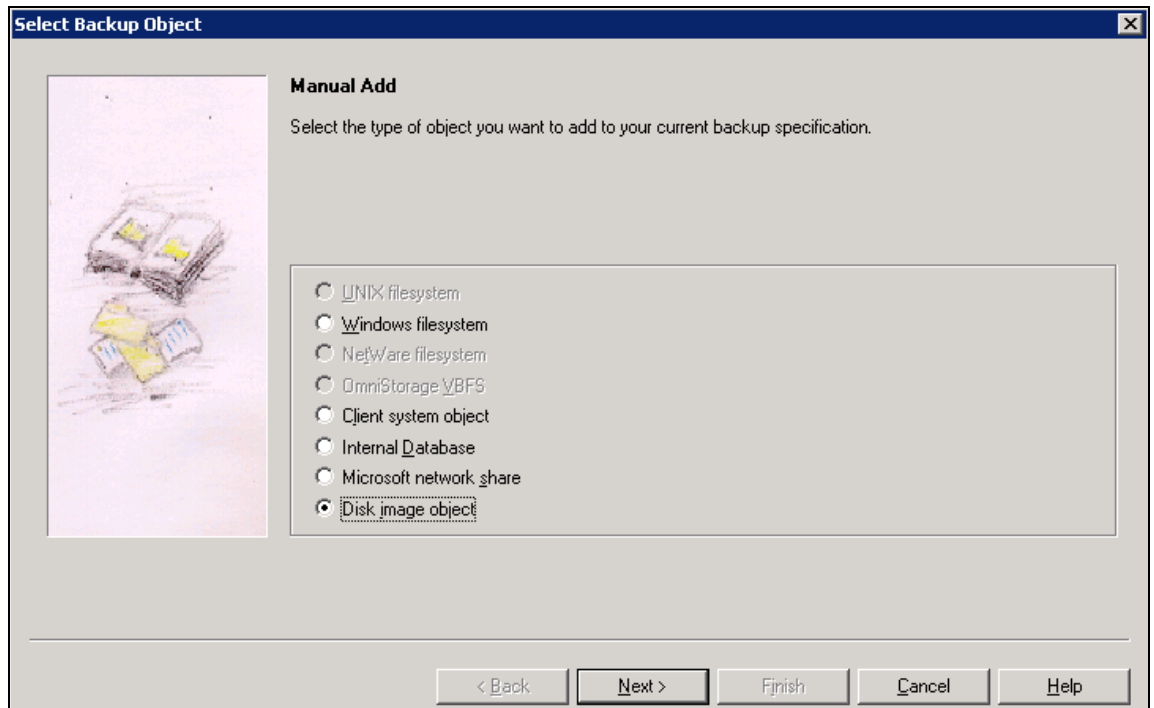
To add a new Disk Agent, go through the **Manual add...** option, and follow the wizard to specify the filesystem backup details:



Chose which type of object is used for the backup specification. Then select the client and mount point, optional filters and reporting parameters, advanced properties and other filesystem options. If you select the same properties as the original filesystem properties, a new unique name will be created for the copy:



**Note:** You can also specify a new raw disk partition via this option in the GUI. Click on **Manual Add**, and chose a **Disk Image Object**.



## About multiplexing

Multiplexed media contain interleaved data of multiple objects. Such media may arise from backup sessions with a device concurrency of more than 1. Multiplexed media may compromise the privacy of backups and require more time for restore.

Using the Data Protector object copy functionality, you can demultiplex media. Objects from a multiplexed medium are copied to several media. Data Protector however reads the source medium only once. To enable demultiplexing of all objects on the medium, the minimum number of destination devices needed for the operation is the same as the device concurrency that was used for writing the objects. If fewer devices are available, some objects will still be multiplexed on the target medium.

During the copy operation definition, a number of parameters can be customized for backup and catalog protection, recycling source copies, and ejecting media after a successful copy:

### Automated Copy Operation - Options

You can change copy options.

---

**Source object options:**

Change data and catalog protection after successful copy

Recycle data and catalog protection of failed source objects after successful copy  
Note: Failed source objects are not copied

---

**Target object options:**

**Protection:**

Same as source

**Catalog protection:**

Same as source

**Logging:**

Log All

---

**Target media options:**

Eject target media after successful copy

**Location:**

Schedule the copy session, or launch an interactive copy. The post-backup copy session will run after the backup session has been completed.

For an interactive copy, chose the session that needs to be copied:

**Save as...**  
Save the newly created specification...

**Start interactive copy...**  
Start an interactive session with...

**Start Copy**

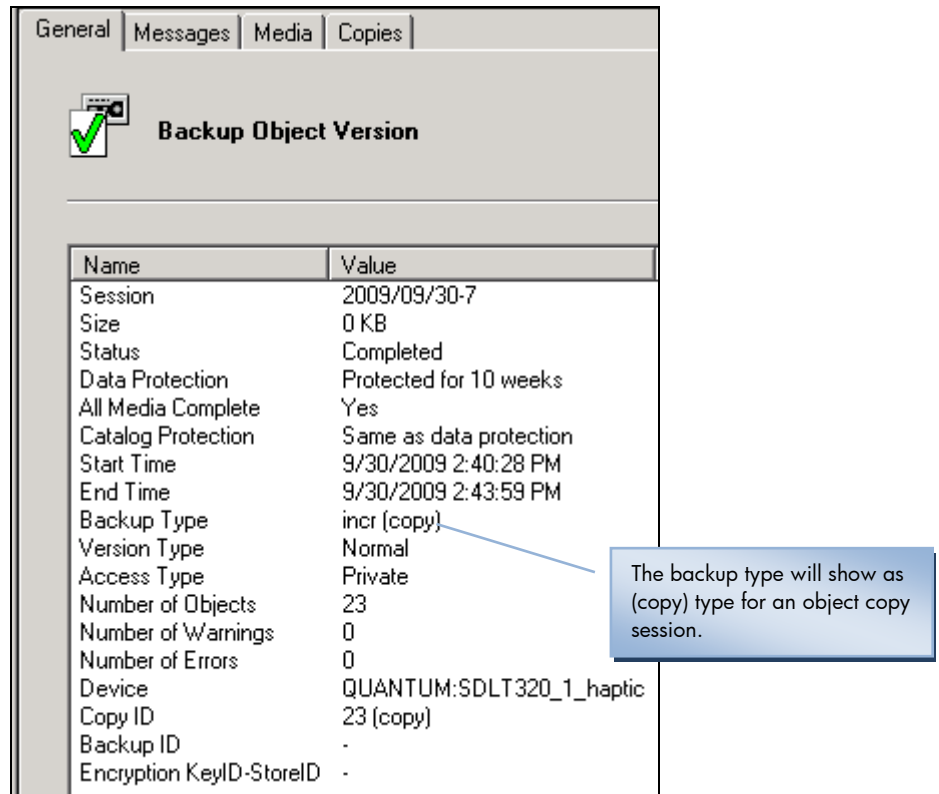
Select session.

Session: 2009/09/29-14

Session ID	Type	Status	Start Time	End Time	Backup Type	Application Type	Specificat
2009/09/29-14	Backup	Completed	9/29/2009 12:37:18 PM	9/29/2009 12:39:42 PM	incr	Filesystem	zdb_hapt
2009/09/29-13	Backup	Completed	9/29/2009 12:28:47 PM	9/29/2009 12:32:18 PM	full	Filesystem	zdb_hapt
2009/09/29-12	Backup	Completed/Failures	9/29/2009 12:22:29 PM	9/29/2009 12:25:51 PM	full	Filesystem	zdb_hapt
2009/09/29-11	Backup	Completed/Failures	9/29/2009 12:06:11 PM	9/29/2009 12:10:00 PM	full	MS Volume Shadow Copy Writers	local_yss
2009/09/29-10	Backup	Completed	9/29/2009 11:51:33 AM	9/29/2009 11:52:01 AM	full	Filesystem	nul_hapt
2009/09/29-9	Backup	Completed	9/29/2009 11:50:00 AM	9/29/2009 11:50:33 AM	full	Filesystem	Interactiv
2009/09/29-7	Backup	Completed	9/29/2009 11:06:12 AM	9/29/2009 11:09:29 AM	full	MS Volume Shadow Copy Writers	local_yss
2009/09/29-6	Backup	Completed/Failures	9/29/2009 10:46:05 AM	9/29/2009 10:49:29 AM	full	MS Volume Shadow Copy Writers	local_yss
2009/09/29-5	Backup	Completed/Failures	9/29/2009 10:36:19 AM	9/29/2009 10:39:40 AM	full	MS Volume Shadow Copy Writers	transp_v
2009/09/29-4	Backup	Completed/Failures	9/29/2009 10:23:44 AM	9/29/2009 10:24:55 AM	full	MS Volume Shadow Copy Writers	local_yss

Select the source session version from the interactive copy wizard.

After the session has run successfully, the session messages in the IDB will show a **(copy)** backup type:



Name	Value
Session	2009/09/30-7
Size	0 KB
Status	Completed
Data Protection	Protected for 10 weeks
All Media Complete	Yes
Catalog Protection	Same as data protection
Start Time	9/30/2009 2:40:28 PM
End Time	9/30/2009 2:43:59 PM
Backup Type	incr (copy)
Version Type	Normal
Access Type	Private
Number of Objects	23
Number of Warnings	0
Number of Errors	0
Device	QUANTUM:SDLT320_1_haptic
Copy ID	23 (copy)
Backup ID	-
Encryption KeyID-StoreID	-

## Object copy

The Data Protector object copy functionality enables you to copy selected object versions to a specific media set. You can select object versions from one or several backup sessions or object consolidation sessions. During the object copy session, Data Protector reads the backed up data from the source media, transfers the data, and writes it to the target media.

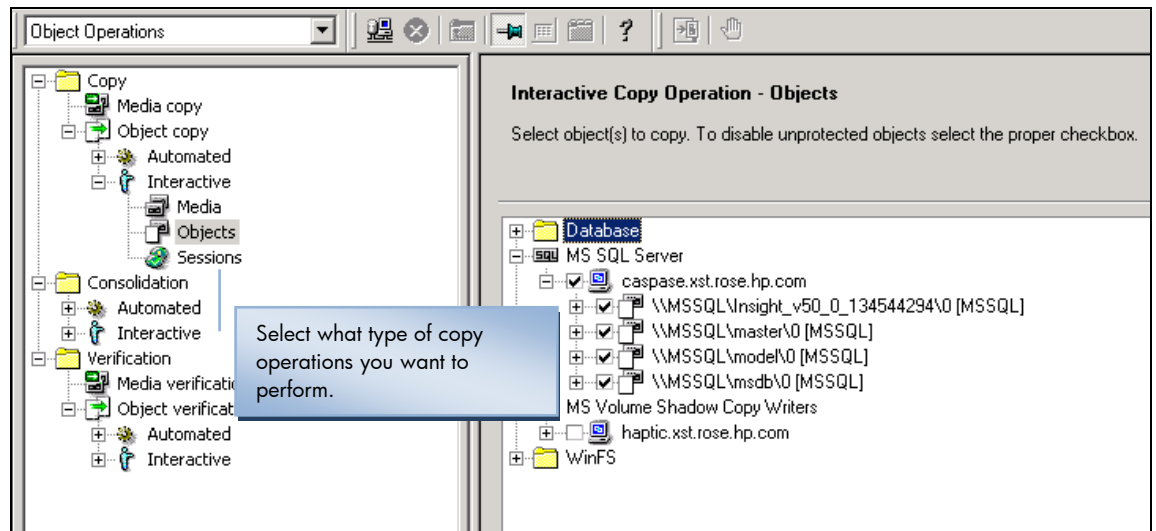
The result of an object copy session is a media set that contains copies of the object versions you specified.

Additional copies of backed up data are created for multiple purposes:

- Vaulting. You can make copies of backed up objects and keep them in several locations.
- Freeing media. To keep only protected object versions on media, you can copy such object versions, and then leave the medium for overwriting.
- Demultiplexing of media. You can copy objects to eliminate interleaving of data.
- Consolidating a restore chain. You can copy all object versions needed for a restore to one media set.
- Migration to another media type. You can copy your backups to media of a different type.
- Support of advanced backup concepts. You can use backup concepts such as disk staging.



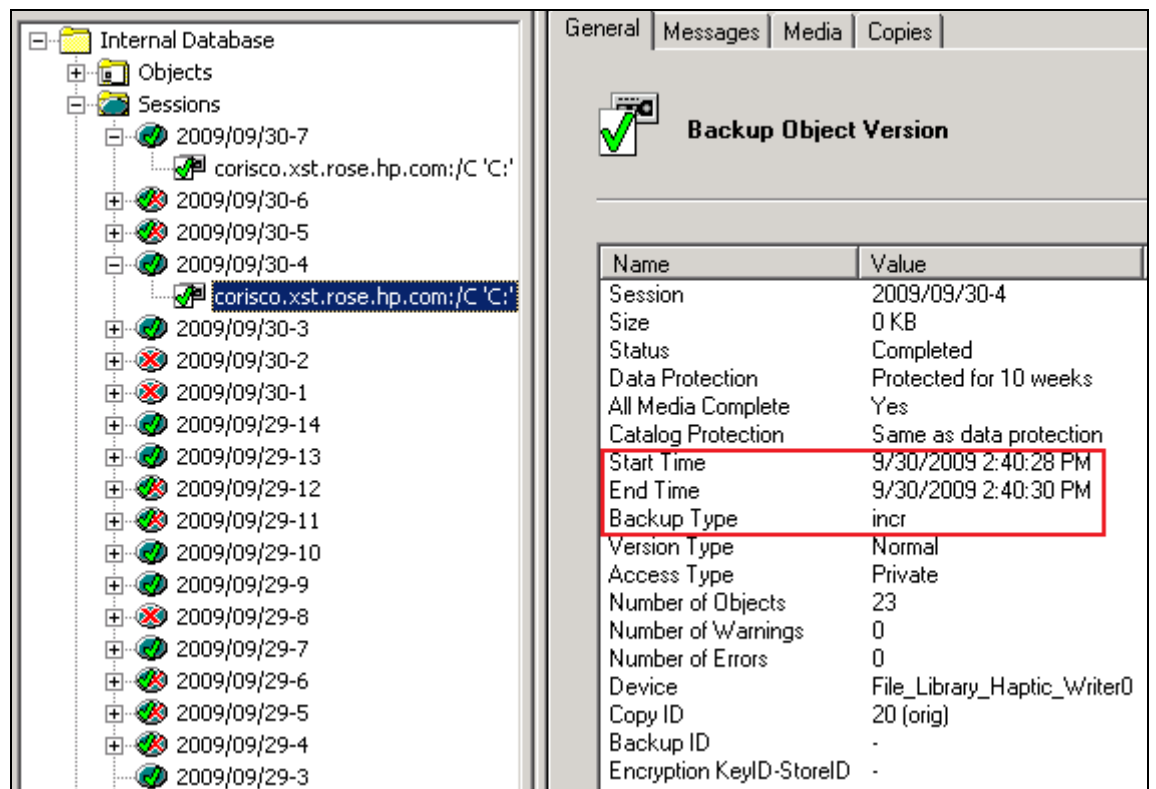
Object copy sessions can be run interactively, or scheduled, based on media, sessions, or objects.

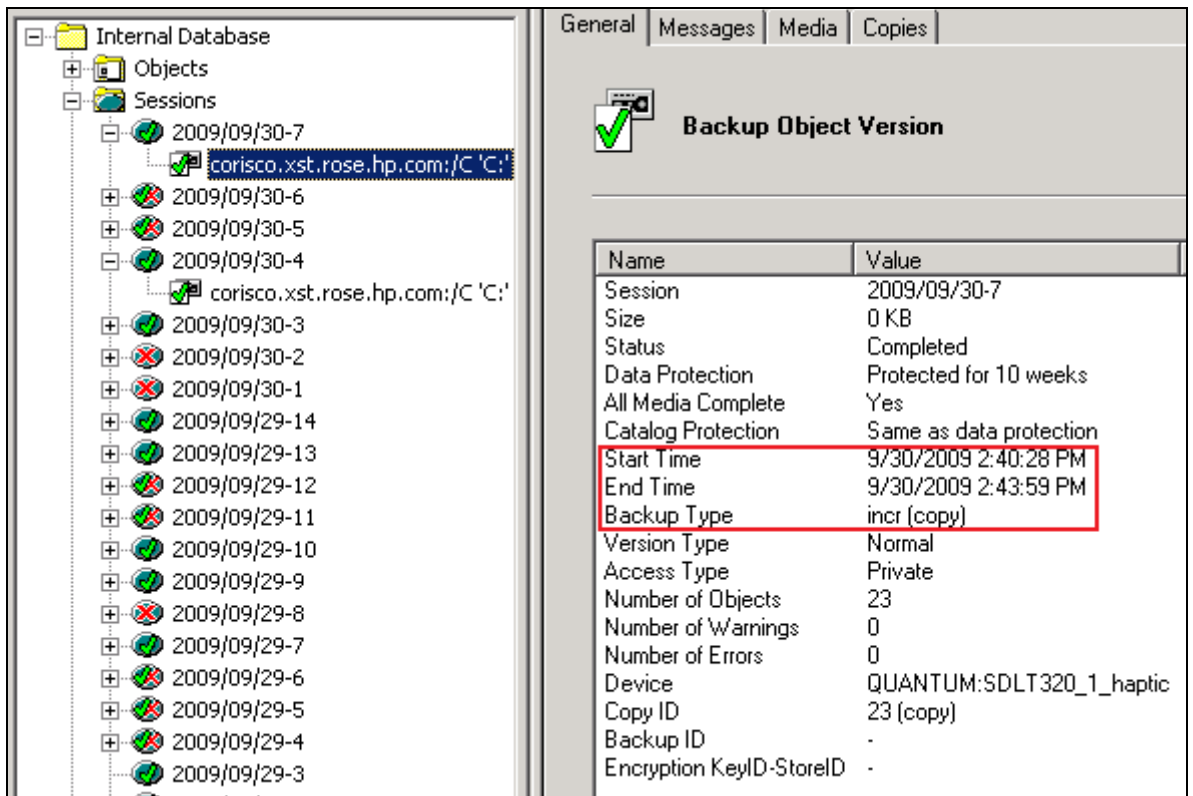


**Note:**  
See the *HP Data Protector concepts guide (B6960-90151)* for further information on object copy.

## Copy session start time

The copy session start time will always be the time of the original backup session.

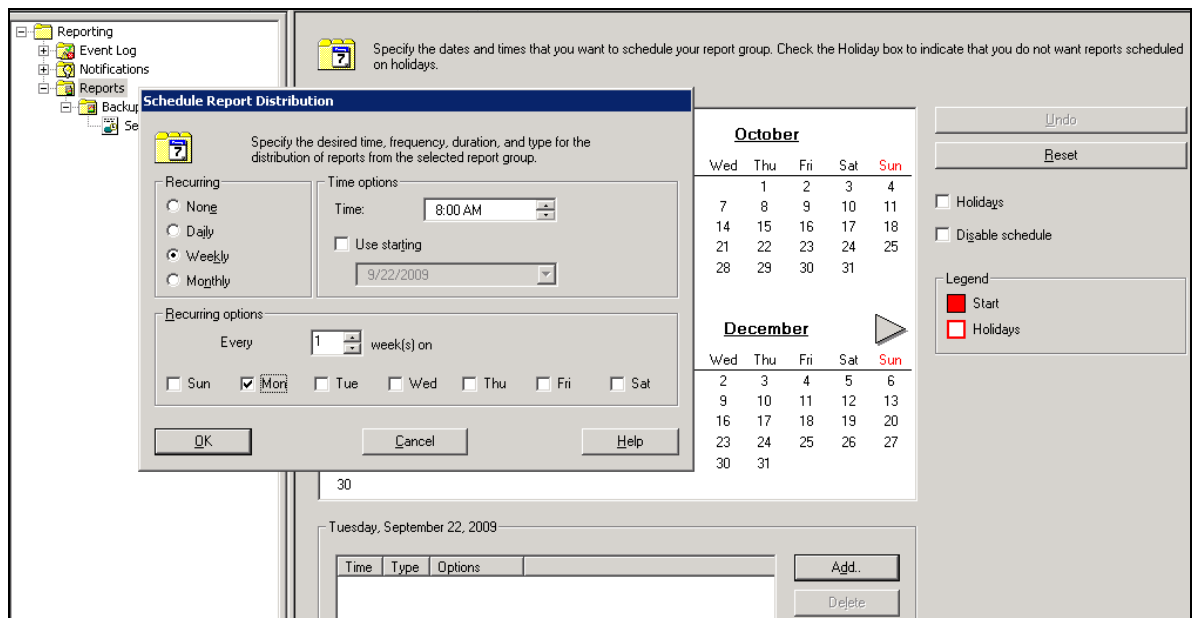




It is not possible to calculate the exact duration of an object copy on a per object level.

## Emailing backup session reports

A schedule can be added at the report *group* level. If only 1 report needs to be scheduled to be sent, create a different group with a single report for each schedule.



## Setting up webbased reporting

Data Protector's web-based reporting allows you to view reports on backup, object copy, and object consolidation status and Data Protector configuration, using the web-interface.

From the system that has the Data Protector GUI installed, copy the following directory with all subdirectories to the web server:

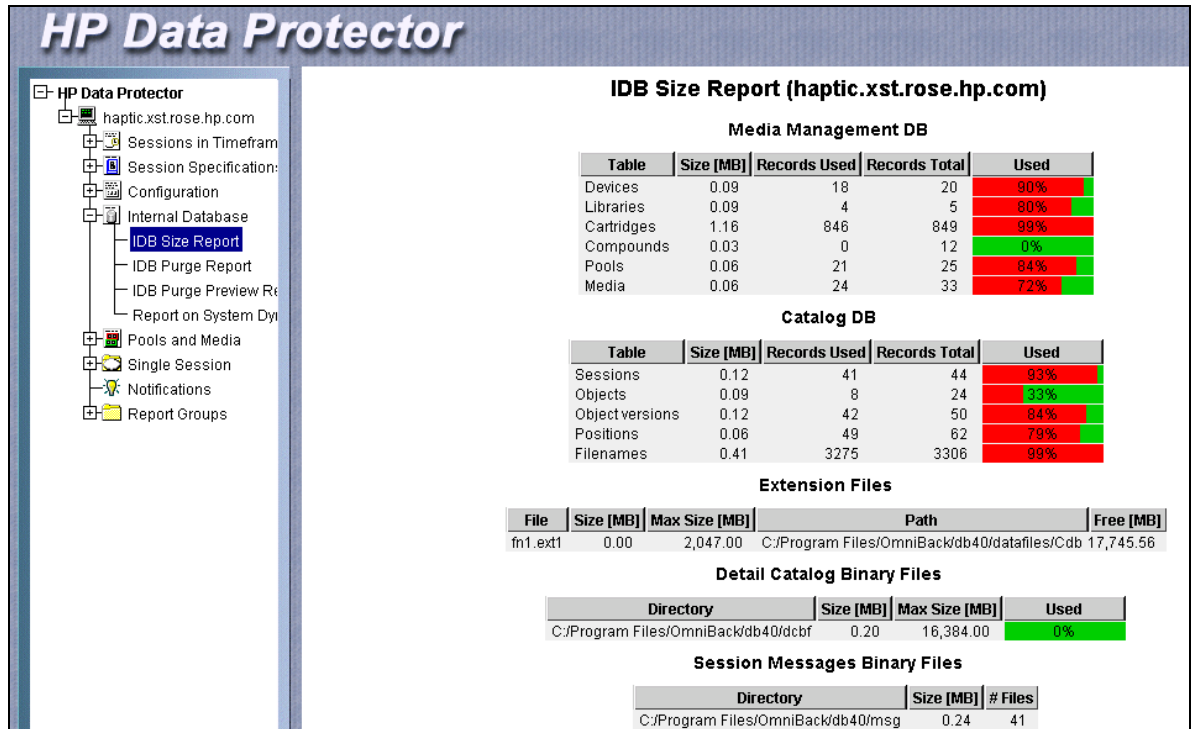
- **UNIX:** /opt/omni/java/bin
- **Windows:** C:\Program Files\Omniback\java\bin

In a browser on any system with access to the web server, open the following file from the copied java folder on the web server to display the Data Protector reporting:

- **UNIX:** /bin/webreporting.html
- **Windows:** C:\Program Files\Omniback\bin\WebReporting.html

Make this file available to the users of the web reporting in the full URL form. For example, put a link to this file from your Intranet site.

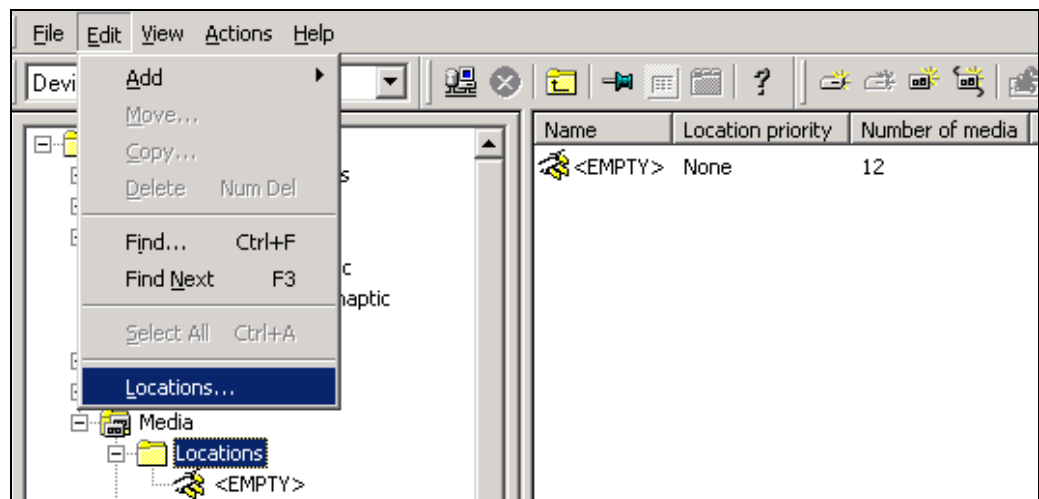
You can also access Data Protector web reporting using Data Protector GUI. In the Reporting context, select **Web Reporting** from the Actions menu.



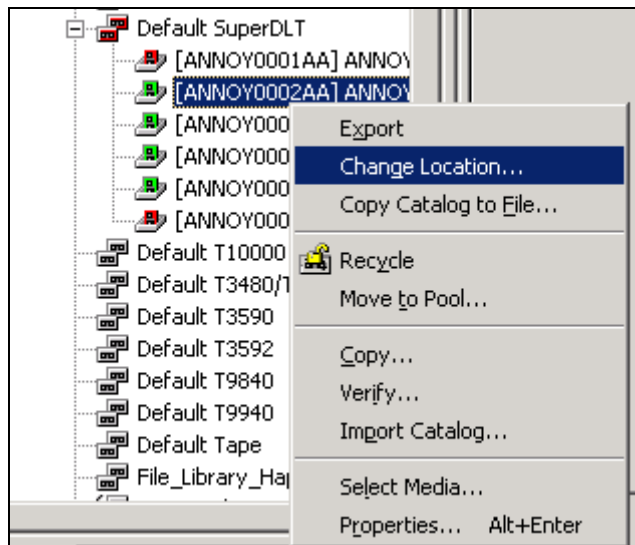
To enable security, In the Context List, select **Users**. From the Actions menu, click **Set Web User Password**.

## Monitoring offsite procedures

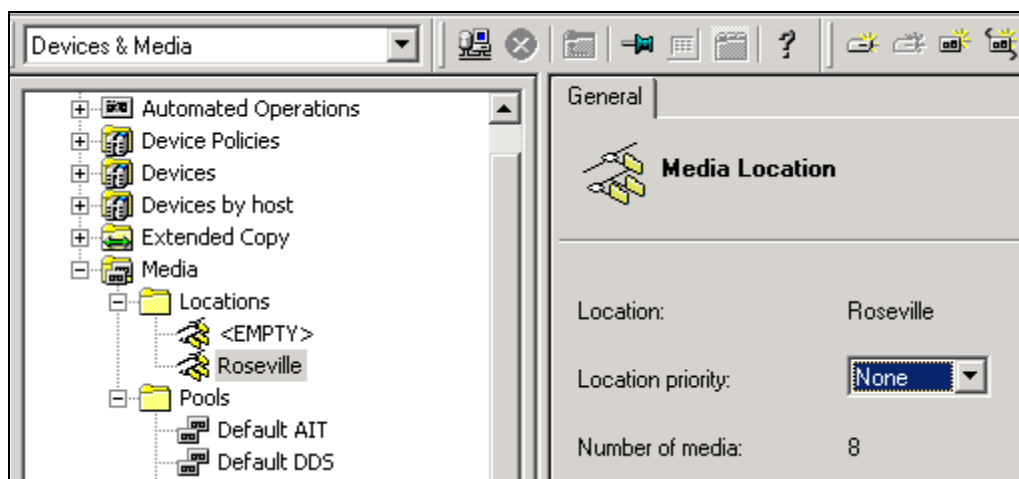
To add a new location, under Devices & Media, click on the **Edit** menu and go to **Locations**. Add the location name and reconnect the Data Protector GUI.



To add media to the location, right-click on the media properties, and select **Change Location**. Hold down the Shift key to change the location for several media at once.



The location will show the number of media added. Each medium will also show the location details.



## Performance monitoring using a nul device

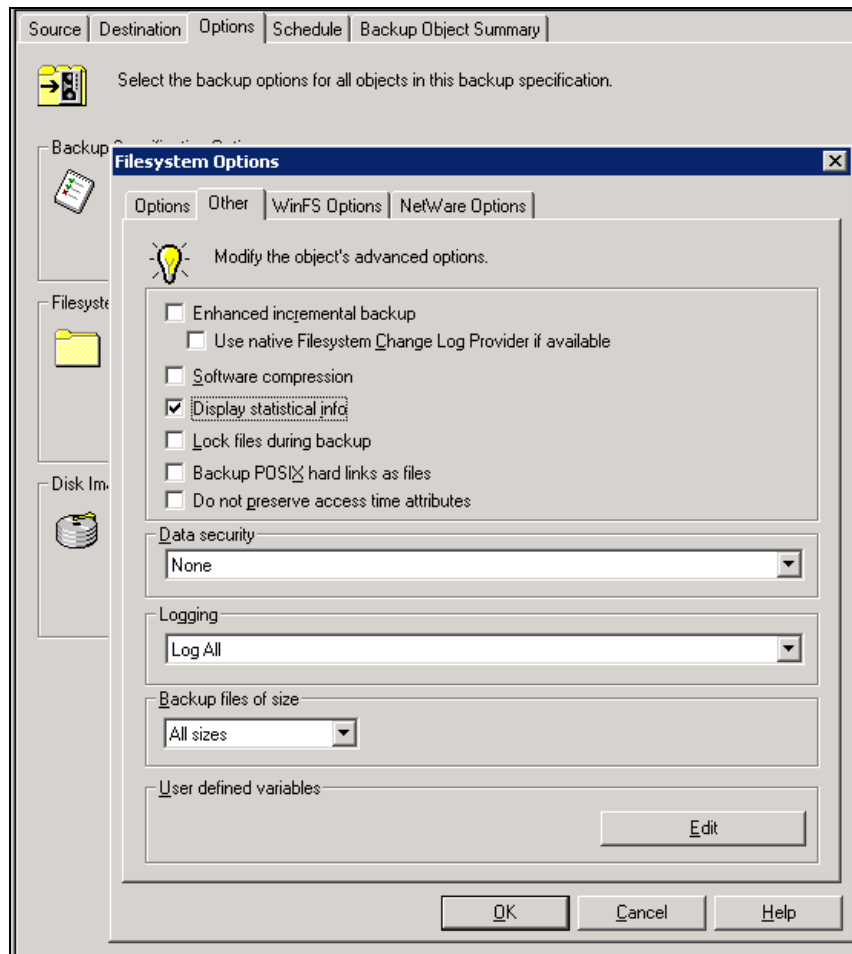
Backup performance numbers are displayed at the end of each backup session as a summary. Data Protector does not offer interactive performance monitoring for ongoing sessions through the GUI.

If you suspect the sustained data flow to the tape device to be too low, or the device does not handle it correctly, you can improve performance by simulating a high-speed device.

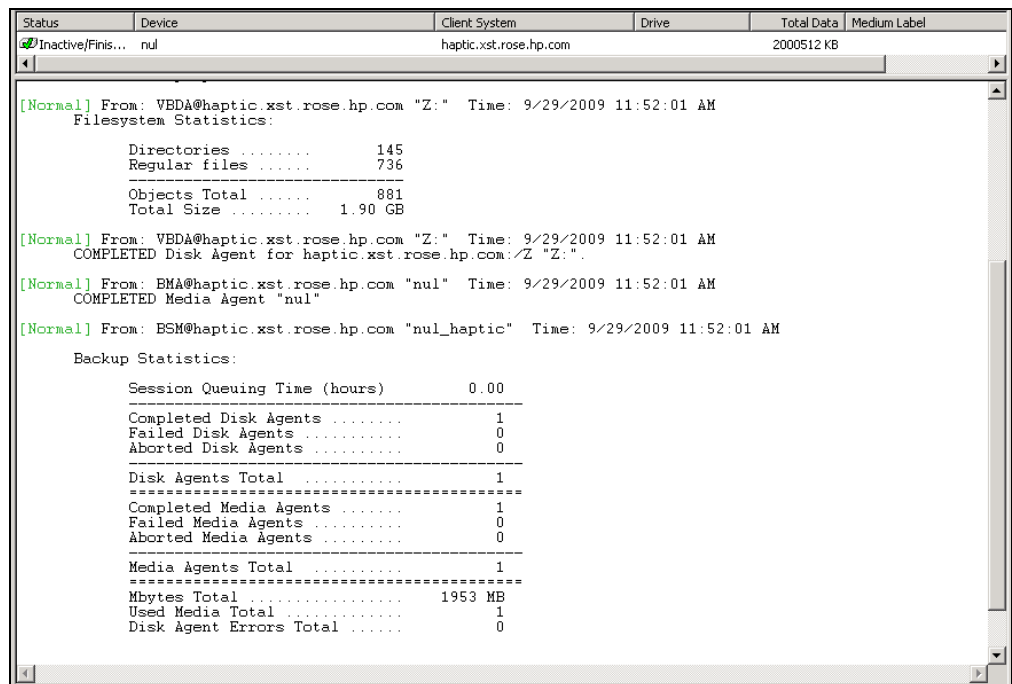
To create a nul device:

1. Create a standalone file device and a device file
    - o *UNIX*: /dev/null
    - o *Windows*: nul
  2. Create a new media pool, select the **Loose** allocation policy option and set the global variable InitOnLoosePolicy to 1 in
    - o *UNIX*: /etc/opt/omni/server/options/global
    - o *Windows*: C:\Program Files\OmniBack\Config\Server\Options
- Change this pool under the device settings of the device created in step 1.

3. Create a backup specification. In the Options wizard page, set data protection to **None** and catalog protection to **Same as data protection**. Select the option **Display Statistical Info** to see the performance summary at the end of the backup session.



4. Perform backups to this nul device and check if the performance discrepancy between backups to the file device and backups to the real device can be explained.



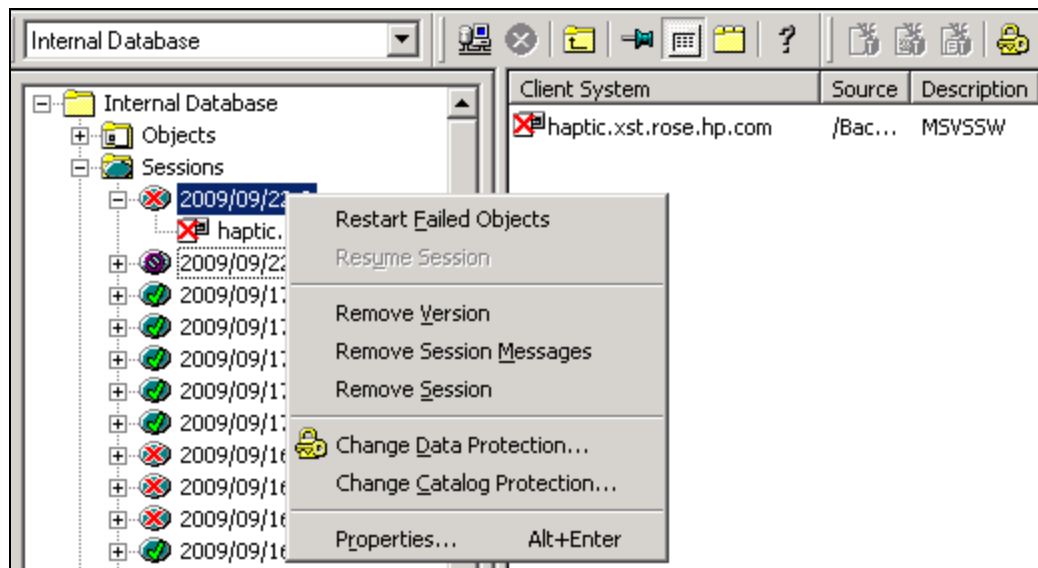
## Restarting failed sessions

You can restart a failed session or a completed session with failures after you have resolved related problems. This restarts only the failed objects. The option can be used for clustered failed objects as well.

You cannot restart failed sessions that are the result of an unsaved backup specification.

To restart sessions:

1. In the Context List, click **Internal Database**.
2. In the Scoping Pane, expand the Internal Database item and click **Sessions**.
3. A list of sessions is displayed in the Results Area. The status of each session is marked in the Status column. Right-click a failed, aborted, or completed session with failures and select **Restart Failed Objects** to back up the objects that failed.



**Note:** If the Cell Manager is setup with high availability clustering, and a failover of the Cell Manager occurs during backup activity, the backup session will fail. The session can be restarted automatically if this option is selected in the backup specification.

## Resuming sessions

Using the Data Protector resume session functionality, you can resume backup and restore sessions that failed for any of the following reasons:

- network problem
- fatal Disk Agent problem
- fatal Media Agent problem
- fatal session manager problem
- fatal media problem (for example, torn tape)
- you aborted the session

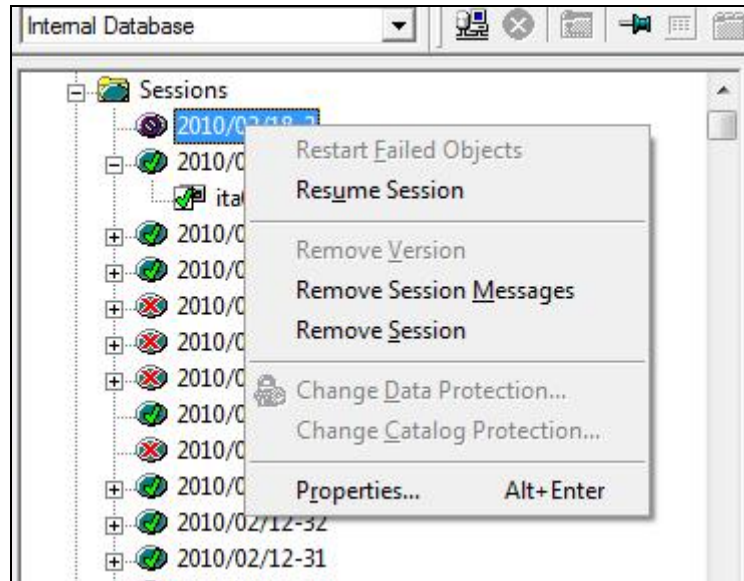
However, first you have to resolve the problem.

When you resume a failed session, Data Protector continues the backup or restore in a new session, starting where the failed session left off. The resumed session inherits all the options from the original session.

However, not all session types can be resumed. Currently, Data Protector supports the following:

- Filesystem restore sessions
- IDB restore sessions
- Data Protector Oracle Server integration backup sessions
- Data Protector Oracle Server integration restore sessions

The following screenshot shows how to resume a failed session. Right-click on the session name, and chose **Resume Session**:

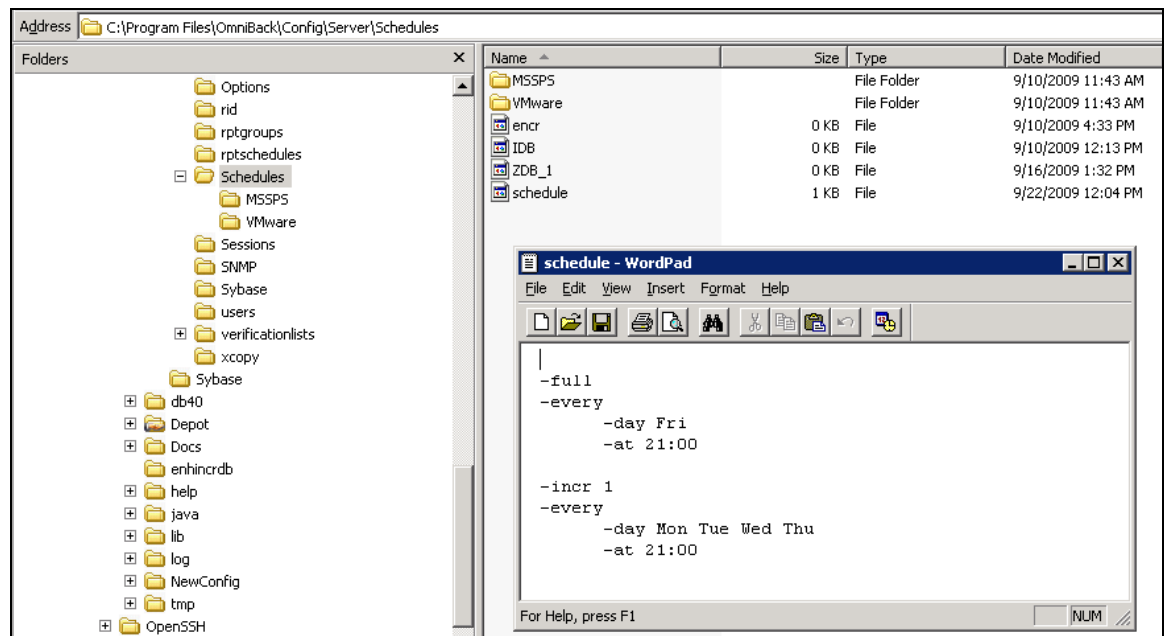


## Editing the backup schedules

You cannot edit a backup schedule created in Data Protector from the GUI. You need to delete and recreate it. You can edit it via the schedule template file by following the required format. Bulk edits are also quicker done from the templates than the GUI.

The backup schedules are kept under the following location:  
 C:\Program Files\OmniBack\Config\Server\Schedules

Copy-paste schedules into backup specifications to enable new schedules via the templates:



**Note:** Use `omnitrig -stop` to stop the scheduler:

```
C:\Program Files\OmniBack\bin>omnitrig ?
Usage synopsis:
omnitrig -version | -help
omnitrig [-start] [-log]
omnitrig -stop
omnitrig -run_checks

C:\Program Files\OmniBack\bin>omnitrig -stop
C:\Program Files\OmniBack\bin>omnitrig -start -log
C:\Program Files\OmniBack\bin>_
```

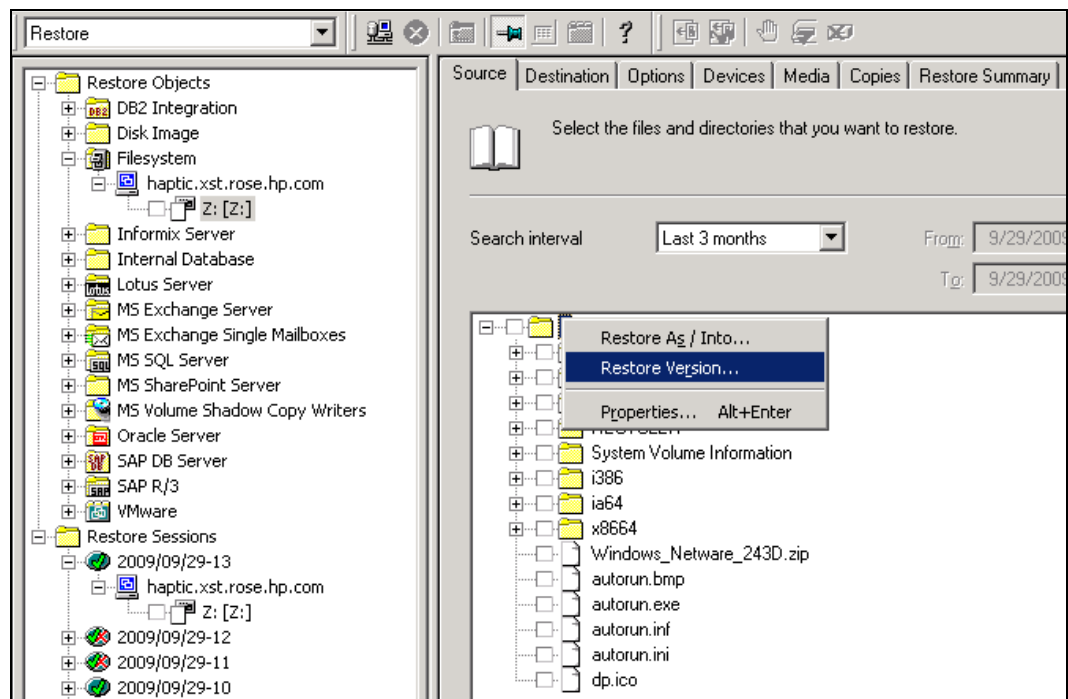
## Restore management

This chapter covers file version and file search based restore operations, and performing a restore after a library configuration has been deleted.

### File version restore

File version restore is available via the backup session history, or via the backup objects. The backup objects will show the backup sessions for the file: full, incremental, enhanced incremental, or synthetic or virtual full session details.

Right-click on the data that you want to restore, and select **Restore Version...**:



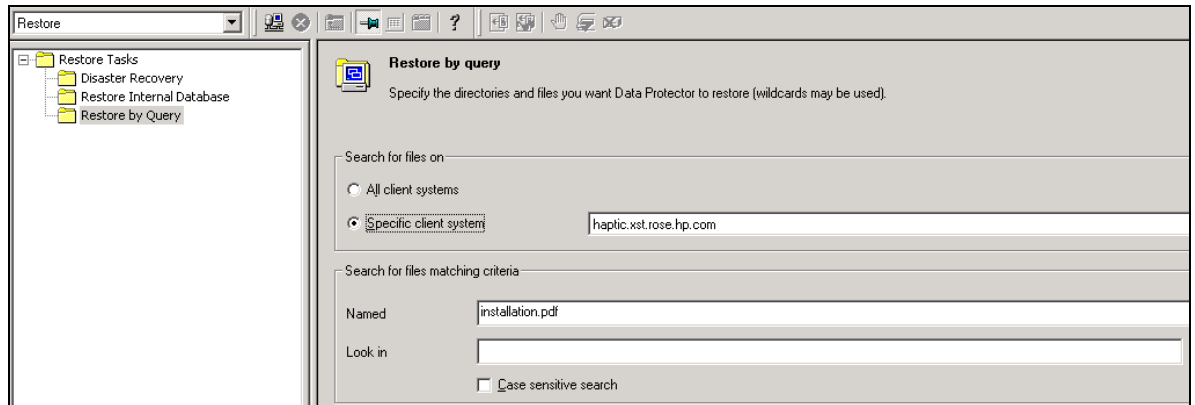
A list of files will be displayed, select the version that you want to restore from.



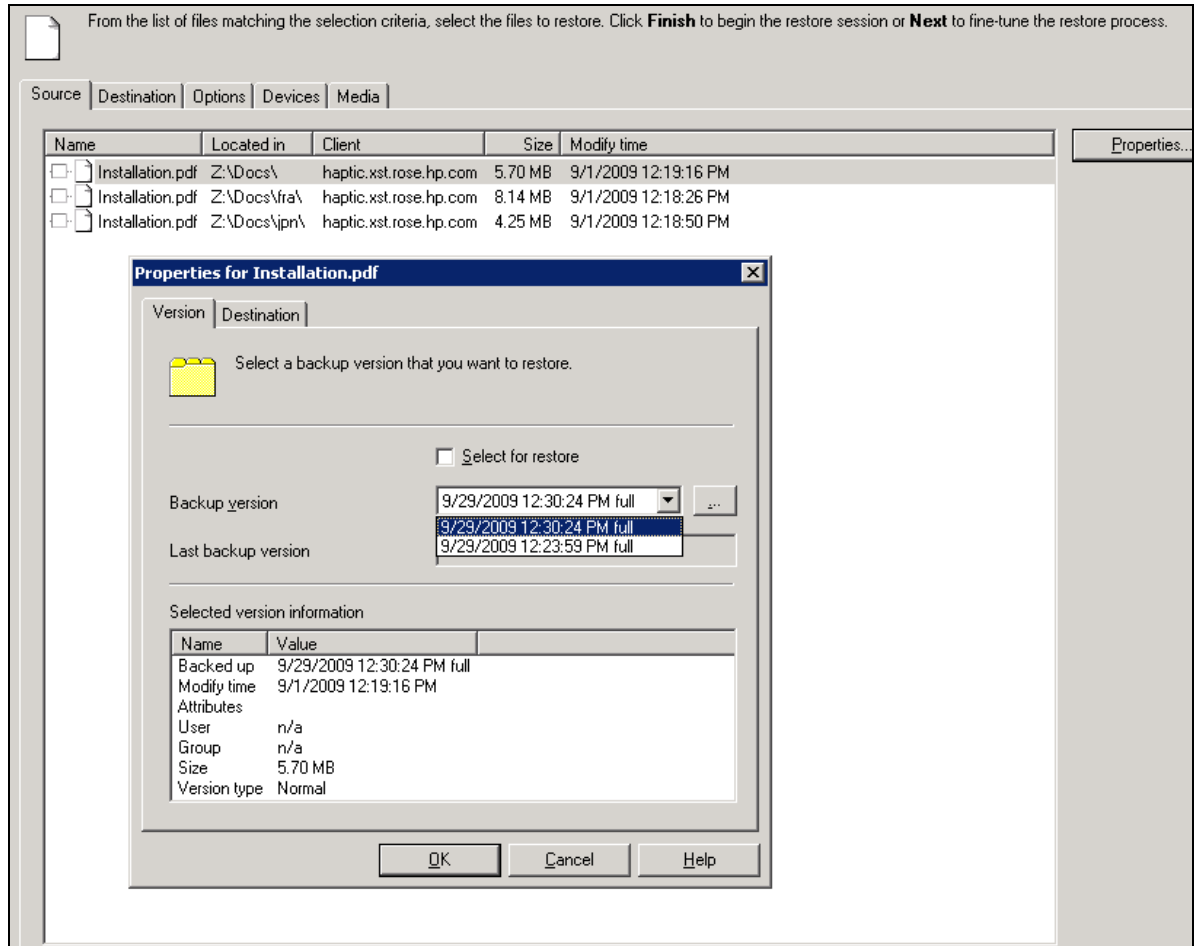
## Restore query

To search for a file and version backed up, go to the Task list under the Restore options, and use the wizard to find the file.

Select the client(s) to search from:



Select the file's **Properties...** to find more details about the backup version of the file:



## Performing a restore when a library configuration has been deleted

For backups that were completed using a "deleted" device configuration, the Data Protector IDB may still contain the original device information as the destination of the host. This can be handled by any of the following methods:

- Select a different device at the time of restore: chose the device tab in the restore context, and selecting the new device.

For File system backups only, you can achieve the same by specifying the `-device` option to `omnir` on the command line. For integrations backup, you can use other alternatives.

- Keeping a `restoredev` file under the directory:
  - **UNIX:** `/etc/opt/omni/server/cell`
  - **Windows:** `<DP_HOME>\Config\Server\cell`

This is a plain text file containing the old and new device names separated by a space. It is referred to whenever the device is called, and the old name is replaced by the new name. A typical file looks like this:

```
"old_device1_name" "new_device1_name"  
"old_device2_name" "new_device2_name"  
"old_device3_name" "new_device1_name"  
"old_device4_name" "new_device2_name"
```

- Change the device information permanently in the IDB by running:  
`omnidbutil -changebdev FromDev ToDev`

You can also use this command for one particular session if you do not want to change it completely. For the complete usage of this command, refer to the *Data Protector CLI guide*.

## IDB maintenance activities

The HP Data Protector IDB is a RAIMA Velocis database. It is recommended to perform certain maintenance tasks in addition to the scheduled maintenance tasks. This chapter covers daily maintenance, as well as long-term maintenance actions, for instance purging, maintaining DCBF files and tablespaces.

### Short-term IDB maintenance

#### Daily notifications

Data Protector provides its own checking and maintenance mechanism, which performs maintenance tasks and checks daily. Daily maintenance runs a series of commands that purge obsolete data from many sections of the Data Protector Internal Database. It does not purge all parts of the IDB, only those that do not require exclusive access to the IDB. By default, the daily maintenance takes place at noon each day.

Every day at 12:00 P.M. by default, Data Protector:

- deletes obsolete DC binary files, sessions, and related messages.
- finds any free (unprotected) media in media pools in which the Use free pool and Move free media to free pool options are set and deallocates the free media to a free pool by issuing the command:  
`omnidbutil -free_pool_update`

The daily maintenance runs the following `omnidbutil -purge` commands:

- `-sessions`
- `-messages`
- `-dcbf`
- `-mpos`

The daily maintenance sessions command is determined by the setting of the `KeepObsoleteSessions` variable, the messages command by the `KeepMessages` variable, and the `mpos` command by the `QuickMediaFormat` variable in the global options file, and `FormatOversPerTransaction`:

- `QuickMediaFormat` = prevent purge of all obsolete object versions at media format/overwrite/export
- `FormatOversPerTransaction` = the number of object versions per purge (default 50)

Every day at 12:30 P.M. by default, Data Protector starts checks for the following:

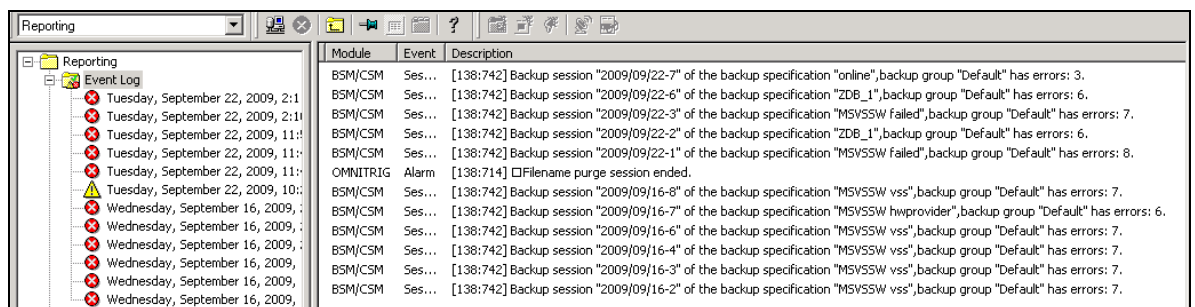
- IDB Space Low
- IDB Tablespace Space Low
- Not Enough Free Media
- Health Check Failed
- User Check Failed (if configured)
- Unexpected Events
- License Warning
- License Will Expire
- IDB Purge Needed

By default, any triggered notification is sent to the Data Protector Event Log.

The following message will show when there are new events in the Event Log:



Go to **Reporting -> Event Log**, to view the error messages:



## Long-term IDB maintenance

The IDB files are located in the following directories:

- *Unix*: /var/opt/omni/server/db40/
- *Windows 2000/2003/XP*: C:\Program Files\OmniBack\db40
- *Windows Vista/2008*: C:\Program Data\OmniBack\db40

## IDB Purge preview

It is recommended to turn off the automatic purge preview scheduled at 12:30 PM. The purge preview uses a lot of RDS processing power.

To turn it off, set the option DbPurgeCheck=0 in the global options file on the cell server:

- *UNIX*: /etc/opt/omni/server/options/global
- *Windows*: C:\Program Files\OmniBack\Config\Server\Options

Uncomment the option in the `global` file, and select 0 or 1 to enable the option:

```
# default: 0
# If this option is set (=1), IDB check will do a quick scan of
# IDB. If this option is not set (=0), IDB check will do a full
# scan of IDB. Applies to omnidbcheck and DBBDA.

# DbPurgeCheck=0 or 1

# default: 1
# If this option is set (=1), IDB purge check will be included
# when daily check is started. If this option is not set (=0),
# IDB purge check will be skipped.

# SMTPServer=Hostname

# default: <cell manager host>
# SMTP server for sending emails.

# SMTPSenderAddress=username@hostname

# default: <sender@localhost>
# SMTP sender address also acts as reply-to address. If you want
# to control replies to reporting or notification mails, change
# sender address to some fixed controlled address.
```

Instead of the automatic scheduled purge preview, it is recommended to script or manually run a purge preview session once a month, using the following command:

```
C:\Program Files\OmniBack\bin>omnirpt -report db_purge_preview
```

```
C:\Program Files\OmniBack\bin>omnirpt -report db_purge_preview
IDB Purge Preview Report

Cell Manager: muggy.xst.rose.hp.com
Creation Date: 1/25/2010 10:20:43 AM

Client          # Filename # Est. Obs Est. Durat
-----
nw65sp8         28         0         6
nw65sp8gw       28         0         6
```

Analyze the output of the `db_purge_preview` report by looking at the column `Est. Obs`. If you see that there are clients with values over 1,000,000, a filenames purge session should be executed for that Cell Manager.

**Note:** If you set the `DbPurgeCheck` to 0, it is highly recommended to do it manually or scripted. If you do not do this, you will not be notified if a purge is needed and you may run into problems.

### IDB Purge

Keep using the default scheduled db purge session of `dcbf`, messages and sessions. No changes are required.

For heavily loaded cells, perform a filename purge twice a year if possible, but once a year at the minimum.

The filenames purge should be combined with a `writedb/readdb` in order to reduce the IDB size and eliminate fragmentation.

First run the filenames purge then perform the `writedb/readdb`.

Note: This operation might take several hours in which no Data Protector operation are possible, so plan enough downtime for this purge session.

```
/opt/omni/sbin/omnidbutil -purge -filenames <force>
```

```
C:\Program Files\OmniBack\bin>omnidbutil -purge -filenames <force>
```

Example:

```
C:\Program Files\OmniBack\bin>omnidbutil -purge -filenames  
Filename purge session started.
```

**Note:**

```
C:\Program Files\OmniBack\bin>omnidbutil -purge_stop  
This is useful command to stop a purge in case you need to run urgent Data Protector operations.
```

```
/opt/omni/sbin/omnidbutil -writedb [-mmdb /db_unload/mmdb] -cdb /db_unload/cdb  
C:\Program Files\OmniBack\bin>omnidbutil -readdb [-mmdb Directory ] [--cdb  
Directory ] [-no_detail ] [-check_overs ]  
C:\Program Files\OmniBack\bin>omnidbutil -writedb [-mmdb Directory ] [-cdb  
Directory ] [-no_detail ]
```

**Note:**

The [-mmdb /db\_unload/mmdb] option is only required when executing a writedb on the Manager of Managers (MOM) server. If you have a Manager of Managers (MOM) you need no -mmdb on a client cell server.

Excluding the mmdb from maintenance on a standalone cell is not a best practice.

During the course of the writedb, you will be prompted to copy the IDB message and dcbf files as follows:

**Note:**

Please make a copy of following Internal Database directories and then press ENTER to return Internal Database to normal state:

```
"/var/opt/omni/server/db40/msg"  
"/var/opt/omni/server/db40/dcbf"
```

For example, copy them as follows:

```
cp -r /var/opt/omni/server/db40/msg/* /db_unload/idb/msg  
cp -r /var/opt/omni/server/db40/dcbf/* /db_unload/idb/dcbf  
/opt/omni/sbin/omnidbinit -force  
/opt/omni/sbin/omnidbutil -readdb [-mmdb /db_unload/mmdb] -cdb /db_unload/cdb
```

**Caution:** Do not use the omnidbinit command without being directed to do so by HP Support.

After the readdb has completed, you need to copy the msg and dcbf files back to their original location:

For example, copy them as follows:

```
cp -r /db_unload/idb/msg/* /var/opt/omni/server/db40/msg/  
cp -r /db_unload/idb/dcbf/* /var/opt/omni/server/db40/dcbf/
```

**Note:** Refer to the *HP Data Protector IDB Purge Best Practices White Paper (4AA2-4988ENW)* for more details.

## DCBF

For Data Protector 6.x, it is recommended that the dcbf directories have the following properties:

- Maximum usage in MB (-maxsize) = 32768
- Maximum number of files in directory (-maxfiles) = 10000
- Minimum free space in MB (-space\_low) = 2048

**Note:** The sequence number, Allocation sequence (-seq), is not important since the global option DCDirAllocation will be set.

Run the following command to determine the layout of the `dcbf` directories and files:

- **UNIX:** `/opt/omni/sbin/omnidbutil -list_dcdirs`
- **Windows:** `C:\Program Files\OmniBack\bin>omnidbutil -list_dcdirs`

```
C:\Program Files\OmniBack\bin>omnidbutil -list_dcdirs
Configured DC Directories:

Allocation sequence
|
| Maximum Usage in MB
| Maximum number of files in directory
| Minimum free space in MB
| Directory
|=====
0          16384    10000    2048    C:/Program Files/OmniBack/db40/dcbf
```

Analyze the output and modify all existing `dcbf` directories if they do not meet the above recommendations, using the following command:

- **UNIX:** `/opt/omni/sbin/omnidbutil (-modify_dcdir /var/opt/omni/server/db40/dcbf (-maxsize 32768 (-maxfiles 10000 (-spacelow 100`
- **Windows:** `C:\Program Files\OmniBack\bin>omnidbutil -modify_dcdir Pathname [ -maxsize Size_MB ] [-maxfiles NumberOfFiles ] [ -spacelow Size_MB ] [ -seq Number ]`

**Note:** The path here is only an example. You will need to specify the correct path to the `dcbf` directory.

Create at least one new `dcbf` directory, unless 10 `dcbf` directories already exist. For DP 6.1x, this is automatically done at installation time. It is recommended to create five if possible. Empty `dcbf` directories will not negatively impact the performance of the IDB.

```
/opt/omni/sbin/omnidbutil -add_dcdir -maxsize 32768 -maxfiles 10000 -spacelow 100
```

**Note:** This is not required unless you need less than 32 GB, 10000 files. Spacelow 100 MB is recommended. 32 GB is quite large; the 10000 limit will be reached first, even with 12 or 16GB of dir sizes.

Set the option `DCDirAllocation` to 1 in the global options file on the cell server:

- **Unix:** `/etc/opt/omni/server/options/global`
- **Windows 2000/2003/XP:** `C:\Program Files\OmniBack\Config\Server\Options`
- **Windows Vista/2008:** `C:\Program Data\OmniBack\Config\Server\Options`

This is default in DP 6.1.

This will cause all `dcbf` directories to be filled at the same rate instead of one after the other.

```

# Also, in case only ASCII characters are used on all Windows
# clients, the variable can be set to zero ("0"), because
# the IDB filename conversion is not needed.

# BrowseMPosCache=NumberOfMegabytes

# default: 40
# This option specifies upper limit of memory used by DBSM when
# browsing Detail Catalog. Specifying 0 disables the cache
# altogether.

# DCDirAllocation=0, 1, 2

# default: 1
# This global option controls which algorithm will be used to
# select the directory for the creation of the new DCBF file.
# 0 - Fill in sequence
# 1 - Balance size
# 2 - Balance number

# MaxDCDirs=NumberOfDirectories

# default: 10

```

## Tablespaces

It is recommended to check the size of the following tablespaces: fnames.dat, fn1.ext, fn2.ext, fn3.ext, fn4.ext and dirs.dat, using the following command:

- *UNIX:* /opt/omni/sbin/omnidbutil -extendinfo
- *Windows:* C:\Program Files\OmniBack\bin>omnidbutil -extendinfo

```

H:\Program Files\OmniBack\bin>omnidbutil -extendinfo

Base file "dirs.dat":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 14432 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 14432 [kB]

Base file "fn1.ext":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 18112 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 18112 [kB]

Base file "fn2.ext":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 17504 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 17504 [kB]

Base file "fn3.ext":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 6720 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 6720 [kB]

Base file "fn4.ext":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 1312 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 1312 [kB]

Base file "fnames.dat":
  Device                = H:/Program Files/OmniBack/db40/datafiles/cdb
  Number of extensions  = 0
  Maximum size          = 2097152 [kB]
  Current size          = 167808 [kB]
  Maximum size with extensions = 2097152 [kB]
  Current size with extensions = 167808 [kB]

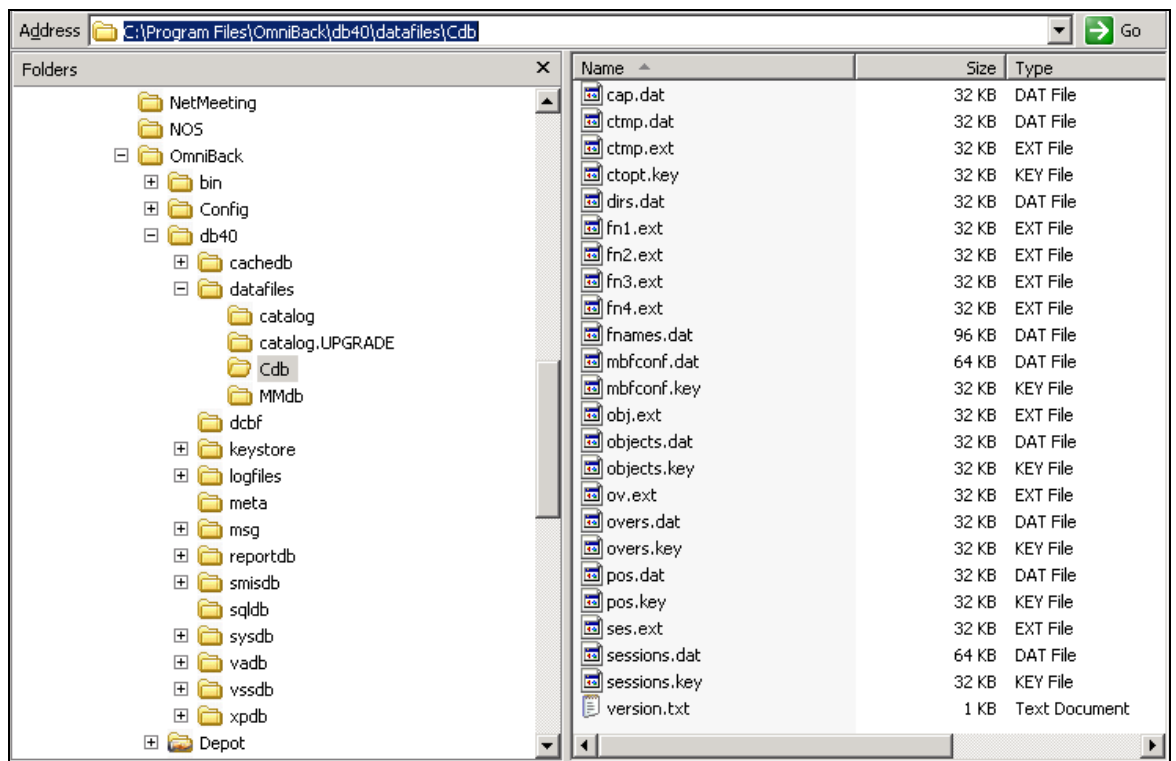
```

Each tablespace listed must have enough space otherwise you will encounter the **no Log** message and will not be able to select individual files for restore.

Analyze the output to see if any of the tablespaces need to be extended by comparing the Maximum size and Current size for each tablespace. If they are within 500 MB of each other, extend the tablespace using the following example command:

- **UNIX:** `/opt/omni/sbin/omnidbutil -extendtblspace fn2.ext /var/opt/omni/server/db40/datafiles/cdb -maxsize 2048`
- **Windows:** `C:\Program Files\OmniBack\bin>omnidbutil -extendtblspace Tablespace Pathname -maxsize Size_MB`

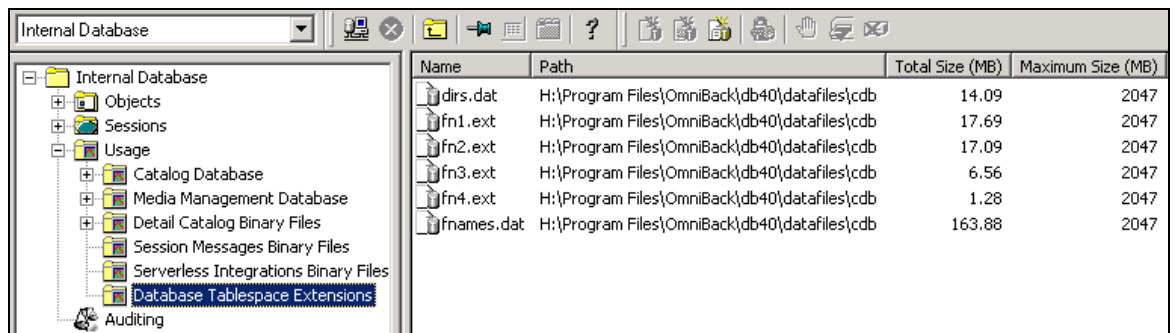
**Note:** Not all tablespaces can be extended from the GUI/CLI, like `pos.dat` or `overs.dat`. In case of issues, contact HP support.



Example:

```
C:\Program Files\OmniBack\bin>omnidbutil -extendtblspace fn1.ext "C:\Program Files\OmniBack\db40\datafiles\Cdb" -maxsize 2047_MB
DONE!
```

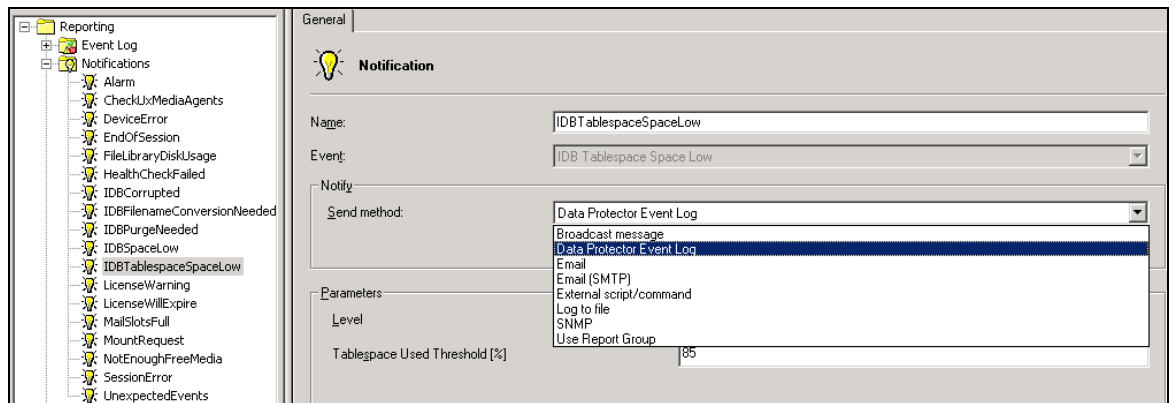
In general, it is recommended to always have at least one empty extent for each tablespace available. For `fnames`, it is recommended to have 2 or 3 available.





## IDB notifications and reporting

Setup report notification for IDB maintenance related tasks.



## Recovering the IDB

Several recovery methods are available for recovering the Internal Database. Depending on the identified level of corruption, your requirements, and the availability of the IDB recovery file and the original device and transaction logs, the recovery procedure can differ.

### *The most convenient complete recovery*

This recovery method guides you through restoring the IDB and replaying transaction logs. If transaction logs are not available, you can still update the IDB by importing all media since the last IDB backup.

Corruption level	Problem type	Current situation	Recovery procedure
Critical	The complete IDB is missing or the core part is corrupted.	The IDB recovery file and the original device used for the IDB backup are available.	Perform the Guided Autorecovery (IDB Restore and Replay Logs) if possible. Otherwise, follow one of the methods given under More recovery methods.

### *Omitting (removing) corrupted IDB parts*

If the identified level of corruption is major or minor (corruption is not in the core part), you can consider omitting (removing) the missing or corrupted parts of the IDB or perform the complete IDB recovery instead.

Corruption level	Problem type	Recovery procedure
Major	Filename tablespace is corrupted.	Handle Major IDB Corruption in the Filenames Part
Minor	DC binary files are missing or corrupted.	Handle Minor IDB Corruption in the DCBF Part

### *More recovery methods*

These recovery procedures are adapted to specific situations. They assume that you want to recover the complete IDB, but for some reason you cannot perform the guided autorecovery method. The recovery consists of restoring the IDB and updating the IDB.

Restore:

Current situation	Remark	Recovery procedure (restoring IDB)
The IDB recovery file is available but the original device used for the IDB backup has changed.	The method is essentially the same as the guided autorecovery method, but less guided, more complex, and time consuming.	Restore the IDB Using IDB Recovery File and Changed Device
The IDB recovery file is not available.	The method is essentially the same as the guided autorecovery method, but less guided, more complex, and time consuming.	Restore the IDB Without IDB Recovery File
You want to recover the IDB from a specific IDB backup (not the latest one).	This method does not provide the latest state of the IDB as a result.	Restore the IDB from a Specific IDB Session
You want to recover to a different disk layout.	This method is equivalent to disaster recovery from a Data Protector configuration where you lost the IDB transaction logs, the IDB recovery file, and the media.log file. It is far more complex than the guided autorecovery and does not provide the latest state of the IDB as a result.	Restore the IDB to a Different Disk Layout

Update the IDB since the last IDB backup:

Current situation	Recovery procedure (updating the IDB)
The transaction logs are available.	Replay IDB Transaction Logs
The transaction logs are not available.	Update IDB by Importing Media

### *Steps to manually recover the IDB*

1. Create a new IDB.
2. Configure a logical device that is compatible with the media containing the IDB backup. View the `media.log` file to determine the tape that contains the latest IDB backup.
3. Import the tape into the existing IDB into a Media Pool using the Logical Device.  
**Note:** This is not needed if the database is still operational and contains the session information from the desired backup session.
4. Restore the desired backup session data onto the system in an alternate location using the "into" feature of Restore, using the restore wizard. You may be able to restore into the partition or directory where you have located the `db40`, since you will likely have available disk space there, just don't overwrite the existing active database, `db40` directory.
5. After the `restore - into` has completed, stop the Data Protector servers. Be sure to stop all GUI's and sessions before proceeding, the database will be moved. Stop the Data Protector services; do not move the IDB while the services are running.  
`omnisv -stop`
6. Move/rename the current database to a temporary name, then move the restored database into place. For Windows Cell Managers, use the windows explorer. For Unix use the following commands:

```

mv /var/opt/omni/server/db40
/var/opt/omni/server/db40.save
mv <restore_location>/db40
/var/opt/omni/server/db40

```

- The restore process also restored the configuration files into the same location as the database files. You may want to move them into place as well if they need to be recovered. Note: this step may be optional, if the files are intact. For Windows Cell Managers, use the windows explorer. For Unix use the following commands:

```

mv /etc/opt/omni/server
/etc/opt/omni/server/omni.bkup
mv <restore_location>/omni/server
/etc/opt/omni/server

```

- Start the Data Protector Servers using the newly recovered database.  
omnisv -start
- Verify that the database and all of the configurations are operational.  
omnidbcheck ...

## Data Protector cell and client tuning

### global variables

Global options affect the entire Data Protector cell and cover various aspects of Data Protector, such as timeouts and limits. All global options are described in the global options file, which you can edit to customize Data Protector.

Global options are read at the start of each backup session. Editing the global options file does not require restarting the Data Protector services.

The global options file is located on the Cell Manager:

- UNIX systems:* /etc/opt/omni/server/options/global
- Windows Server 2008:*  
Data\_Protector\_program\_data>\Config\Server\Options\global
- Other Windows systems:* <Data\_Protector\_home>\Config\Server\Options\global

To set global options, edit the global file. Uncomment the line of the desired option by removing the “#” mark, and set the desired value.

Most users should be able to operate Data Protector without changing the global options.

The following list includes the most often used global variables. See the global options file for a complete description:

Global variable	Description
MediaView	Changes the fields and their order in the Media Management context.
MaxBSessions	Changes the default limit of five concurrent backups.
InitOnLoosePolicy	Enables Data Protector to automatically initialize blank or unknown media if the loose media policy is used.
MaxMAperSM	Changes the default limit of concurrent devices per backup session (maximum device concurrency is 32).
DCDirAllocation	Determines the algorithm used for selecting the dcbf directory for a new detail catalog binary file: fill in sequence (default), balance size, or balance number.
DailyMaintenanceTime	Determines the time after which the daily maintenance tasks can begin. <i>Default:</i> 12:00 (noon).
DailyCheckTime	Determines the time after which the daily check can begin. <i>Default:</i> 12:30 pm. You can also disable the daily check.

Other frequently used maintenance related global options are the following:

- dcbf related options
  - ✓ DCDirAllocation=0, 1, 2
  - ✓ MaxDCDirs=NumberOfDirectories
  - ✓ SessionMessagesDir=FullPathToTheMessageDir
- cdb related options
  - ✓ DBFreeDiskSpace=MinSpaceInMBytes
  - ✓ DBFreeExtFileSpace=MinSpaceInMBytes
- general options
  - ✓ RecoveryIndexDir=FullPathToTheBackupDir
  - ✓ DbXXXXXXXXXXLimit=GBytes
  - ✓ DBPurgeSuspension=0 or 1
  - ✓ DBPurgeSuspensionDuringDBCheck=0 or 1
  - ✓ DailyMaintenanceTime=HH:MM
  - ✓ DailyCheckTime=HH:MM

## omnirc variables

The `omnirc` options are useful for troubleshooting or overriding other settings affecting the behavior of the Data Protector client only. However, use them only if your operating environment demands it. The Disk Agents and Media Agents use the values of these options.

**Note:** Editing the `omnirc` variables does not require restarting the Data Protector services for most variables.

The `omnirc` variables can be set on each client in the file:

- *UNIX systems:* `/usr/omni/.omnirc`
- *Windows Vista, Windows Server 2008:* `C:\Program Files\OmniBack\omnirc`
- *Other Windows systems:* `C:\Program Data\OmniBack\omnirc`
- *Novell NetWare:* `sys:\usr\omni\omnirc`

To set `omnirc` options:

1. Depending on the platform, copy the template `omnirc.tpl` or `.omnirc.TMPL` to `omnirc` or `.omnirc`, respectively.
2. Edit the file `omnirc` or `.omnirc`. Uncomment the line of the desired option by removing the “#” mark, and set the desired value.
3. After setting the variables:
  - When creating the `omnirc` file (either by copying or by using an editor), verify its permissions. On UNIX, permissions will be set according to your `umask` settings and may be such that some processes may be unable to read the file. Set the permissions to `644` manually.
  - When changing the `omnirc` file, restart the Data Protector services/daemons on the Data Protector client where you modified the `omnirc` file. This is mandatory for the `crs` daemon on UNIX and recommended for Data Protector CRS and `Inet` services on Windows. Specifically on Windows, restarting is not required when adding or changing entries, only when removing entries (or renaming the file). A restart is required when a variable affects the Data Protector services and `omnirc` is running on the cell server. The majority of `omnirc` changes are made on the Data Protector client side, so no restart is required.

**Note:** When using special characters in variable names in the `omnirc` file, take into account operating system specific limitations regarding supported characters for setting environment variables. For example, on UNIX systems, variables cannot contain any of the following characters: Space Tab / : \* " < > | .

## scsitab file

It is recommended that you let Data Protector configure backup devices automatically. Data Protector can automatically configure most common backup devices, including libraries. You still need to prepare the media for a backup session, but Data Protector determines the name, policy, media type, media policy, and the device file or SCSI address of the device, and also configures the drive and slots.

You can also configure a backup device manually. How you configure a backup device depends on the device type. You can use devices that are not listed as supported in the *HP Data Protector product announcements, software notes, and references*. Unsupported devices are configured using the `scsitab` file.

Modifying the `scsitab` file is not supported.

To use a device that is not listed as supported in the *HP Data Protector product announcements, software notes, and references*, download the latest software package for the `scsitab` file from the HP Data Protector web site at <http://www.hp.com/go/dataprotector>.

After you have downloaded the package, follow the installation procedure provided with it.

The `scsitab` file is located on the system to which the device is connected, on the following location:

- *HP-UX and Solaris systems:* `/opt/omni/scsitab`
- *Other UNIX systems:* `/opt/omni/scsitab`
- *Windows Vista, Windows Server 2008:* `C:\Program Files\OmniBack\scsitab`
- *Other Windows systems:* `C:\Program Data\OmniBack\scsitab`

If you still receive the same error while configuring your device, contact HP Support to find when the device will be supported.

```
#####
#
# (C) Copyright 1993-2008 Hewlett-Packard Development Company, L.P.
#
# MODULE      TABLE OF SUPPORTED DEVICES
# FILE        scsitab
# RCS         $Header: /src/files/init/scsitab /main/hsl_dp61/hsl_hpit2_2/3 2009-05-15 11:02:22 mirzat $
# BUILD NUMBER:  NSMbb70553
#
# DESCRIPTION
# TABLE OF SUPPORTED DEVICES
#
#####

# TABLE OF SUPPORTED DEVICES

# LIST OF TAPES

# type\subtype\productID\vendorID\media class type\flags\number of drives\number of slots\element status serial number offset\function
( 1, 1, "VLS 4MH", "ADIC", 1, 2144, 0, 0, 0, 0, 7, 31, "", ADIC VLS 4mh)
( 1, 1, "PYTHON", "ARCHIVE", 1, 2144, 0, 0, 0, 0, 0, 39, "", Archive Python)
( 1, 1, "L500", "ATL", 10, 18423, 0, 0, 0, 0, 2, 8, "", Quantum ATL L500)
( 1, 1, "L200", "ATL", 10, 18423, 0, 0, 0, 0, 2, 8, "", Quantum ATL L200)
( 1, 1, "DLT1", "BENCHMARK", 10, 18422, 0, 0, 0, 1, 0, 319, "", Benchmark lib)
( 1, 1, "DLT1", "BENCHMARK", 10, 18422, 0, 0, 0, 0, 0, 319, "", Benchmark DLT1 drive)
( 1, 1, "VS160", "BENCHMARK", 10, 18400, 0, 0, 0, 0, 0, 1023, "", Benchmark VS160 drive)
( 1, 1, "VS640", "BENCHMARK", 10, 18400, 0, 0, 0, 0, 0, 1023, "", Benchmark VS640 drive)
( 1, 1, "ULTRIUM 2", "CERTANCE", 13, 2144, 0, 0, 0, 0, 0, 289, "", Certance Ultrium 2 Drive)
( 1, 1, "ULTRIUM 3", "CERTANCE", 13, 2144, 0, 0, 0, 0, 0, 35, "", Certance Ultrium 3 Drive)
( 1, 1, "VS160", "COMPAQ", 10, 18400, 0, 0, 0, 0, 0, 1023, "", Compaq VS160 drive)
( 1, 1, "DLT", "COMPAQ", 10, 18422, 0, 0, 0, 1, 0, 6223, "", Compaq DLT drive)
( 1, 1, "SUPERDLT", "COMPAQ", 14, 16992, 0, 0, 0, 0, 0, 7167, "", Compaq SuperDLT drive)
( 1, 1, "SDX-400C", "COMPAQ", 4, 96, 0, 0, 0, 0, 0, 7167, "", SDX-400C Drive)
( 1, 1, "SDT-10000", "COMPAQ", 1, 2144, 0, 0, 0, 0, 0, 7167, "", Compaq SDT-10000 DDS4)
( 1, 1, "SBLT320", "COMPAQ", 14, 16992, 0, 0, 0, 0, 0, 7167, "", Compaq SuperDLT 160/320 GB)
( 1, 1, "DLT8", "COMPAQ", 10, 18400, 0, 0, 0, 0, 0, 7167, "", DLT 8000 series drive)
( 1, 1, "TSL-10000", "COMPAQ", 1, 2144, 0, 0, 0, 0, 0, 1023, "", TSL-10000)
( 1, 1, "TSL-9000", "COMPAQ", 1, 2144, 0, 0, 0, 0, 0, 1023, "", TSL-9000)
( 1, 1, "SDX-500C", "COMPAQ", 4, 96, 0, 0, 0, 0, 0, 1023, "", SDX-500C)
( 1, 1, "SuperDLT1", "COMPAQ", 14, 16992, 0, 0, 0, 0, 0, 1023, "", SuperDLT1)
```

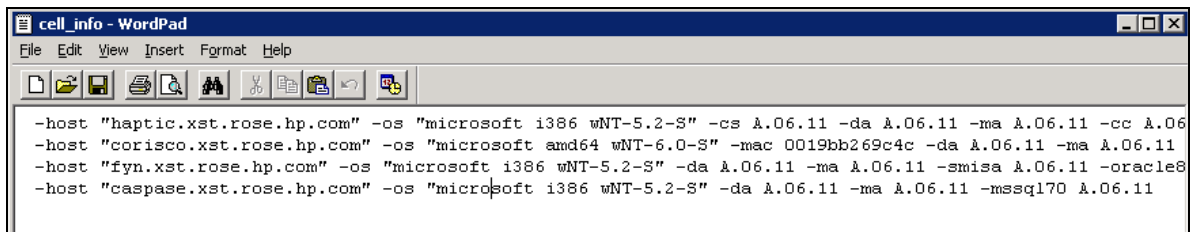
## cell\_info

The `cell_info` file lists all clients configured in the Cell Manager, and all online extensions and agents configured for each host.

The cell\_info file can be found in the following directory:

C:\Program Files\OmniBack\Config\Server\cell

**Important:** cell\_info is a file created and edited during installation. Do not manually edit the file.



```
cell_info - WordPad
File Edit View Insert Format Help
- host "haptic.xst.rose.hp.com" -os "microsoft i386 wNT-5.2-S" -cs A.06.11 -da A.06.11 -ma A.06.11 -cc A.06
- host "corisco.xst.rose.hp.com" -os "microsoft amd64 wNT-6.0-S" -mac 0019bb269c4c -da A.06.11 -ma A.06.11
- host "fyn.xst.rose.hp.com" -os "microsoft i386 wNT-5.2-S" -da A.06.11 -ma A.06.11 -smisa A.06.11 -oracle8
- host "caspase.xst.rose.hp.com" -os "microsoft i386 wNT-5.2-S" -da A.06.11 -ma A.06.11 -mssql170 A.06.11
```

## Variables currently undocumented

### Treewalk

A treewalk is performed when backing up a file system to calculate how many files have changed since the last full backup.

NOTREEWALK=1 is the correct variable for Data Protector 6.0. It works exactly the same in the Data Protector 6.1 code, only the syntax is different. It is undocumented in the the Data Protector 6.0 omnirc file.

- Data Protector 6.0:
  - o if (EnvGetBool(\_T("NoTreeWalk"))) opt.firstTreeWalk=0; /\* old variable still checked \*/
- Data Protector 6.1:
  - o if (EnvGetBool(\_T("OB2NOTREEWALK"))) opt.firstTreeWalk=0; /\* new variable \*/

**Note:** If you abort a backup session while it is still determining the sizes of the disks that you have selected for the backup, it does not abort immediately. The backup is aborted once the size determination (treewalk) is completed.

**Note:** Windows and Unix treewalks are run differently. See the *HP Data Protector Performance White Paper (4AA1-3836ENW)* for further details.

## Event management

### Setting up SNMP trap forwarding

To set up SNMP event forwarding, follow the basic configuration steps as described in the Data Protector online help.

To configure SNMP trap forwarding from the HP Data Protector Cell Manager to any trap-receiving recipient, follow the following steps:

1. Run omnismnp.exe command from the <Data\_Protector\_home>\bin directory. It will create the appropriate Data Protector entry in the System registry under CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents.
2. In the Control Panel, select **Network and Dial-up Connections** (Windows 2000) or **Network Connections** (Windows XP/Server 2003).
3. In the Advanced menu, select **Optional Networking Components** to start the wizard.
4. Select **Management and Monitoring tools** and click **Next**.
5. Follow the wizard to install the management and monitoring tools.
6. Open **Control Panel -> Administrative Tools -> Services**.

7. Right-click **SNMP Service** and select **Properties**.
  - a. Select the Traps tab. Enter **public** in the **Community name** text box and the hostname of the Management Server in the **Trap Destinations** text box.
  - b. Select the Security tab. Under **Accepted community names**, select the community **public**, click **Edit** and set Community rights to **READ CREATE**.
  - c. Confirm your settings.
8. Run `omnisnmp`.

**Note:** The community name is case sensitive.

To finish the setup, there are a few additional configuration steps.

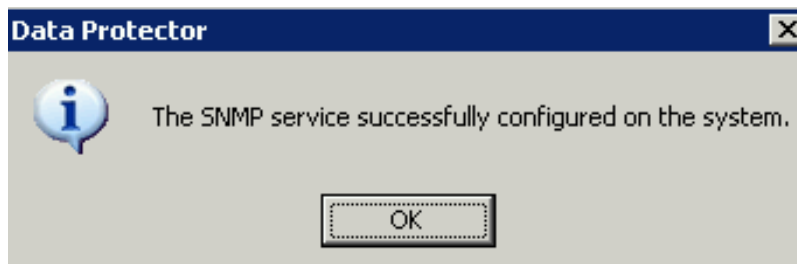
### Running omnisnmp

When following step 1, the following popup message may appear:



Action: Perform steps 2 to 7 and rerun step 1 when this message appears.

After successful configuration, you should see the following popup message:



### Setting OVdests trap destination

Action: To enable SNMP trap forwarding on Data Protector, edit the `OVdests` file to add the remote trap destination host IP address:

Add the Server hostname as trap destination to the `OVdests` file in the Data Protector root or the `Omniback/Program Files/Config/server/SNMP` directory.

```
C:\Program Files\OmniBack\Config\Server\SNMP
10/23/2006 04:35 PM 22 OVdests
10/23/2006 04:35 PM 17 OVfilter
```

Example:

```
trap-dest: 10.50.3.38
```

Example before editing the `OVdests` file:

```
C:\Program Files\OmniBack\bin>omnisv -status
ProcName  Status  [PID]
=====
rds       : Active [2292]
crs       : Active [1688]
mmd       : Active [1928]
kms       : Active [2024]
uiproxy  : Active [2184]
omniinet : Active [1808]
Sending of traps disabled.
=====
Status: All Data Protector relevant processes/services up and running.
```

Example after editing the `OVdests` file:

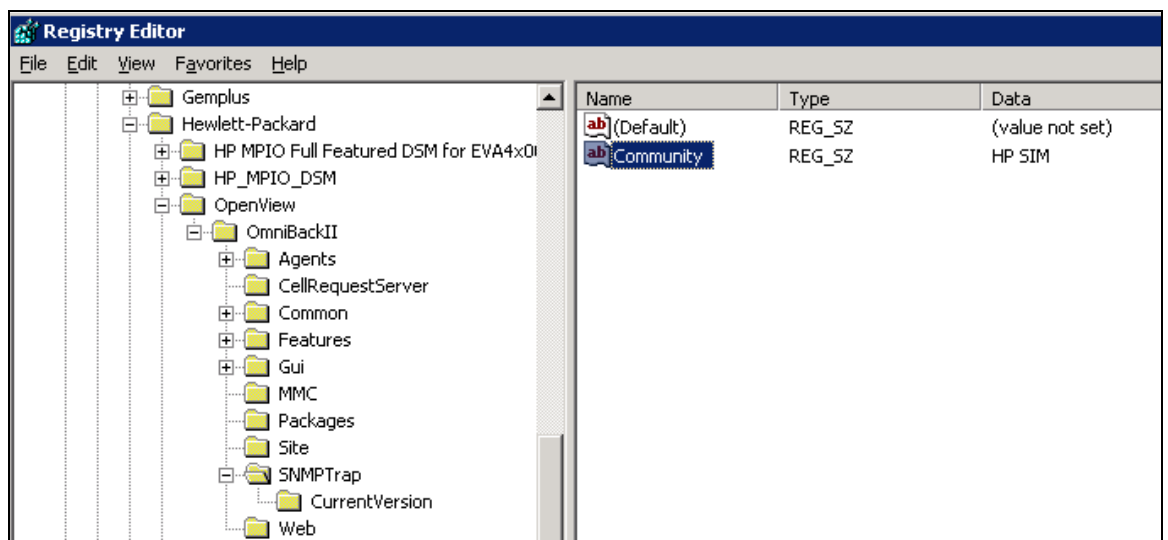
```
C:\Program Files\OmniBack\bin>omnisv -status
ProcName  Status  [PID]
=====
rds       : Active [2292]
crs       : Active [1688]
mmd       : Active [1928]
kms       : Active [2024]
uiproxy  : Active [2184]
omniinet : Active [1808]
Sending of traps enabled for the following hosts:
10.50.3.38
=====
Status: All Data Protector relevant processes/services up and running.
```

### Adding a community name registry key other than public

Executing the `omnisnmp` command will create the Data Protector registry keys required.

Action: An optional additional registry key entry can be created to add a community name other than public. If it is NULL, public is assumed as a value for the registry key. If traps need to be sent to the public community name, no entry is necessary.

Add a new string value with the name `Community`, and define the name of the community under the value data:



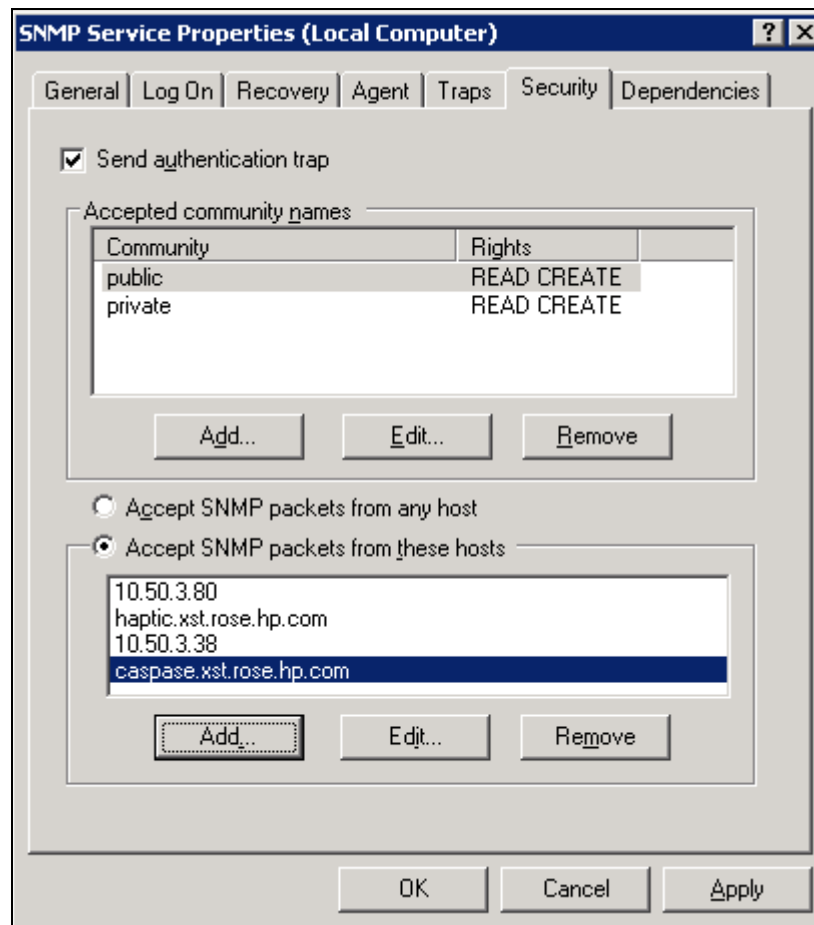
### Configuring the SNMP service destination host

Action: Under the SNMP services properties, ensure that the community name **public** is added, and add also the trap destination host under the "Accept SNMP packages" list as well as the local Cell Manager DNS name and IP address (Data Protector prefers DNS; the IP address is required in case DNS is not resolving).



In the example below, the local Cell Manager hostname or Cell Manager IP address is added, as well as the hostname or IP address of the remote trap receiver destination host.

The Cell Manger name/address in the security tab is necessary. If you set it to 'Accept SNMP traps from any host', then no entries are necessary.



For further information, refer to SNMP Configuration on Windows in chapter 2 of the *HP Data Protector A06.10 integration guide for HP Operations Manager for Windows*. For the latest updates, check the integration guide.

Configure the Windows system to forward its SNMP traps to the Operations Manager Server as follows:

1. To enable Data Protector to send SNMP traps, run the command: `omnisnmp`
2. To set the SNMP mode execute the following command:  
`ovconfchg -ns eaagt -set SNMP_SESSION_MODE NO_TRAPD`
3. Configure the SNMP Service on a Windows system to send traps to the Operations Manager Server. The community name should be **public** (the default community name that Data Protector SNMP traps use). The trap destination must be the IP address or the hostname of the Operations Manager Server and the rights of the community must be **READ CREATE**.

To use a custom community name other than public, set the value in the Registry. Data Protector will then use this name for sending SNMP traps:

```
HKEY_LOCAL_MACHINE\SOFTWARE\HewlettPackard\OpenView\OmniBackII\SNMPTrap CommunityREG_SZ:custom community name
```

4. Configure Data Protector to send SNMP traps to the Operations Manager Server system:
  - a. Using the Data Protector GUI Reporting context, set up all notification events to use:
    - SNMP as delivery method
    - Operations Manager Server system as the destination.
  - b. Add the Operations Manager Server hostname as trap destination to the `OVdests` file in `Data Protector Root/Config/server/SNMP`.
  - c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `Data Protector Root/Config/server/SNMP`.

## Frequently used commands

In this section, the following parameters are used:

- Cell Manager hostname is `haptic.xst.rose.hp.com`
- Object is the `C:` drive
- Object description or label in the backup specification is `"C:"`
- Backup session is `2009/09/10-18`
- Backup object type is `"winfs"`

**Note:** The objects and description are case-sensitive. The description for Windows Cell Managers must be enclosed in double quotes (`"C:"`).

## omnidbutil

All frequently-run database utilities are run from the `omnidbutil` command line option:

```

c:\Program Files\OmniBack\bin>omnidbutil
Usage synopsis:

omnidbutil -help
omnidbutil -version
omnidbutil -list_dcdirs
omnidbutil -add_dcdir Pathname [ -maxsize Size_MB ] [ -maxfiles NumberOfFiles ] [ -spacelow Size_MB ] [
omnidbutil -modify_dcdir Pathname [ -maxsize Size_MB ] [ -maxfiles NumberOfFiles ] [ -spacelow Size_MB ]
omnidbutil -remove_dcdir Pathname
omnidbutil -remap_dcdir
omnidbutil -fixmpos
omnidbutil -readdb [ -mmdb Directory ] [ -cdb Directory ] [ -no_detail ] [ -check_overs ]
omnidbutil -writedb [ -mmdb Directory ] [ -cdb Directory ] [ -no_detail ]
omnidbutil -show_locked_devs
omnidbutil -free_locked_devs [ devname ! mediumId ! cartName phyLocation ! serial_ldev ! wwn_lun ]
omnidbutil -mergemmdb Cell_Server_Hostname
omnidbutil -cdbsync Cell_Server_Hostname
omnidbutil -changebdev FromDev ToDev [ -session SessionID ]
omnidbutil -extendfnames Pathname -maxsize Size_MB
omnidbutil -extendtblspace Tablespace Pathname -maxsize Size_MB
omnidbutil -extendinfo
omnidbutil -purge -filenames [ host_1 ... host_n ] [ -force ] ! -sessions [ NumberOfDays ] ! -days [ Numb
omnidbutil -purge_failed_copies
omnidbutil -purge_stop
omnidbutil -info
omnidbutil -clear
omnidbutil -change_cell_name [ old_host ]
omnidbutil -show_cell_name
omnidbutil -set_session_counter new_session_ID
omnidbutil -upgrade_info
omnidbutil -show_db_files
omnidbutil -free_pool_update
omnidbutil -list_large_directories MinNumberOfFiles [ -top NumOfTopDirectories ] [ -detail ] [ -csv CSUFile ]
omnidbutil -list_large_mpos MinNumberOfMpos [ -top NumOfTopMedia ] [ -detail ] [ -csv CSUFile ]
omnidbutil -list_mpos_without_overs [ -csv CSUFile ]
omnidbutil -free_cell_resources
omnidbutil
c:\Program Files\OmniBack\bin>

```

## omnidb

To view what type of backup objects have been run:

```

c:\Program Files\OmniBack\bin>omnidb -winfs
Object Name                                     Object type
=====
corisco.xst.rose.hp.com:/C 'C:'                WinFS
fyn.xst.rose.hp.com:/C 'C:'                   WinFS
haptic.xst.rose.hp.com:/C 'C:'                 WinFS
haptic.xst.rose.hp.com:/Z 'Z:'                 WinFS

c:\Program Files\OmniBack\bin>omnidb -omnidb
Object Name                                     Object type
=====
haptic.xst.rose.hp.com:/ ' [Database]: haptic.xst.rose.hp.com' IDB

```

To verify what files have been backed up before a session aborted or failed, specify the session name with the session ID and the `-report` option:

```
C:\Program Files\OmniBack\bin>omnidb -winsfs "haptic.xst.rose.hp.com:/C" "C:"
SessionID      Started      Duration Object Status      Size  KKB  NumberOfErr
=====
2009/09/22-7   2:11:31     00:00:06 Failed          119701 2
2009/09/22-5   1:49:46     00:00:39 Completed       703253 0
2009/09/15-2   3:25:51     00:03:30 Completed      3348239 0
2009/09/15-1   3:05:52     00:03:41 Completed      3348239 0
2009/09/11-1   2:33:19     00:08:33 Completed      2291677 0
2009/09/10-18  4:48:12     00:02:28 Completed      2291677 0
2009/09/10-16  4:34:59     00:02:06 Completed      2291677 0
2009/09/10-12  4:27:43     00:02:13 Failed          2291677 0
2009/09/10-11  4:23:40     00:00:07 Failed           4 0

C:\Program Files\OmniBack\bin>omnidb -winsfs "haptic.xst.rose.hp.com:/C" "C:" -session 2009/09/22-7 -report
[Normal] From: UBDA@haptic.xst.rose.hp.com "C:" Time: 9/22/2009 2:11:32 PM
STARTING Disk Agent for haptic.xst.rose.hp.com:/C "C:".

[Critical] From: UBDA@haptic.xst.rose.hp.com "C:" Time: 9/22/2009 2:11:37 PM
Received ABORT request from SM => aborting.

[Critical] From: UBDA@haptic.xst.rose.hp.com "C:" Time: 9/22/2009 2:11:37 PM
Connection to Media Agent broken => aborting.

[Normal] From: UBDA@haptic.xst.rose.hp.com "C:" Time: 9/22/2009 2:11:37 PM
ABORTED Disk Agent for haptic.xst.rose.hp.com:/C "C:".
```

To view the session catalog information, specify the session ID and the `-catalog` option:

```
C:\Program Files\OmniBack\bin>omnidb -winsfs "haptic.xst.rose.hp.com:/C" "C:" -session 2009/09/22-7 -catalog
Protection Owner Group Size Time Path
=====
d---w---- -2 nogroup 0 9/18/2006 4:20:56 PM /Data_Protector_6_0/
d---w---- -2 nogroup 0 9/7/2006 1:32:06 PM /Data_Protector_6_0/DP_Demo/
d---w---- -2 nogroup 0 9/7/2006 1:32:29 PM /Data_Protector_6_0/Docs/
-w----- -2 nogroup 2313270 9/7/2006 1:30:46 PM /Data_Protector_6_0/autorun.bmp
-w----- -2 nogroup 428032 9/7/2006 1:30:47 PM /Data_Protector_6_0/autorun.exe
-w----- -2 nogroup 159 9/7/2006 1:30:47 PM /Data_Protector_6_0/autorun.inf
-w----- -2 nogroup 2081 9/7/2006 1:30:47 PM /Data_Protector_6_0/autorun.ini
-w----- -2 nogroup 1078 9/7/2006 1:30:47 PM /Data_Protector_6_0/dp_ico
d---w---- -2 nogroup 0 9/7/2006 1:32:16 PM /Data_Protector_6_0/DP_Demo/data/
d---w---- -2 nogroup 0 9/7/2006 1:32:16 PM /Data_Protector_6_0/DP_Demo/data/Config/
-w----- -2 nogroup 0 9/7/2006 1:32:06 PM /Data_Protector_6_0/DP_Demo/data/backup_list
-w----- -2 nogroup 4620 9/7/2006 1:32:06 PM /Data_Protector_6_0/DP_Demo/data/cell_info
d---w---- -2 nogroup 0 9/7/2006 1:32:13 PM /Data_Protector_6_0/DP_Demo/data/db40/
d---w---- -2 nogroup 0 9/7/2006 1:32:12 PM /Data_Protector_6_0/DP_Demo/data/devices/
d---w---- -2 nogroup 0 9/7/2006 1:32:11 PM /Data_Protector_6_0/DP_Demo/data/dpdemo_data/
d---w---- -2 nogroup 0 9/7/2006 1:32:17 PM /Data_Protector_6_0/DP_Demo/data/Config/Datalists/
d---w---- -2 nogroup 0 9/7/2006 1:32:16 PM /Data_Protector_6_0/DP_Demo/data/Config/RptGroups/
d---w---- -2 nogroup 0 9/7/2006 1:32:16 PM /Data_Protector_6_0/DP_Demo/data/Config/Schedules/
d---w---- -2 nogroup 0 9/7/2006 1:32:16 PM /Data_Protector_6_0/DP_Demo/data/Config/Server/
```

To find which backed-up objects are available:

```
C:\Program Files\OmniBack\bin>omnidb -object
```

```
C:\Program Files\OmniBack\bin>omnidb -object
Object Name Object type
=====
haptic.xst.rose.hp.com:/ '[Database]: haptic.xst.rose.hp.com' IDB
haptic.xst.rose.hp.com:/BackupSession/Metadata MSUSSW
haptic.xst.rose.hp.com:/Filesystem/Z MSUSSW
corisco.xst.rose.hp.com:/C 'C:' WinFS
fyn.xst.rose.hp.com:/C 'C:' WinFS
haptic.xst.rose.hp.com:/C 'C:' WinFS
haptic.xst.rose.hp.com:/Z 'Z:' WinFS
```

To find the backup sessions in the database:

```
C:\Program Files\OmniBack\bin>omnidb -session
```

```
C:\Program Files\OmniBack\bin>omnidb -session
SessionID Type Status User.Group@Host
=====
2009/09/10-1 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-2 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-3 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-4 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-5 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-6 Backup Failed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-7 Backup Failed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-10 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-11 Backup Completed/Failure HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-12 Backup Completed/Failure HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-13 Media Failed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-14 Backup Failed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-15 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-16 Backup Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-17 Media Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/10-18 Backup Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/11-1 Backup Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
2009/09/15-1 Backup Completed HAPTIC\ADMINISTRATOR@haptic.xst.rose.hp.com
```

To perform a query of a specific session:

```
C:\Program Files\OmniBack\bin>omnidb -session 2009/09/10-18
```

```
C:\Program Files\OmniBack\bin>omnidb -session 2009/09/10-18
Object Name                               Object Type   Object Status  CopyID
=====
haptic.xst.rose.hp.com:/C 'C:'           WinFS        Completed     9 (0)
corisco.xst.rose.hp.com:/C 'C:'         WinFS        Completed     10 (0)
```

To look at a detailed session report:

```
C:\Program Files\OmniBack\bin>omnidb -session 2009/09/10-18 -detail
```

```
C:\Program Files\OmniBack\bin>omnidb -session 2009/09/10-18 -detail
Object name : haptic.xst.rose.hp.com:/C 'C:'
  Object type      : WinFS
  Object status    : Completed
  Started          : Thursday, September 10, 2009, 4:48:12 PM
  Finished         : Thursday, September 10, 2009, 4:50:40 PM
  Object size      : 2291677 KB
  Backup type      : Full
  Protection       : Protected for 1 day (Expired)
  Catalog retention : Same as data protection.
  Version type     : Normal
  Access           : Private
  Number of warnings : 0
  Number of errors  : 0
  Device name      : QUANTUM:SDLT320_1_haptic(2)
  Backup ID        : n/a
  Copy ID          : 9 (Orig)
  Encrypted        : Yes

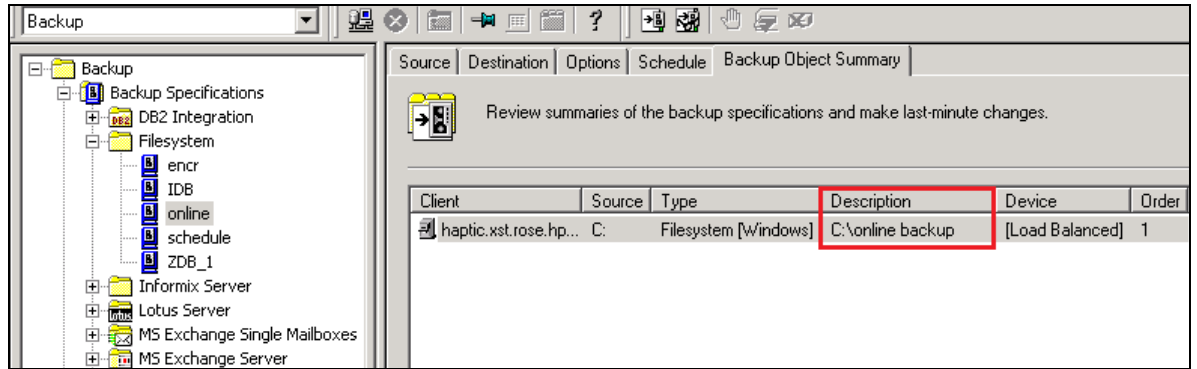
Object name : corisco.xst.rose.hp.com:/C 'C:'
  Object type      : WinFS
  Object status    : Completed
  Started          : Thursday, September 10, 2009, 4:48:12 PM
  Finished         : Thursday, September 10, 2009, 4:51:30 PM
  Object size      : 1773602 KB
  Backup type      : Full
  Protection       : Protected for 1 day (Expired)
  Catalog retention : Same as data protection.
  Version type     : Normal
  Access           : Private
  Number of warnings : 0
  Number of errors  : 0
  Device name      : QUANTUM:SDLT320_1_haptic(2)
  Backup ID        : n/a
  Copy ID          : 10 (Orig)
  Encrypted        : No
```

To see a list of files backed up during a specific session:

```
C:\Program Files\OmniBack\bin>omnidb -winfs "haptic.xst.rose.hp.com:/C" "C:" -
session 2009/09/22-5 -catalog
```

```
C:\Program Files\OmniBack\bin>omnidb -winfs "haptic.xst.rose.hp.com:/C" "C:" -session 2009/09/22-5 -catalog
Protection  Owner      Group      Size      Time      Path
=====
d---w----- -2  nogroup    0  9/18/2006  4:20:56 PM  /Data_Protector_6_0/
d---w----- -2  nogroup    0  9/7/2006   1:32:06 PM  /Data_Protector_6_0/DP_Demo/
d---w----- -2  nogroup    0  9/7/2006   1:32:29 PM  /Data_Protector_6_0/Docs/
d---w----- -2  nogroup    0  9/7/2006   1:31:21 PM  /Data_Protector_6_0/License/
d---w----- -2  nogroup    0  9/7/2006   1:31:21 PM  /Data_Protector_6_0/MPE/
d---w----- -2  nogroup    0  9/7/2006   1:31:14 PM  /Data_Protector_6_0/NetWare/
d---w----- -2  nogroup    0  9/7/2006   1:31:14 PM  /Data_Protector_6_0/OFM_9.5/
d---w----- -2  nogroup    0  9/7/2006   1:31:12 PM  /Data_Protector_6_0/OrderTool/
d---w----- -2  nogroup    0  9/7/2006   1:31:03 PM  /Data_Protector_6_0/Product_Information/
d---w----- -2  nogroup    0  9/12/2006  4:40:05 PM  /Data_Protector_6_0/debugviewers/
-w-----   -2  nogroup    2313270  9/7/2006   1:30:46 PM  /Data_Protector_6_0/autorun.bmp
-w-----   -2  nogroup    428032   9/7/2006   1:30:47 PM  /Data_Protector_6_0/autorun.exe
-w-----   -2  nogroup     159     9/7/2006   1:30:47 PM  /Data_Protector_6_0/autorun.inf
-w-----   -2  nogroup    2081     9/7/2006   1:30:47 PM  /Data_Protector_6_0/autorun.ini
-w-----   -2  nogroup    1078     9/7/2006   1:30:47 PM  /Data_Protector_6_0/dp.ico
d---w----- -2  nogroup    0  10/10/2006 12:24:28  /Data_Protector_6_0/i386/
d---w----- -2  nogroup    0  9/7/2006   1:31:41 PM  /Data_Protector_6_0/ia64/
d---w----- -2  nogroup    0  9/7/2006   1:31:02 PM  /Data_Protector_6_0/x8664/
d---w----- -2  nogroup    0  9/7/2006   1:32:06 PM  /Data_Protector_6_0/DP_Demo/Doc/
```

If the object is using a backup description, this needs to be specified on the command line as well. Both hostname and backup specification need to be specified between double quotes:



```
C:\Program Files\OmniBack\bin>omnidb -object
Object Name                                     Object type
-----
haptic.xst.rose.hp.com:/ [Database]: haptic.xst.rose.hp.com' IDB
haptic.xst.rose.hp.com:/BackupSession/Metadata MSU$SW
haptic.xst.rose.hp.com:/Filesystem/Z MSU$SW
corisco.xst.rose.hp.com:/C 'C:' WinFS
fyn.xst.rose.hp.com:/C 'C:' WinFS
haptic.xst.rose.hp.com:/C 'C:' WinFS
haptic.xst.rose.hp.com:/C 'C:\online backup' WinFS
haptic.xst.rose.hp.com:/Z 'Z:' WinFS

C:\Program Files\OmniBack\bin>omnidb -winfs "haptic.xst.rose.hp.com:/C" "C:\online backup"
SessionID      Started      Duration Object Status      Size [Kb]  NumberOfErr
-----
2009/09/22-8   2:28:11    00:00:28 Completed          703253      0
```

## omnimm

To see what files exist on a particular medium ID:

```
C:\Program Files\OmniBack\bin>omnimm -catalog cb180ec0:4320cd09:0714:0019
```

```
C:\Program Files\OmniBack\bin>omnimm -catalog 5003320a:4aa98cec:13ac:0001
Session : 2009/09/10-16
ObjectName : haptic.xst.rose.hp.com:/C 'C:'
ObjectType : WinFS
DiskAgentID : 1252625689
Object Status : Completed
=====
Session : 2009/09/10-18
ObjectName : corisco.xst.rose.hp.com:/C 'C:'
ObjectType : WinFS
DiskAgentID : 1252626472
Object Status : Completed
=====
Session : 2009/09/10-18
ObjectName : haptic.xst.rose.hp.com:/C 'C:'
ObjectType : WinFS
DiskAgentID : 1252626471
Object Status : Completed
=====
```

## devbra

To verify what devices are visible to the host, use the following command line option:

```
C:\Program Files\OmniBack\bin>devbra -dev
Tape    QUANTUM:SDLT320 Path: "scsi2:0:11:5" SN: "01Ub7I4k07"
        Description: Quantum SDLT1
        Revision: R210 Device type: sdlt [14] Flags: 0x0001
Tape    QUANTUM:SDLT320 Path: "scsi2:0:11:4" SN: "01Ub7I4k06"
        Description: Quantum SDLT1
        Revision: R210 Device type: sdlt [14] Flags: 0x0001
Tape    QUANTUM:SDLT320 Path: "scsi2:0:11:3" SN: "01Ub7I4k05"
        Description: Quantum SDLT1
        Revision: R210 Device type: sdlt [14] Flags: 0x0001
Tape    QUANTUM:SDLT320 Path: "scsi2:0:11:2" SN: "01Ub7I4k04"
        Description: Quantum SDLT1
        Revision: R210 Device type: sdlt [14] Flags: 0x0001
Exch    HP:MSL6000 Series Path: "Changer2:0:11:1" SN: "01Ub7I4k03"
        Description: CLAIMED:HP StorageWorks MSL 6000 Series
        Revision: 0430 Flags: 0x0016 Slots: 60 Drives: 4
        Drive(s) SN:
                "01Ub7I4k04"
                "01Ub7I4k05"
                "01Ub7I4k06"
                "01Ub7I4k07"
```

**Note:** As an alternative is the `devbra` command, you can use the HP StorageWorks Library and Tape Tools (HP L&TT):

<http://h18006.www1.hp.com/products/storageworks/lit/index.html>

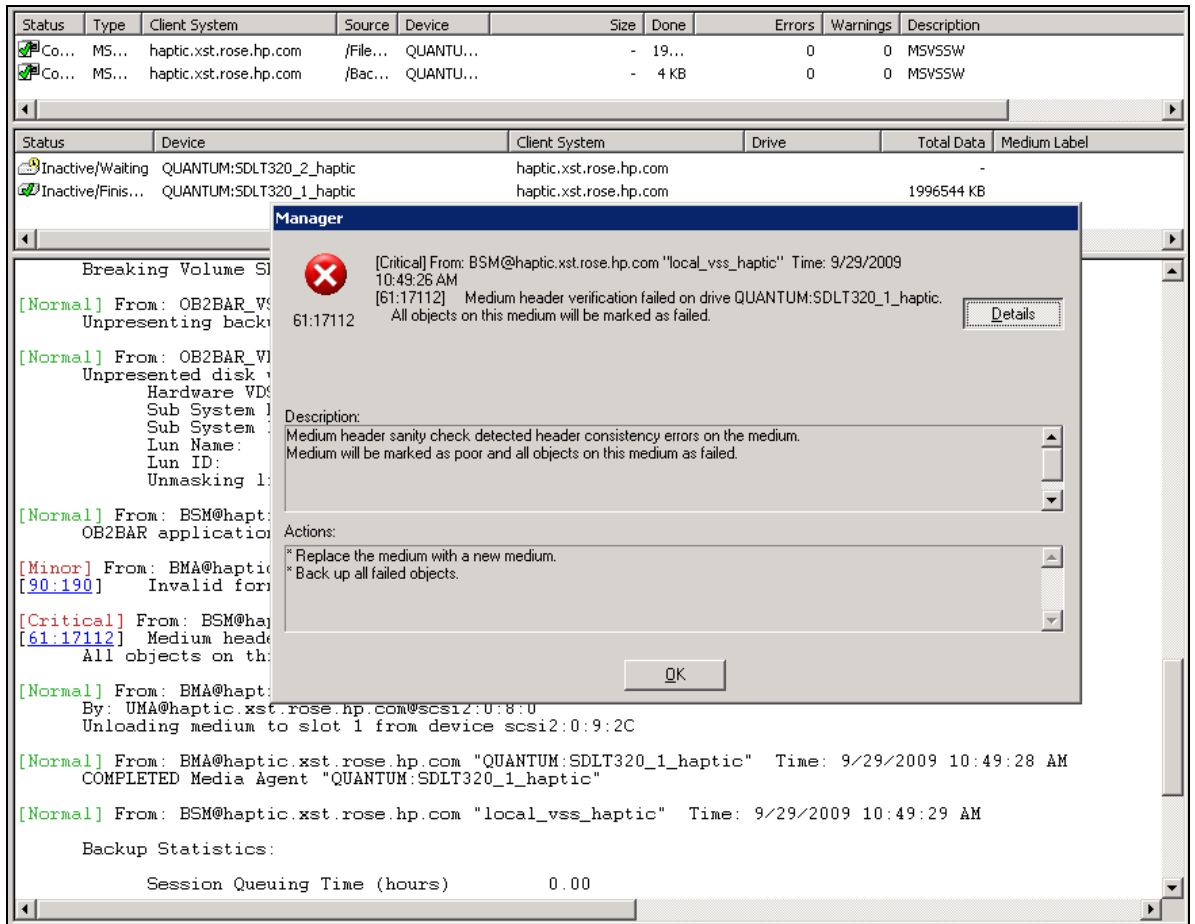
## Log files and troubleshooting

### Data required for support calls

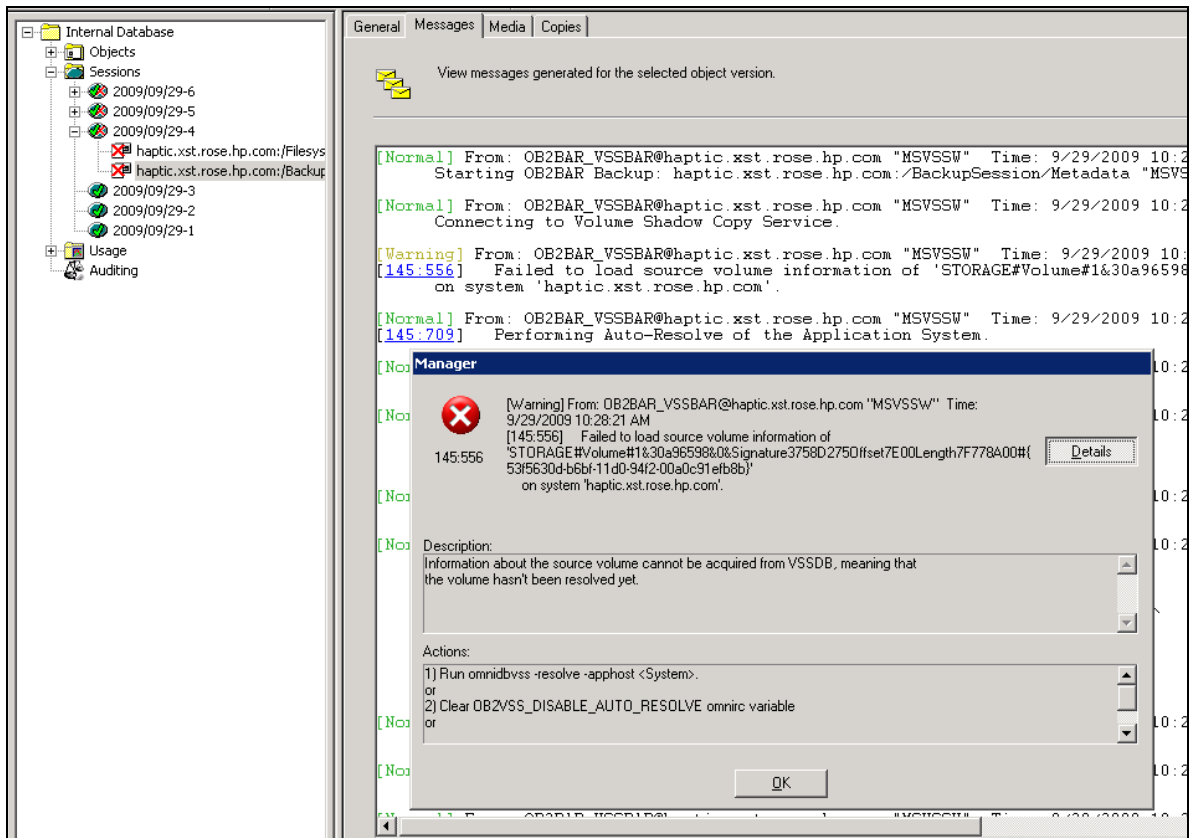
#### The session log

The Data Protector session log lists error messages. Click on an error to get more details.

*Example:* When Data Protector finds poor media in the library, it will fail the backup session with error messages such as those below in the session window. You can also view running sessions via the Monitor window.



To look at the failed session messages after the session window has been closed, go to the Internal Database view, and find the session message window.





## Support files

The table below describes the Data Protector log files:

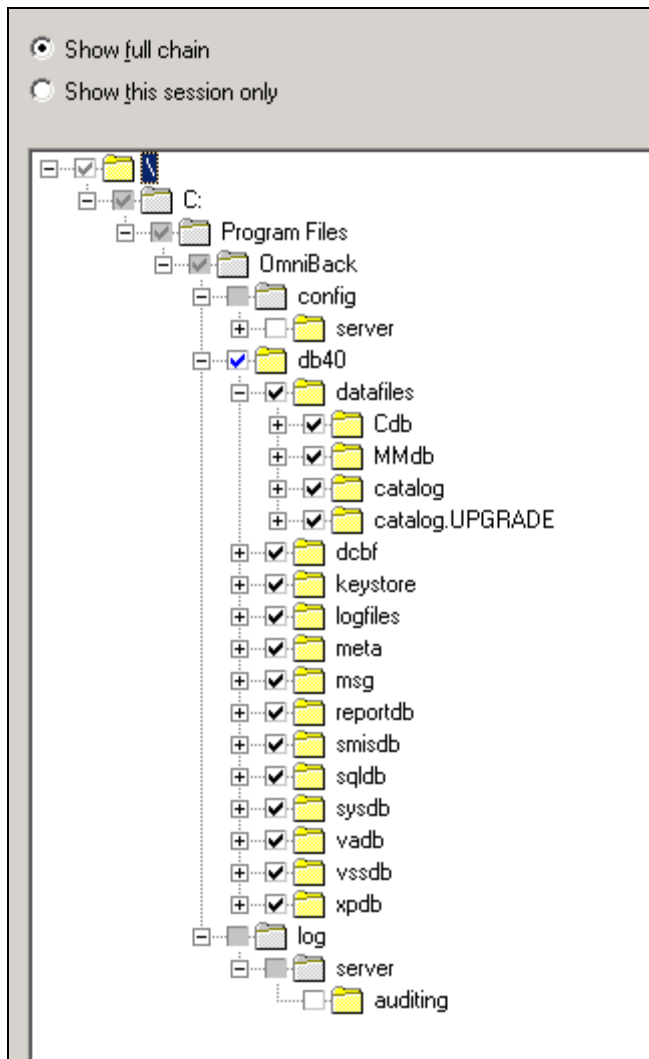
Log File	Description
debug.log	Contains unexpected conditions. While some can help you, the information is mainly used by the support organization.
inet.log	Contains local security-related events for the client, such as denied requests. On UNIX, it also contains all requests made to the Data Protector Inet service.
enhincr.log	Contains information on enhanced incremental backup activities, for example detailed error information for problems with the enhanced incremental backup repository.
Ob2EventLog.txt	Contains Data Protector events and notifications. The Event log represents a centralized Data Protector event depository.
media.log	Each time a medium is used for backup, initialized, or imported, a new entry is made to this log. The file can be used when recovering the IDB to find the medium with the IDB backup and to find out which media were used after the last backup of the IDB.
omnisv.log	Contains information on when Data Protector services were stopped and started.
security.log	Contains security-related events on the Cell Manager. Some events may be a result of normal operation and simply mean that an operation was attempted that is not allowed by a particular user. On the other hand, events can indicate that deliberate break-in attempts may be in progress.
purge.log	Contains traces of the background purge of the IDB.
RDS.log	Contains IDB logs. The file resides on the Cell Manager in: <ul style="list-style-type: none"> <li>• <i>UNIX systems:</i> /var/opt/omni/server/db40/datafiles/catalog</li> <li>• <i>Windows Server 2008:</i> &lt;Data_Protector_program_data&gt;\db40\datafiles\catalog</li> <li>• <i>Other Windows systems:</i> &lt;Data_Protector_home&gt;\db40\datafiles\catalog</li> </ul>
sanconf.log	Contains session reports generated by the sanconf command.
sm.log	Contains details on internal errors that occurred during backup and restore sessions, such as errors in parsing backup specifications.
upgrade.log	Created during upgrade; contains upgrade core part (UCP) and upgrade detail part (UData Protector) messages.
OB2_Upgrade.log (UNIX only)	Created during upgrade; contains traces of the upgrade process.
IS_install.log	Contains a trace of remote installation and resides on the Installation Server.
sap.log, oracle8.log, informix.log, sybase.log, db2.log	Application-specific logs containing traces of integration calls between the application and Data Protector. The files reside on the application systems.

## Database copy

If a copy of the IDB is needed for support, stop the Data Protector services, zip up the db40 directory and restart the Data Protector services. The required files can be found under the restore window of the IDB backup. Configuration parameters such as omnirc and global files, are part of the IDB backup session. Zip up the entire db40 folder and the config/server folder.

**Note:** If no downtime is possible, a backup can be run from the IDB as well, and the tapes can be exported and sent to HP Support.





## Debugging Data Protector

Almost all Data Protector commands can be started with an additional `-debug` parameter that has the following syntax:

```
-debug 1-99[,C:<n>][,T:<s>][,U] <XYZ> [<host>]
```

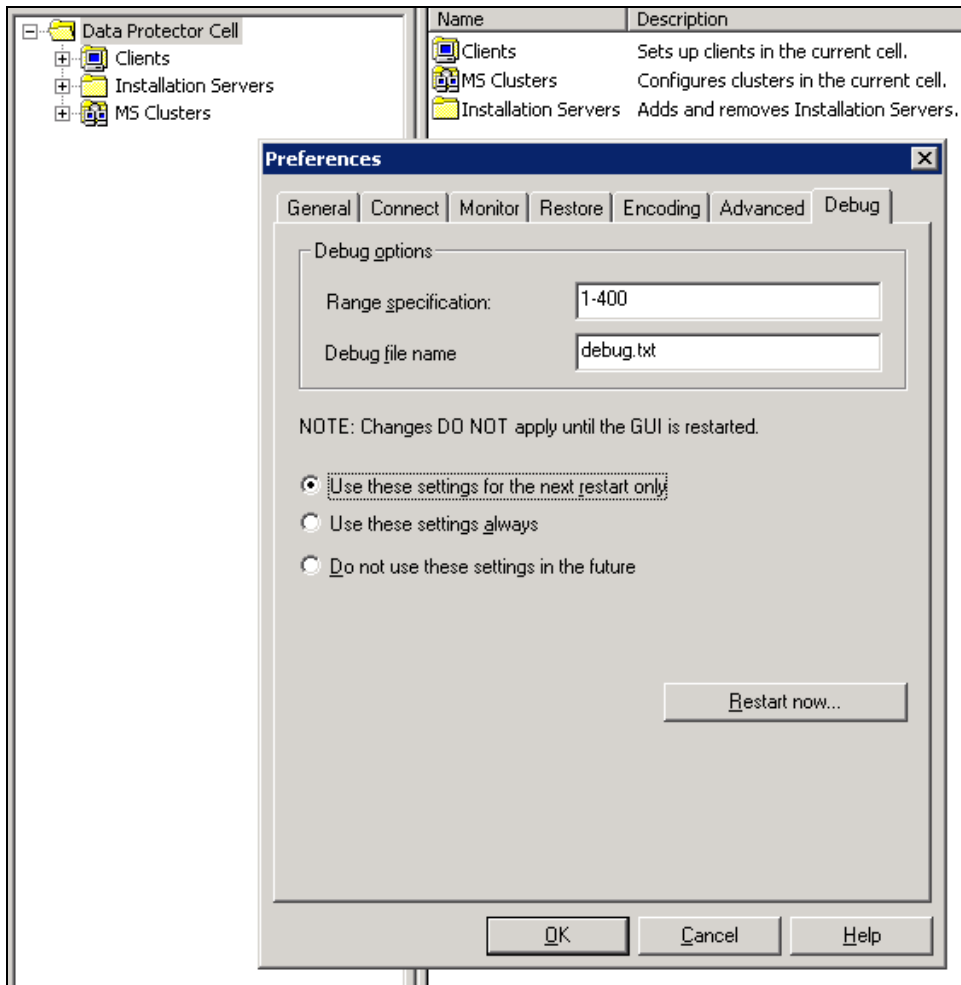
Where:

- 1–200 is the debug range. Specify the range 1–200 unless instructed otherwise. Specify optional parameters as a part of the range parameter, separated by commas:
  - C:<n> limits the size of debug files to n kilobytes. The minimum value is 4 (4 kB) and the default value is 1024 (1 MB).
  - T:<s> is the timestamp resolution, where the default value is 1, 1000 means the resolution is one millisecond and 0 means timestamps are turned off.
 

**Note:** On some platforms (Novell NetWare, MPE), millisecond resolution is not available.
  - U is the Unicode flag. If it is specified, the debug files on Windows are written in the Unicode format.
- <XYZ> is the debug postfix, for example `DBG_01.txt`.
- <host> is a list of clients where debugging is turned on.

To enable debugging, go to **File -> Preferences -> Debug**, and enable the debug settings: Range 1–400, filename `debug.txt`.

Click on **Use these settings for the next restart only**, and click **Restart now...**



The Data Protector debug log files will be located under:

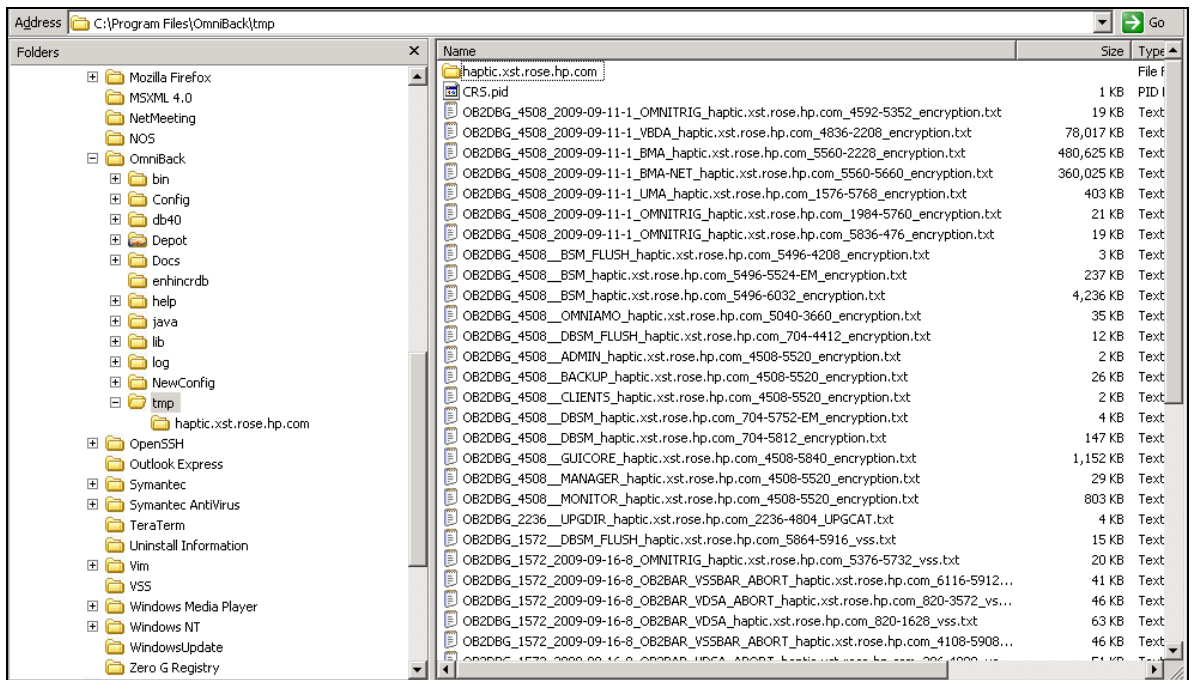
- Unix: /tmp
- Windows: C:\Program Files\Omniback\tmp

You can change the location with omnirc option OB2DBGDIR:

```
# OB2DBGDIR=<pathname>
# Default: none
# This variable is used to change the location of debug files on a per
# system basis. You have to specify a fully qualified path of an existing
# directory. This variable has precedence over the paths specified by the
# postfix parameter.
# By default, this variable is not set. If this variable is not set, the
# pathname is set as /tmp (UNIX) or <Data_Protector_home>\tmp (Windows).
```

Special debug files created during installation are located in the `TMP` directory of the account used at installation time.

Make sure they do not fill up the C drive; older debug files can be deleted when they have been made available to HP support.



Use the command line debug log collector to zip up the debug files from Cell Manager and clients.

```
C:\Program Files\OmniBack\bin>omnidlc
Usage: omnidlc -version | -help
Usage: omnidlc {-session sessionID | -did debugID
| -postfix string | -no_filter}
[-hosts list]
[-pack filename | -depot directory | -space | -delete_dbg]
[-no_logs | [-no_getinfo] [-no_compress] [-no_config]
[-no_debugs | -debug_loc Dir1 [Dir2 ...]] [-verbose]
[-add_info [-any | host] path]
Usage: omnidlc -localpack [filename]
Usage: omnidlc -unpack [filename]
Usage: omnidlc -uncompress filename
Usage: omnidlc [-hosts list] -del_ctrace_log
```

To unpack debug files that have been zipped on a UNIX Cell Manager, on a Windows system, copy the omnidlc.exe file over to a Windows system, and unpack the \*.pck files, running omnidlc -unpack.

**Note:** This is an undocumented and unsupported operation.

## Inet connection

When the Data Protector agent is running, the port 5555 should respond with the Data Protector agent information to the telnet command:

```
telnet [-a[-e escape char]][-f log file][-l user][-t term][host [port]]
-a Attempt automatic logon. Same as -l option except uses
the currently logged on user's name.
-e Escape character to enter telnet client prompt.
-f File name for client side logging
-l Specifies the user name to log in with on the remote system.
Requires that the remote system support the TELNET ENVIROM option.
-t Specifies terminal type.
Supported term types are vt100, vt52, ansi and vtnt only.
host Specifies the hostname or IP address of the remote computer
to connect to.
port Specifies a port number or service name.
```

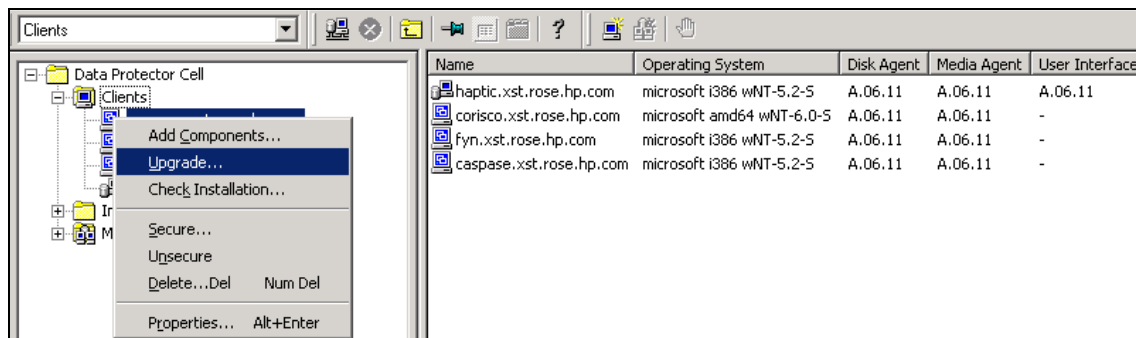
Example:

```
C:\Program Files\OmniBack\bin>telnet caspase 5555
```

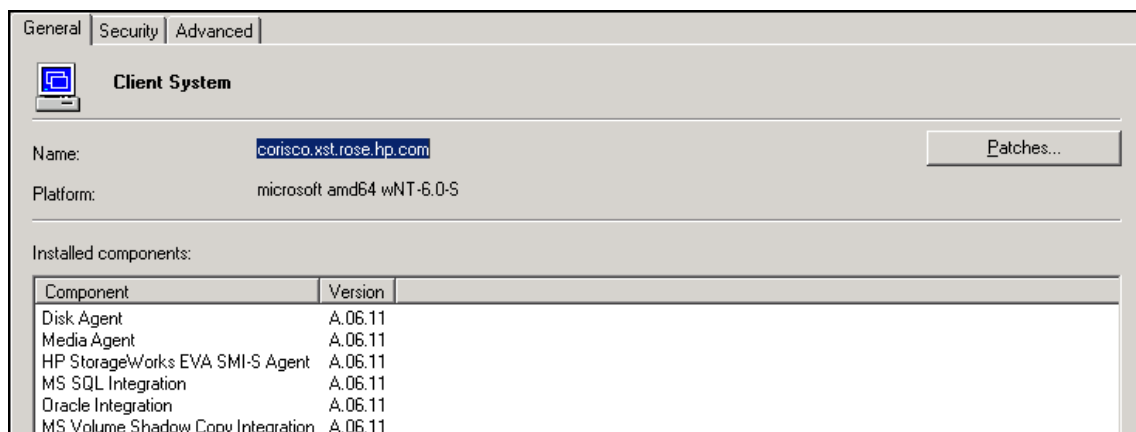
```
HP Data Protector A.06.11: INET, internal build 243, built on Tuesday, August 25, 2009, 7:08 AM
```

## Patch upgrade and versioning

Patches can be pushed from the Cell Manager or Installation Server GUI, or installed locally from the CDs or DVD. Right-click on the host name to choose **Add Components** or **Upgrade**, and select the components that need to be installed.



To verify the components that are installed, click on the client system **Patches**, and you will see the installed patch list and levels.



## Security

### Secure cell/client

You can secure all clients in the cell:

1. In the Context List, click **Clients**.
2. In the Scoping Pane, right-click **Clients** and click **Cell Secure**.
3. Type the names of the systems that will be allowed to access all clients in the cell or search for the systems using the Network (on Windows GUI only) or Search tabs. Click **Add** to add each system to the list.
4. Click **Finish** to add the selected systems to the `allow_hosts` file.

Clients will verify the source for each request and allow only those requests received from clients selected in the Enable Security on selected client(s) window. These clients are listed in the `allow_hosts` file. If the request is denied, the event is logged to the `inet.log` file in the following directories:

- *HP-UX and Solaris systems:* `/var/opt/omni/log`
- *Other UNIX:* `/usr/omni/config/cell`
- *Windows Vista, Windows Server 2008:* `<Data_Protector_program_data>/log`
- *Other Windows systems:* `<Data_Protector_home>/log`

When you secure an entire cell, all clients residing in this cell at the time are secured. When you add new clients to the cell, you should also secure them.

**Note:** For more information on securing clients and security considerations, see the *HP Data Protector installation and Licensing Guide (B6960-90152)*.

## Firewall configuration

You can configure your backup environment so that the Cell Manager and GUI are in the intranet and some Disk Agents and Media Agents are in the DMZ.

The Disk Agent and a Media Agent need to accept connections from the Session Manager on port 5555. This leads to the following rules for a firewall:

- Allow connections from the CM system to port 5555 on the DA system
- Allow connections from the CM system to port 5555 on the MA system

A Media Agent also needs to accept connections from the Disk Agent. However, since these two agents do not communicate through the firewall, you do not need to define a firewall rule for them.

Both agents may connect to the Session Manager and a Media Agent may need to connect to a Utility Media Agent (UMA). However, this only occurs when shared tape libraries are used or the `Reconnect broken connections` option is enabled.

Since all connections that need to go through the firewall connect to the fixed port number 5555, you do not need to define the `OB2PORTRANGE` or `OB2PORTRANGESPEC` variables in this environment.

### Notes:

- This setup does not allow the backup of databases or applications using on clients in the DMZ.
- If a device in the DMZ has robotics configured on a separate client, this client must also be in the DMZ.

# Operation audit checklist

## Backing-up data

Control Objective	Procedure	Result
Backup concepts	Before you backup, review key concepts and requirements.	
	Determine where you will store the backup.	
	Determine which files, folders, or volumes you want to back up and whether the backups will need to be used for operating system (critical volumes only), full server (all volumes), system state, or bare metal recovery.	
	Determine how many times a day and at what times you want to run backups.	
	Determine whether you will use a volume, a single disk, multiple disks, or a remote shared folder, or tape devices to store the backups.	
Backup operations	Verify that you are logged on as a member of the Backup Operators group or Administrator group.	
	Verify that you can connect to all shared folders on other computers that need to be backed up.	
	If you are using an external storage device, verify that it is on the hardware compatibility list. Make sure it is cabled directly to the computer performing the backup and that the computer is turned on.	
	Insert the required tape(s) into the tape drive. If backing up to a disk drive, verify there is enough available space.	
	If you are backing up an Encrypted File System, first back up the designated recovery agent's private key to ensure the successful recovery of encrypted data in case of a disaster such as a full system failure.	
	To back up files manually, use the Backup wizard or click the Backup tab to select files to backup. To back up files automatically, use the schedule feature in backup.	
	Verify if the backup policies and procedures cover following minimum requirements: <ul style="list-style-type: none"> <li>• The Servers to be backed up.</li> <li>• Location of mission critical files.</li> <li>• The files/folders to be backed up for users.</li> <li>• Schedule of back up.</li> <li>• Backup operators and their rights.</li> <li>• Key backup procedures (If key based encryption or authentication are used).</li> <li>• Location of Backups.</li> <li>• Users authorized to restore data.</li> <li>• Restoration procedures.</li> </ul>	
	Identify all critical computer processing environments for which backup copies are required.	
	For each environment, outline the specific	

	rotational procedure by identifying the type and level of backup, which generation is moved off-site, how many generations are retained off-site, and which day the rotation occurs.	
	For each environment, obtain screen captures from the backup software that show: <ul style="list-style-type: none"> <li>• The selection of files that are backed up.</li> <li>• The schedule that the backup job is set to follow.</li> <li>• A recent log file showing a successful backup of the system.</li> <li>• A recent restore log file (if available) showing a successful restore of the system.</li> </ul>	

## Restoring data

<b>Control Objective</b>	<b>Procedure</b>	<b>Result</b>
Restore concepts	Before you restore, review concepts and requirements.	
	Determine what you want to recover.	
	Determine what backup you will use to recover from.	
	Determine where you want to recover to.	
	Determine what backup you will use to recover from.	
	Determine where you want to recover to (the same computer or another computer) and whether it has enough space for what you are recovering.	
	Determine whether you want to recover all critical volumes (volumes containing operating system components—you can exclude non-critical volumes during the recovery) or the full server (all volumes).	
Restore operations	Verify that you are logged on as a member of the Backup Operators group or Administrators group.	
	Verify that you can connect to all shared folders on other computers that need to be restored.	
	Insert the required tape(s) into the tape drive or library.	
	To restore files manually, click the Restore tab to select files to restore, or use the Backup or Restore Wizard.	
	If you are restoring an Encrypted File System on a system where the private key for the encrypted data is somehow inaccessible (for example, on a computer that is not part of a network), or is corrupted or lost, import the designated recovery agent's private key.	

## Short-term maintenance checklist

<b>Control Objective</b>	<b>Procedure</b>	<b>Result</b>
Backup maintenance	Check the Data Protector Event log for daily notifications.	
	Restart failed backup sessions.	
	Resume failed sessions.	
Media maintenance	Verify media and pool usage.	
	Resolve poor media issues.	

## Long term maintenance checklist

<b>Control Objective</b>	<b>Procedure</b>	<b>Result</b>
Database maintenance	Run the IDB purge operation.	
	Analyze DCBF directories' capacity usage.	
	Check the size of the tablespaces.	
	Verify IDB notifications and reporting.	
Log files	Monitor log file sizes.	

## Off-site vaulting

<b>Control Objective</b>	<b>Procedure</b>	<b>Result</b>
Distance of off-site storage	Physically visit the off-site storage facility, if it is within reasonable distance of the site, or use alternative review techniques. Describe the location of the off-site storage facility.	
Off-site backup tape	While at the off-site storage facility, verify that the proper backup media including all incremental and full image backups identified above as being retained off-site are safe, current, and readily available in off-site storage.	
Existence of system documentation in the off-site storage	While at the off-site storage facility, verify that appropriate systems documentation is retained in off-site storage.	
Environmental control of the off-site storage	Determine that the off-site storage area is reasonably removed from the computer room to avoid simultaneous destruction resulting from a likely natural or man-made disaster, is environmentally safe for the type of media stored, is adequately safeguarded to prevent the loss or	



	misappropriation of the information stored, and is reasonably accessible during non-business hours.	

## References

[www.hp.com/go/dataprotector](http://www.hp.com/go/dataprotector)

© Copyright 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a U.S. registered trademark of Linus Torvalds. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group.

4AA1-8817ENA, March 2010

