

HP Data Protector A.06.11

Command line interface reference



Legal and notice information

© Copyright 1999, 2009 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft®, Windows®, Windows XP®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Java is a US trademark of Sun Microsystems, Inc.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Printed in the US

Contents

Publication history	7
About this guide	9
Reference page organization	9
Intended audience	10
Documentation set	10
Guides	10
Online Help	13
Documentation map	14
Abbreviations	14
Map	15
Integrations	16
Document conventions and symbols	18
Reference page conventions	19
General information	20
HP technical support	20
Subscription service	20
HP websites	21
Documentation feedback	21
 I Section 9: Introduction	 23
omniintro	25
 II Section 1: User Commands	 45
omniabort	47
omniamo	49
omnib	51
omnicc	71
omnicellinfo	77
omniclus	81
omnicreatedl	85
omnidb	99
omnidbsmis	111

omnidbva	121
omnidbvss	125
omnidbvp	131
omnidownload	137
omniiso	139
omnimcopy	143
omniminit	147
omnimlist	151
omnim	155
omnimnt	167
omnimver	169
omniobjconsolidate	171
omniobjcopy	179
omniobjverify	189
omnir	195
omnirpt	241
omnistat	265
omniupload	269
omniusers	271
syb_tool	275

III Section 1M: Administrative Commands 279

cjutil	281
NNMpost.ovpl	283
NNMpre.ovpl	285
NNMScript.exe	287
ob2install	289
omnicheck	293
omnicjutil	297
omnidbcheck	301
omnidbinit	305
omnidbrestore	307
omnidbupgrade	315
omnidbutil	317
omnidlc	331
omnidr	339
omnihealthcheck	343
omniinetpasswd	345
omniinstlic	349
omniintconfig.pl	351
omnikeymigrate	355
omnikeytool	357

omnimigrate.pl	361
omniofflr	365
omniresolve	373
omnirsh	375
omnisetup.sh	377
omnisrupdate	383
omnistoreapputil	387
omnisv	389
omnitrig	391
sanconf	393
uma	403
upgrade_cm_from_evaa	411
util_cmd	413
util_oracle8.pl	421
util_vmware.exe	427
winomnimigrate.pl	433
 IV Section 5: Miscellaneous	 437
omnigui	439

Tables

1	Edition history	7
2	Document conventions	18

Publication history

Guide updates may be issued between editions to correct errors or document product changes. To ensure that you receive updated or new editions, subscribe to the appropriate product support service. See your HP sales representative for details.

Table 1 Edition history

Part number	Guide edition	Product
N/A	October 2004	Data Protector Release A.05.50
B6960-90030	August 2006	Data Protector Release A.06.00
N/A	November 2008	Data Protector Release A.06.10
N/A	September 2009	Data Protector Release A.06.11

About this guide

This guide provides information about:

- Data Protector command line interface commands, their options, and usage

This reference guide does *not* describe concepts, the GUI, or provides details about the integrations.

The HP Data Protector command line interface reference contains the reference pages for Data Protector A.06.11 commands.

Reference pages are available on UNIX systems as man pages. For more information about man pages, refer to the man page for `man` using the command `man man`.

The command synopsis for every command is also available using the `-help` option.

For an introduction to Data Protector A.06.11 commands, refer to the “[omniintro](#)” reference page in section 9.



IMPORTANT:

On Windows Vista and Windows Server 2008 systems, Data Protector commands can only be invoked in a Command Prompt window which is granted administrative privileges.

Reference page organization

The reference pages are divided in specialized sections (volumes), based on the UNIX man page organization. Each reference page belongs to a volume:

Section 1: User Commands

Commands, used by the user.

Section 1M: Administrative Commands

Commands, used by the administrator.

Section 5: Miscellaneous

A variety of information, such as information about GUI components, and more.

Section 9: Introduction

Introduction to HP Data Protector.

All commands in a section are sorted by alphabetical order.

Reference pages are often referred to by name and section number in the form *pagename(section)*.

Intended audience

This guide is intended for administrators with knowledge of:

- Basic operating system commands and utilities
- Command prompt/shell concepts and usage
- Data Protector backup and restore concepts

The reference pages supplement other Data Protector documentation and require good overall knowledge of the product.

Documentation set

Other documents and online Help provide related information.

Guides

Data Protector guides are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the *English Documentation & Help* component on Windows or the *OB2-DOCS* component on UNIX. Once installed, the guides reside in the *Data_Protector_home\docs* directory on Windows and in the */opt/omni/doc/C* directory on UNIX.

You can find these documents from the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

In the Storage section, click **Storage Software** and then select your product.

- *HP Data Protector concepts guide*

This guide describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented online Help.

- *HP Data Protector installation and licensing guide*
This guide describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This guide also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.
- *HP Data Protector troubleshooting guide*
This guide describes how to troubleshoot problems you may encounter when using Data Protector.
- *HP Data Protector disaster recovery guide*
This guide describes how to plan, prepare for, test and perform a disaster recovery.
- *HP Data Protector integration guides*
These guides describe how to configure and use Data Protector to back up and restore various databases and applications. They are intended for backup administrators or operators. There are four guides:
 - *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*
This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server, Microsoft SQL Server, and Volume Shadow Copy Service.
 - *HP Data Protector integration guide for Oracle and SAP*
This guide describes the integrations of Data Protector with Oracle, SAP R/3, and SAP DB/MaxDB.
 - *HP Data Protector integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino*
This guide describes the integrations of Data Protector with the following IBM applications: Informix Server, IBM DB2, and Lotus Notes/Domino Server.
 - *HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*
This guide describes the integrations of Data Protector with VMware Virtual Infrastructure, Sybase, Network Node Manager, Network Data Management Protocol Server, and Citrix XenServer.
- *HP Data Protector integration guide for HP Service Information Portal*

This guide describes how to install, configure, and use the integration of Data Protector with HP Service Information Portal. It is intended for backup administrators. It discusses how to use the application for Data Protector service management.

- *HP Data Protector integration guide for HP Reporter*
This manual describes how to install, configure, and use the integration of Data Protector with HP Reporter. It is intended for backup administrators. It discusses how to use the application for Data Protector service management.
- *HP Data Protector integration guide for HP Operations Manager for UNIX*
This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX.
- *HP Data Protector integration guide for HP Operations Manager for Windows*
This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on Windows.
- *HP Data Protector integration guide for HP Performance Manager and HP Performance Agent*
This guide provides information about how to monitor and manage the health and performance of the Data Protector environment with HP Performance Manager (PM) and HP Performance Agent (PA) on Windows, HP-UX, Solaris, and Linux.
- *HP Data Protector zero downtime backup concepts guide*
This guide describes Data Protector zero downtime backup and instant recovery concepts and provides background information on how Data Protector works in a zero downtime backup environment. It is intended to be used with the task-oriented *HP Data Protector zero downtime backup administrator's guide* and the *HP Data Protector zero downtime backup integration guide*.
- *HP Data Protector zero downtime backup administrator's guide*
This guide describes how to configure and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility and TimeFinder, and HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.
- *HP Data Protector zero downtime backup integration guide*
This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases. The guide also

describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.

- *HP Data Protector MPE/iX system user guide*
This guide describes how to configure MPE/iX clients and how to back up and restore MPE/iX data.
- *HP Data Protector Media Operations user guide*
This guide provides tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.
- *HP Data Protector product announcements, software notes, and references*
This guide gives a description of new features of HP Data Protector A.06.11. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.
- *HP Data Protector product announcements, software notes, and references for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal*
This guide fulfills a similar function for the listed integrations.
- *HP Data Protector Media Operations product announcements, software notes, and references*
This guide fulfills a similar function for Media Operations.
- *HP Data Protector command line interface reference*
This guide describes the Data Protector command-line interface, command options and their usage as well as provides some basic command-line examples.

Online Help

Data Protector provides context-sensitive (F1) Help and Help Topics for Windows and UNIX platforms.

You can access the online Help from the top-level directory on the installation DVD-ROM without installing Data Protector:

- **Windows:** Unzip `DP_help.zip` and open `DP_help.chm`.
- **UNIX:** Unpack the zipped tar file `DP_help.tar.gz`, and access the online Help system through `DP_help.htm`.

Documentation map

Abbreviations

Abbreviations in the documentation map that follows are explained below. The guide titles are all preceded by the words “HP Data Protector”.

Abbreviation	Guide
CLI	Command line interface reference
Concepts	Concepts guide
DR	Disaster recovery guide
GS	Getting started guide
Help	Online Help
IG-IBM	Integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service
IG-O/S	Integration guide for Oracle and SAP
IG-OMU	Integration guide for HP Operations Manager for UNIX
IG-OMW	Integration guide for HP Operations Manager for Windows
IG-PM/PA	Integration guide for HP Performance Manager and HP Performance Agent
IG-Report	Integration guide for HP Reporter
IG-SIP	Integration guide for HP Service Information Portal
IG-Var	Integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, Network Data Management Protocol Server, and Citrix XenServer.

Abbreviation	Guide
Install	Installation and licensing guide
MO GS	Media Operations getting started guide
MO RN	Media Operations product announcements, software notes, and references
MO UG	Media Operations user guide
MPE/iX	MPE/iX system user guide
PA	Product announcements, software notes, and references
Trouble	Troubleshooting guide
ZDB Admin	ZDB administrator's guide
ZDB Concept	ZDB concepts guide
ZDB IG	ZDB integration guide

Map

The following table shows where to find information of different kinds. Shaded squares are a good place to look first.

	Help	GS	Concepts	Install	Trouble	DR	PA	Integration Guides							ZDB			MO			MPE/iX	CLI
								MS	O/S	IBM	Var	OV	OVOU	OVOW	Concept	Admin	IG	GS	User	PA		
Backup	X	X	X					X	X	X	X				X	X	X				X	
CLI																						X
Concepts/ Techniques	X		X					X	X	X	X	X	X	X	X	X	X				X	
Disaster Recovery	X		X			X																
Installation/ Upgrade	X	X		X			X					X	X	X				X	X		X	
Instant Recovery	X		X												X	X	X					
Licensing	X			X			X												X			
Limitations	X				X		X	X	X	X	X			X			X			X		
New features	X						X															
Planning strategy	X		X									X			X							
Procedures/ Tasks	X			X	X	X		X	X	X	X	X	X	X		X	X		X			
Recommendations			X				X								X					X		
Requirements				X			X	X	X	X	X			X				X	X	X		
Restore	X	X	X					X	X	X	X					X	X				X	
Supported configurations															X							
Troubleshooting	X			X	X			X	X	X	X	X				X	X					

Integrations

Look in these guides for details of the following integrations:

Integration	Guide
HP Operations Manager for UNIX/for Windows	IG-OMU, IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA

Integration	Guide
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	all ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	all ZDB
HP StorageWorks Virtual Array (VA)	all ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
Media Operations	MO User
MPE/iX system	MPE/iX
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG

Integration	Guide
Sybase	IG-Var
EMC Symmetrix	all ZDB
VMware	IG-Var

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: Table 2 on page 18	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
<i>Italic text</i>	Text emphasis
Monospace text	<ul style="list-style-type: none"> • File and directory names • System output • Code • Commands, their arguments, and argument values
<i>Monospace, italic text</i>	<ul style="list-style-type: none"> • Code variables • Command variables
Monospace, bold text	Emphasized monospace text

CAUTION:

Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT:

Provides clarifying information or specific instructions.



NOTE:

Provides additional information.



TIP:

Provides helpful hints and shortcuts.

Reference page conventions

All reference pages follow established section formats, but not all sections are present in each reference (man) page.

NAME

Gives the name of the command and a brief description of the commands purpose.

SYNOPSIS

Describes the syntax of the command.

The command line synopsis is formatted in the following way:

```
command -option replaceable [-option2  
replaceable...] {-option3 | -option4}
```

Where:

- *Italic* strings represent variables that should be replaced by the user with the appropriate value.
- Square brackets ([]) indicate that the argument is optional.
- An ellipsis (. . .) indicates that the previous argument can be repeated.
- Vertical bars (|) between several arguments indicate that only one argument from the group can be specified at once.

Groups can be optional (inside square brackets) or required (inside curly brackets, {}).

DESCRIPTION	A more detailed description of the command.
OPTIONS	Detailed descriptions for all options.
NOTES	Contains important notes.
EXAMPLES	Provides examples on command usage.
SEE ALSO	Lists man pages, containing related information.

General information

General information about Data Protector can be found at <http://www.hp.com/go/dataprotector>.

HP technical support

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/e-updates>

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- <http://www.hp.com>
- <http://www.hp.com/go/software>
- <http://www.hp.com/support/manuals>
- <http://h20230.www2.hp.com/selfsolve/manuals>
- <http://www.hp.com/support/downloads>

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to DP.DocFeedback@hp.com. All submissions become the property of HP.

Section 9: Introduction

omniintro

introduction to HP Data Protector command utilities

omniintro

DESCRIPTION

HP Data Protector is an enterprise backup solution that provides reliable data protection and high accessibility for business data. Data Protector provides extensive media management, unattended backups, post-backup data management, integrations with various databases and supports various backup and other backup-dedicated devices. For information on Data Protector functionality and concepts, refer to the online documentation.

COMMANDS

USER COMMANDS (1):

`omniabort`

Aborts an active session.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniamo`

Starts an automated media operation session.

This command is available on the Data Protector Cell Manager.

`omnib`

Backs up filesystems, disk images, the Data Protector internal database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Portal Server (SPS), SAP R/3, SAP DB/MaxDB, Oracle, Informix Server, VMware Virtual Infrastructure (VMware), Sybase, Lotus, IBM DB2 UDB, NetWare objects, and NDMP objects. This is the only command supported with the MPE/iX integration.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnicc`

Handles the Data Protector licensing, reports the number of configured and available Data Protector licenses, installs the licenses, imports and exports Data Protector clients, and manages access to secured clients.

This command is available on systems with any Data Protector component installed.

`omnicellinfo`

Displays configuration information about the Data Protector cell.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniclus`

Manages load balancing in a cluster environment in the event of an application (Data Protector or other) failover.

This command is available on systems with the Data Protector `MS Cluster Support` component installed (Windows systems) and on the Data Protector Cell Manager (UNIX systems).

`omnicreatedl`

Creates a Data Protector backup specification file (datalist); or an HP StorageWorks Disk Array XP, HP StorageWorks Virtual Array, or HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB backup specification file (datalist).

This command is available on systems with the Data Protector `User Interface` component installed.

`omnidb`

Queries the Data Protector internal database (IDB).

This command is available on systems with the Data Protector `User Interface` component installed.

`omnidbsmis`

Executes administrative tasks required for managing the HP StorageWorks Enterprise Virtual Array (EVA) Command View.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnidbva`

Queries the ZDB database (VADB) and administers the VA LUN Exclude File, instant recovery and password information.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnidbvss`

Queries the VSS database; manages, browses, and lists the items of the VSS database.

This command is available on systems with the Data Protector User Interface component installed.

`omnidbxp`

Queries the ZDB database (XPDB), manipulates the XP LDEV exclude file, and configures the HP StorageWorks Disk Array XP command devices usage.

This command is available on systems with the Data Protector User Interface component installed.

`omnidownload`

Downloads information about a backup device and a library from the Data Protector internal database (IDB).

This command is available on systems with the Data Protector User Interface component installed.

`omniiso`

Primarily serves as a pre-exec script to prepare the ISO image file for One Button Disaster Recovery (OBDR); can also be used as a standalone command to automate your backup and disaster recovery process.

This command is available on systems with the Data Protector Automatic Disaster Recovery component installed.

`omnimcopy`

Makes a copy of a Data Protector medium using Data Protector backup devices as the source and destination.

This command is available on systems with the Data Protector User Interface component installed.

`omniminit`

Initializes a Data Protector medium.

This command is available on systems with the Data Protector User Interface component installed.

`omnimlist`

Lists the contents of a Data Protector medium.

This command is available on systems with the Data Protector User Interface component installed.

`omnimm`

Provides media management for Data Protector.

This command is available on systems with the Data Protector User Interface component installed.

`omnimnt`

Responds to a Data Protector mount request for a medium.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnimver`

Verifies data on a medium.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniobjconsolidate`

Consolidates Data Protector backup objects into synthetic full backups.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniobjcopy`

Creates additional copies of objects backed up with Data Protector on a different media set.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniobjverify`

Verifies Data Protector backup objects, either interactively or using pre-configured post-backup, or scheduled verification specifications.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnir`

Restores filesystems, disk images, the Data Protector database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Portal Server (SPS), SAP R/3, SAP DB/MaxDB, Informix Server, VMware Virtual Infrastructure (VMware), Lotus, IBM DB2 UDB, NetWare objects, and NDMP objects backed up with Data Protector. The command is also used to start the instant recovery process. To restore a Sybase database, refer to the `syb_tool` man page.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnirpt`

Generates various reports about the Data Protector environment, for example, about backup, object copy, object consolidation, and object verification sessions in a specific time frame, session specifications, media, Data Protector configuration, and single sessions.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnistat`

Displays the status of active Data Protector backup and restore sessions.

This command is available on systems with the Data Protector `User Interface` component installed.

`omniupload`

Uploads information about a backup device from an ASCII file to the Data Protector internal database (IDB).

This command is available on systems with the Data Protector `User Interface` component installed.

`omniusers`

Adds or removes Data Protector users to or from an existing Data Protector user group, or lists the configured Data Protector users. It enables you to use all GUI functionality on a Cell Manager platform on which the GUI is not available, using a GUI installed on another system.

This command is available on systems with the Data Protector `User Interface` component installed.

`syb_tool`

A utility used to get ISQL command needed to restore a Sybase database that was backed up by Data Protector.

This command is available on systems with the Data Protector `Sybase Integration` component installed.

ADMINISTRATIVE COMMANDS (1M):

`ob2install`

Runs remote client installation, uninstallation, upgrade, or check of a client from the selected Installation Server.

This command is available on the Data Protector Installation Server.

`omnicheck`

Performs a DNS connections check within a Data Protector cell and lists Data Protector patches installed on Data Protector clients.

This command is available on systems with any Data Protector component installed.

`omnidbcheck`

Checks the consistency of the Data Protector internal database (IDB).

This command is available on the Data Protector Cell Manager.

`omnidbinit`

Initializes the Data Protector internal database (IDB).

This command is available on the Data Protector Cell Manager.

`omnidbrestore`

Restores the Data Protector internal database (IDB).

This command is available on the Data Protector Cell Manager.

`omnidbupgrade`

Converts filenames in the IDB to the new internal character encoding used in Data Protector A.06.11 and thus enables the correct handling of non-ASCII characters in filenames in the Data Protector GUI.

This command is available on the Data Protector Cell Manager.

`omnidbutil`

Handles various Data Protector internal database (IDB) maintenance tasks.

This command is available on the Data Protector Cell Manager.

`omnidlc`

Gathers or deletes Data Protector debug, log, and getinfo files from the Data Protector cell or from a MoM environment.

This command is available on the Data Protector Cell Manager.

`omnidr`

A general purpose Data Protector disaster recovery command. Based on its input, it decides on what type of restore to perform (online restore using `omnir` or offline restore using `omniofflr`), as well as how to perform the restore (whether or not to use live OS features).

This command is available on systems with the Data Protector `User Interface` component installed.

`omnihealthcheck`

Checks the status of Data Protector services, the consistency of the Data Protector internal database (IDB), and if at least one backup of the IDB exists.

This command is available on the Data Protector Cell Manager.

`omniinetpasswd`

Manages the local Data Protector Inet configuration on Windows systems where the Inet process must be run under a specific user account, and sets a user account to be used by the Installation Server during remote installation.

This command is available on systems with any Data Protector component installed.

`omniinstlic`

Starts the HP AutoPass utility or synchronizes the Data Protector licenses between Data Protector and HP AutoPass.

This command is available on the Data Protector Cell Manager.

`omniintconfig.pl`

Configures, updates configuration parameters, and checks the configuration of one or multiple Oracle databases.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnikeymigrate`

Helps you migrate your existing keystore file from Data Protector A.06.00 client system and imports it into the central keystore file on the Data Protector A.06.11 Cell Manager.

This command is available on the Data Protector Cell Manager.

`omnikeytool`

Manages keys used for encryption.

This command is available on the Data Protector Cell Manager.

`omnimigrate.pl`

Helps you migrate your existing Cell Manager from a PA-RISC architecture based HP-UX 11.x system to an HP-UX 11.23 system for the Intel Itanium 2 (IA-64) architecture.

This command is available on the Data Protector Cell Manager.

`omniofflr`

Enables restore of any type of Data Protector backup object in the absence of a working Data Protector internal database (IDB).

This command is available on systems with the Data Protector `User Interface` component installed.

`omniresolve`

Resolves a filesystem object or a list of filesystem objects and writes the results to the standard output or to a Unicode file.

This command is available on systems with any Data Protector integration component installed.

`omnirsh`

Returns the hostnames of the physical and virtual nodes for the specified cluster hostname, or returns the cell information stored in the `cell_info` file on the specified cluster.

This command is available on the Data Protector Cell Manager.

`omnisetup.sh`

Installs or upgrades a Data Protector UNIX Cell Manager, Installation Server, or client system locally.

This command is available on the Data Protector installation DVD-ROMs for UNIX systems.

`omnisrdupdate`

Updates the System Recovery Data (SRD) file.

This command is available on systems with the Data Protector `User Interface` component installed.

`omnisv`

Starts, stops, or displays the status of Data Protector daemons (HP-UX, Solaris, or Linux systems) or services (Windows systems).

This command is available on the Data Protector Cell Manager.

`omnitrig`

Triggers Data Protector scheduled backups.

This command is available on the Data Protector Cell Manager.

`sanconf`

Auto-configures a library, modifies an existing library or drive configuration, or removes drives from a library configuration, within a SAN environment.

This command is available on systems with the Data Protector `User Interface` component installed.

`upgrade_cm_from_evaa`

Upgrades the EVADB entries created by the HP StorageWorks EVA Agent (legacy) to the SMISDB entries created by the HP StorageWorks EVA SMI-S Agent.

This command is available on the Data Protector Cell Manager.

`util_cmd`

Sets, retrieves or lists the parameters stored in the Data Protector Oracle, SAP R/3, VMware Virtual Infrastructure (VMware), Informix, and Sybase configuration files.

This command is available on systems with any Data Protector component installed.

`util_oracle8.pl`

Configures an Oracle database and prepares the environment for backup, and checks the configuration of an Oracle database.

This command is available on systems with the Data Protector `Oracle Integration` component installed.

`util_vmware.exe`

Configures a VMware datacenter, checks the configuration of a VMware datacenter, and lists all configured VMware datacenters.

This command is available on systems with the Data Protector `VMware Integration` component installed.

`winomnimigrate.pl`

Helps you migrate your existing Cell Manager from a 32-bit Windows system to a 64-bit Windows system, or from a 64-bit Windows system to 64-bit Windows Server 2008.

This command is available on the Data Protector Cell Manager.

COMMAND-LINE UTILITIES (1M):

`cjutil`

Starts, stops, and queries the Windows Change Journal.

This command is available on systems with the Data Protector Disk Agent component installed.

`NNMpost.ovpl`

A script with no arguments that resumes the eight processes paused by `NNMpre.ovpl`.

This command is available on systems with the Data Protector HP Network Node Manager Integration component installed.

`NNMpre.ovpl`

Starts NNM embedded database backup.

This command is available on systems with the Data Protector HP Network Node Manager Integration component installed.

`NNMScript.exe`

Finds the location of the NNM Perl compiler and the `NNMpre.ovpl` and `NNMpost.ovpl` scripts and starts the two scripts.

This command is available on systems with the Data Protector HP Network Node Manager Integration component installed.

`omnicjutil`

Remotely controls and administers the Windows Change Journal on Windows clients.

This command is available on the Data Protector Cell Manager.

`omnistoreapputil`

Acts as a user interface to Storage Appliances, such as VLS.

This command is available on the Data Protector Cell Manager.

`uma`

Controls the robotics of SCSI compliant autochangers.

This command is available on systems with the Data Protector General Media Agent or NDMP Media Agent component installed.

RETURN VALUES:

Possible return values of commands are:

- 1 Program failed, command syntax error.
- 2 Program failed, invalid argument.
- 3 Program failed, internal error.
- 4 Program failed, reason unknown.

Some commands may return additional error messages. These are described in individual reference pages.

The *winomnigrate.pl* command returns a different set of errors. See the *winomnigrate.pl(1m)* reference page.

GRAPHICAL USER INTERFACE COMMANDS ON WINDOWS

`manager`

Starts the Data Protector GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector `User Interface` component installed.

`javadpgui`

Starts the Data Protector Java GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector `Java GUI Client` component installed.

`mom`

Starts the Data Protector Manager-of-Managers GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector `Manager-of-Managers User Interface` component installed.

`javadpguimom`

Starts the Data Protector Manager-of-Managers Java GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector Java GUI Client component installed.

GRAPHICAL USER INTERFACE COMMANDS ON UNIX

`xomni`

Starts the Data Protector Java GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector Java GUI Client component installed.

`xomnimom`

Starts the Data Protector Manager-of-Managers Java GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

This command is available on systems with the Data Protector Java GUI Client component installed.

DIRECTORY STRUCTURE ON UNIX CELL MANAGER

`/opt/omni`

- Data Protector home directory

`/etc/opt/omni/server`

- Directory containing the following configuration directories:

`datalists`

backup specifications

`barlists`

database backup specifications

`devices`

templates for devices

```

users
    user configuration
cell
    cell configuration
schedules
    backup schedules
barschedules
    database backup specification schedules
sessions
    data about sessions
options
    default options
sg
    scripts for Service Guard support
snmp
    OpenView/SNMP trap sending configuration
/etc/opt/omni/client
• Directory containing the client configuration directories and files
/etc/opt/omni/server/dr
• Directory containing the following disaster recovery directories:

pls      PIS files for Enhanced Automated Disaster Recovery

srd      SRD files

asr      ASR archive file

/opt/omni
• Directory containing the following executables directories:
bin
    user Data Protector commands
lbin
    Disk Agent and Media Agent files and some administrative commands
sbin

```

Cell Manager and Data Protector Internal Database (IDB) administrative commands

`/var/opt/omni`

- Directory containing the following directories:
 - `/var/opt/omni/log` and `/var/opt/omni/server/log`
log files
 - `/var/opt/omni/tmp`
temporary files
 - `/var/opt/omni/server/sessions`
data about sessions
 - `/var/opt/omni/server/export/keys` and
`/var/opt/omni/server/import/keys`
encryption keys

`/var/opt/omni/server/db40`

- Directory containing the following Data Protector Internal Database (IDB) directories:
 - `/var/opt/omni/server/db40/datafiles`
the IDB tablespaces
 - `/var/opt/omni/server/db40/dcbf`
the IDB Detail Catalog binary files (DCBF)
 - `/var/opt/omni/server/db40/smisdb`
the ZDB database (SMISDB)
 - `/var/opt/omni/server/db40/logfiles`
the IDB transaction logs and the obdrindex.dat file
 - `/var/opt/omni/server/db40/meta`
the Serverless Integrations Binary Files (SIBF) part of the IDB
 - `/var/opt/omni/server/db40/msg`
the Data Protector session messages
 - `/var/opt/omni/server/db40/keystore`
the encryption keystore database
 - `/var/opt/omni/server/db40/keystore/catalog`
the key ID catalogue
 - `/var/opt/omni/server/db40/vadb`
the ZDB database (VADB)

`/var/opt/omni/server/db40/xpdb`

the ZDB database (XPDB)

`/opt/omni/lib`

- Directory containing the following directories:

`/opt/omni/lib/nls`

message catalogs

`/opt/omni/lib/man`

Data Protector man pages

`/opt/omni/help/C`

- The Data Protector help subsystem

`/opt/omni/java`

- Directory containing the following directories:

`/opt/omni/java/server/bin`

Java GUI Server (UIProxy service) executables

`/opt/omni/java/client/bin`

Java GUI Client executables

DIRECTORY STRUCTURE ON WINDOWS CELL MANAGER

Windows Server 2008

Data_Protector_home

- Data Protector home directory

Data_Protector_program_data

- Data Protector program data directory

Data_Protector_program_data\Config\Server

- Directory containing the following configuration directories:

datalists

backup specifications

barlists

database backup specifications

devices

templates for devices

- users
 - the user configuration
- cell
 - the cell configuration
- schedules
 - backup schedules
- barschedules
 - database backup specification schedules
- options
 - default options
- sessions
 - data about sessions
- snmp
 - OpenView/SNMP trap sending configuration

Data_Protector_program_data\Config\client

- Directory containing the client configuration directories and files

Data_Protector_program_data\Config\Server\export\keys and
Data_Protector_program_data\Config\Server\import\keys

- Directories containing encryption keys

Data_Protector_home\bin

- Directory containing Data Protector commands, Disk Agent, Media Agent files, message catalogs, and commands for Cell Manager maintenance

Data_Protector_program_data\log and
Data_Protector_program_data\log\server

- Log files

Data_Protector_program_data\tmp

- Temporary and debug log files

Data_Protector_program_data\db40

- The Data Protector Internal Database (IDB)

Data_Protector_program_data\db40\datafiles

- The IDB tablespaces

Data_Protector_program_data\db40\dcbf

- The IDB Detail Catalog binary files (DCBF)

Data_Protector_program_data\db40\logfiles

- The IDB transaction logs and the obdrindex.dat file

Data_Protector_program_data\db40\meta

- The Serverless Integrations Binary Files (SIBF) part of the IDB

Data_Protector_program_data\db40\msg

- The Data Protector session messages

Data_Protector_program_data\db40\keystore

- The encryption keystore database

Data_Protector_program_data\db40\keystore\catalog

- The keyid catalogue

Data_Protector_home\java\server\bin

- The Java GUI Server (UIProxy service) executables

Data_Protector_home\java\client\bin

- The Java GUI Client executables

Data_Protector_home\help

- The Data Protector help subsystem

Data_Protector_home\docs

- *HP Data Protector command line interface reference*

Other Windows operating systems

Data_Protector_home

- Data Protector home directory

Data_Protector_home\Config\Server

- Directory containing the following configuration directories:

datalists

backup specifications

barlists

database backup specifications

devices

templates for devices

users

the user configuration

cell

- the cell configuration
- schedules
 - backup schedules
- barschedules
 - database backup specification schedules
- options
 - default options
- sessions
 - data about sessions
- snmp
 - OpenView/SNMP trap sending configuration
- Data_Protector_home\Config\client*
 - Directory containing the client configuration directories and files
- Data_Protector_home\Config\Server\dr*
 - Directory containing the following disaster recovery directories:
 - pls*
 - PIS files for Enhanced Automated Disaster Recovery
 - srd*
 - SRD files
 - asr*
 - ASR archive files
- Data_Protector_home\Config\Server\export\keys* and *Data_Protector_home\Config\Server\import\keys*
 - Directories containing encryption keys
- Data_Protector_home\bin*
 - Directory containing Data Protector commands, Disk Agent, Media Agent files, message catalogs, and commands for Cell Manager maintenance
- Data_Protector_home\log* and *Data_Protector_home\log\server*
 - Log files
- Data_Protector_home\tmp*
 - Temporary and debug log files
- Data_Protector_home\db40*
 - The Data Protector Internal Database (IDB)

Data_Protector_home\db40\datafiles

- The IDB tablespaces

Data_Protector_home\db40\dcbf

- The IDB Detail Catalog binary files (DCBF)

Data_Protector_home\db40\logfiles

- The IDB transaction logs and the obdrindex.dat file

Data_Protector_home\db40\meta

- The Serverless Integrations Binary Files (SIBF) part of the IDB

Data_Protector_home\db40\msg

- The Data Protector session messages

Data_Protector_home\db40\keystore

- The encryption keystore database

Data_Protector_home\db40\keystore\catalog

- The keyid catalogue

Data_Protector_home\db40\smisdb

- The ZDB database (SMISDB)

Data_Protector_home\db40\vadb

- The ZDB database (VADB)

Data_Protector_home\db40\xpdb

- The ZDB database (XPDB)

Data_Protector_home\db40\vssdb

- The VSS database (VSSDB)

Data_Protector_home\java\server\bin

- The Java GUI Server (UIProxy service) executables

Data_Protector_home\java\client\bin

- The Java GUI Client executables

Data_Protector_home\help

- The Data Protector help subsystem

Data_Protector_home\docs

- *HP Data Protector command line interface reference*

SEE ALSO

ob2install(1M), omniabort(1), omniamo(1), omnib(1), omnicc(1), omnicellinfo(1), omnicheck(1M), omniclus(1), omnicreatedl(1), omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbsmis(1), omnidbva(1), omnidbvss(1), omnidbvp(1), omnidlc(1M), omnidownload(1), omnidr(1M), omnigui(5), omnihealthcheck(1M), omniinetpasswd(1M), omniinstlic(1M), omniiso(1), omnikeymigrate(1M), omnikeytool(1M), omnimcopy(1), omniminit(1), omnimigrate.pl(1M), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniobjcopy(1), omniobjconsolidate(1), omniofflr(1M), omnidbupgrade(1M), omnidbrestore(1M), omnidbutil(1M), omnir(1), omniresolve(1M), omnirpt(1), omnirsh(1M), omnisetup.sh(1M), omnisrdupdate(1M), omnistat(1), omnisiv(1M), omnitrig(1M), omniupload(1), omniusers(1), sanconf(1M), syb_tool(1), uma(1M), upgrade_cm_from_evaa(1M), util_cmd(1M), util_oracle8.pl(1M), winomnimigrate.pl(1M), NNMpre.ovpl(1M), NNMpost.ovpl(1M), NNMScript.exe(1M), cjutil(1M), omnicjutil(1M)

Section 1: User Commands

omniabort

aborts an active session
(this command is available on systems with the Data Protector User Interface component installed)

omniabort

SYNOPSIS

```
omniabort -version | -help  
omniabort -session SessionID
```

DESCRIPTION

This command aborts an active session, identifying it by the *SessionID*. A list of all active sessions and their session IDs is available using the `omnistat` command.

OPTIONS

`-version`
Displays the version of the `omniabort` command.

`-help`
Displays the usage synopsis for the `omniabort` command.

`-session SessionID`
Specifies the *SessionID* of the session to be aborted. Use the `omnistat` command to get the *SessionID* of the session.

NOTE

When using this command to abort the check for unrequired incrementals, manually terminate the `omniabort` utility afterwards.

EXAMPLES

To abort a session with the `SessionID` "R-2008/08/13-12" use:

```
omniabort -session R-2008/08/13-12  
omniabort -sess 12
```

SEE ALSO

`omnistat(1)`

omniamo

starts an automated media operation session
(this command is available on the Data Protector Cell Manager)

omniamo

SYNOPSIS

```
omniamo -version | -help  
omniamo -amc ConfigurationName {-post_backup | -scheduled}
```

DESCRIPTION

This command starts an automated media operation session for the specified post-backup or scheduled configuration. Before starting a post-backup operation, you must export the session ID of the backup session that used the media you want to copy.

On Windows: `set SESSIONID=SessionID`

On UNIX: `export SESSIONID=SessionID`

Use this command if you want to immediately start an automated media operation. Also, if an automated media operation has failed, you can use this command to start the operation again.

OPTIONS

`-version`

Displays the version of the `omniamo` command.

`-help`

Displays the usage synopsis for the `omniamo` command.

`-amc ConfigurationName {-post_backup | -scheduled}`

Starts the post-backup or scheduled automated media copy operation with the specified name.

EXAMPLES

1. To start the scheduled automated media copy operation with the configuration name "MediaCopy1", run:

```
omniamo -amc MediaCopy1 -scheduled
```

2. To start the post-backup automated media copy operation with the configuration name "MyFiles" and session ID 2008/09/13-0001 on Windows, run:

```
set SESSIONID=2008/09/13-0001  
omniamo -amc MyFiles -post_backup
```

3. To start the post-backup automated media copy operation with the configuration name "MyDocs" and session ID 2008/09/13-0002 on UNIX, if you are using an sh-like shell, run:

```
SESSIONID=2008/09/13-0002  
export SESSIONID  
omniamo -amc MyDocs -post_backup
```

4. To start the post-backup automated media copy operation with the configuration name "MyBackup" and session ID 2008/09/13-0003 on UNIX, if you are using a csh-like shell, run:

```
export SESSIONID=2008/09/13-0003  
omniamo -amc MyBackup -post_backup
```

SEE ALSO

omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1), omnimm(1), omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnib

backs up filesystems, disk images, the Data Protector internal database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Portal Server (SPS), SAP R/3, SAP DB/MaxDB, Oracle, Informix Server, VMware Virtual Infrastructure (VMware), Sybase, Lotus, IBM DB2 UDB, NetWare objects, and NDMP objects. This is the only command supported with the MPE/iX integration.

(this command is available on systems with the Data Protector User Interface component installed)

omnib

SYNOPSIS

```
omnib -version | -help
omnib -filesystem Client:MountPoint Label -device BackupDevice
[MIRROR_OPTIONS [MIRROR_OPTIONS...]] [GENERAL_OPTIONS] [FILESYSTEM_OPTIONS] [-public]
omnib -filesystem Client:MountPoint Label -device BackupDevice
-ndmp Type [NDMP_OPTIONS] [-public]
omnib -winfs Client:MountPoint Label -device BackupDevice [MIRROR_OPTIONS [MIRROR_OPTIONS...]] [GENERAL_OPTIONS] [FILESYSTEM_OPTIONS] [WINFS_OPTIONS] [-public]
omnib -NetWare Client:MountPoint Label -device BackupDevice [MIRROR_OPTIONS [MIRROR_OPTIONS...]] [NETWARE_OPTIONS] [GENERAL_OPTIONS] [FILESYSTEM_OPTIONS] [-public]
omnib -host Client:/ Label -device BackupDevice [MIRROR_OPTIONS [MIRROR_OPTIONS...]] [GENERAL_OPTIONS] [FILESYSTEM_OPTIONS] [-public]
omnib -rawdisk Client Label SectionList -device BackupDevice [MIRROR_OPTIONS [MIRROR_OPTIONS...]] [GENERAL_OPTIONS] [-public]
omnib -omnidb Client:MountPoint Label -device BackupDevice [MIRROR_OPTIONS [MIRROR_OPTIONS...]] [GENERAL_OPTIONS]
omnib -datalist Name [BACKUP_SPECIFICATION_OPTIONS]
omnib -sap_list ListName [-barmode SapMode] [LIST_OPTIONS]
omnib -sapdb_list ListName [-barmode SapdbMode] [LIST_OPTIONS]
omnib -oracle8_list ListName [-barmode Oracle8Mode] [LIST_OPTIONS]
omnib -vmware_list ListName [-barmode VMwareMode] [LIST_OPTIONS]
omnib -sybase_list ListName [-barmode SybaseMode] [LIST_OPTIONS]
omnib -informix_list ListName [-barmode InformixMode] [LIST_OPTIONS]
omnib -mssql_list ListName [-barmode MSSQLMode] [LIST_OPTIONS]
omnib -mssps_list ListName [-barmode MSSPSMode] [LIST_OPTIONS]
```

```
omnib -msese_list ListName [-barmode MSEExchangeMode] [LIST_OPTIONS]  
omnib -mbx_list ListName [-barmode MSMailboxMode] [LIST_OPTIONS]  
omnib -lotus_list ListName [-barmode LotusMode] [LIST_OPTIONS]  
omnib -msvssw_list ListName [-barmode VSSMode] [LIST_OPTIONS]  
omnib -db2_list ListName [-barmode DB2Mode] [LIST_OPTIONS]  
omnib -restart SessionID  
omnib -resume SessionID [-no_monitor]
```

MIRROR_OPTIONS

```
-mirror BackupDevice [ -pool MediaPool -prealloc MediaList ]
```

GENERAL_OPTIONS

```
-preview  
-pool MediaPool  
-prealloc MediaList  
-protect {none | weeks n | days n | until Date | permanent}  
-report {warning | minor | major | critical}  
-pre_exec Pathname  
-post_exec Pathname  
-compress  
-encode [aes256]  
-load {low | medium | high}  
-crc  
-no_monitor  
-keepcatalog {weeks n | days n | until Date}  
-variable VariableNameVariableValue
```

FILESYSTEM_OPTIONS

```
-trees TreeList  
-only MatchPattern  
-exclude TreeList  
-skip MatchPattern  
-lock  
-touch  
-[no_]log | -log_dirs | - log_file  
-mode {Full | Incremental[1-9]}  
-enh_incr [-clp]  
-[no_]hlink  
-size FromRange ToRange
```

WINFS_OPTIONS

-no_share[_info]
-[no_]nthlinks
-[no_]archatt
-vss [fallback]
-async

BACKUP_SPECIFICATION_OPTIONS

-select *SelectList*
-mode {Full | Incremental[1-9]}
-protect {none | weeks *n* | days *n* | until *Date* | permanent}
-preview
-disk_only
-load {low | medium | high}
-crc
-no_monitor

LIST_OPTIONS

-barcmd *Command*
-protect {none | weeks *n* | days *n* | until *Date* | permanent}
-load {low | medium | high}
-crc
-no_monitor
-test_bar
-disk_only

NETWARE_OPTIONS

-[no_]NWuncompress

NDMP_OPTIONS

-ndmp_user *UserName*
-ndmp_passwd *Password*
-ndmp_env *FileName*
-[no_]log -log_dirs -log_file
-mode {full | incremental1}
-pool *MediaPool*
-prealloc *MediaList*
-protect {none | weeks *n* | days *n* | until *Date* | permanent}
-report {warning | minor | major | critical}
-variable *VariableName* *VariableValue*

OTHER_OPTIONS

Type= Generic | NetApp | Celerra

```

SapMode= full | incremental
SapdbMode= full | diff | trans
Oracle8Mode= -full | -incr1 | ... | -incr4
VMwareMode= full | diff | incr
SybaseMode= full | trans
InformixMode= full | inf_incr1 | inf_incr2
MSSQLMode= full | diff | trans
MSSPSMode= full | diff | trans
MSExchangeMode= full | incr
MSMailboxMode= -full | -incr | -incr1
LotusMode= full | incr
VSSMode= full | copy | incr | diff
DB2Mode= -full | -incr | -delta
Date = [YY]YY/MM/DD (1969 < [YY]YY < 2038)

```

DESCRIPTION

The `omnib` command uses a backup specification (list of file or database objects) to back up data objects. The following Data Protector functionality is supported:

Session management

Controls the backup sessions. The Session Manager reads the backup specification or uses the command options to determine what to back up and how many copies of the backup objects to create (object mirroring), then initiates the Disk and Media Agents for disks and backup devices which will be used in the session. Once the session has completed, the Session Manager updates the MMDB with the session information.

Media management

Provides easy and efficient management of large sets of media by grouping media, tracking their status, implementing a media rotation policy, supporting the barcode recognition, vaulting the media, automating the library device operations, storing the media related information in a central place and sharing this information among several Data Protector cells.

Data compression

Writes data to media in a compressed format.

Data encryption

Writes data to media in an encrypted format using the Advanced Encryption Standard (AES) algorithm.

Backup monitoring

When the backup command is executed, it sends a request (specifying the backup objects) to the Session Manager. When the Session Manager (SM) accepts the request, it assigns a unique SessionID to the session. You can use this SessionID to monitor the progress of the session using the `xomnimonitor` or `omnistat` commands. You can also use the `omniabort` command to terminate a session.

OPTIONS

`-version`

Displays the version of the `omnib` command

`-help`

Displays the usage synopsis for the `omnib` command

`-filesystem Client:MountPoint Label`

Specifies the client, mount point and label of the filesystem to be backed up.

`-winfs Client:MountPoint Label`

Specifies the client, mount point and label of the Windows filesystem to be backed up.

`-NetWare Client:MountPoint Label`

Specifies the client, mount point and label of the NetWare filesystem to be backed up.

`-host Client:/ Label`

Specifies the client to be backed up as a set of filesystems defined at backup time. The label is used as a prefix for each of these filesystem labels. Client backup is useful for systems with filesystem configuration that often changes.

`-rawdisk Client Label SectionList`

Specifies the client, sections (pathnames of disk image sections) and label of the node to be backed up.

`-omnidb Client:MountPoint Label`

Specifies the client and label of the Data Protector internal database (IDB) to be backed up.

`-datalist Name`

Specifies the name of the backup specification file for the backup. The backup specification contains the data objects (filesystems and disk image sections) to be backed up.

`-restart SessionID`

Tries to restart a failed session, specified by its sessionID.

`-resume SessionID`

This option is applicable only for the Data Protector Oracle Server integration. It starts a new backup session using the same backup specification as used in the backup session *SessionID*. The main difference, compared to a standard backup session, is that, before the session is started, Data Protector modifies the RMAN script by adding the clause `NOT BACKED UP SINCE` *Original_session_start_time* for each backup command. Consequently, RMAN backs up only those backup sets that failed to be backed up in the original session.

`-sap_list ListName`

Specifies the name of the SAP R/3 backup specification file for the backup. The SAP R/3 backup specification contains the SAP R/3 objects to be backed up.

`-sapdb_list ListName`

Specifies the name of the SAP DB/MaxDB backup specification file for the backup. The SAP DB/MaxDB backup specification contains the SAP DB/MaxDB objects to be backed up.

`-oracle8_list ListName`

Specifies the name of the Oracle backup specification file for the backup. The Oracle backup specification contains the Oracle objects to be backed up.

`-vmware_list ListName`

Specifies the name of the VMware Virtual Infrastructure backup specification file for the backup. The backup specification contains the VMware Virtual Infrastructure objects to be backed up.

`-sybase_list ListName`

Specifies the name of the Sybase backup specification file for the backup. The Sybase backup specification contains the Sybase objects to be backed up.

`-informix_list ListName`

Specifies the name of the Informix Server backup specification file for the backup. The Informix Server backup specification contains the Informix Server objects to be backed up.

`-mssql_list ListName`

Specifies the name of the Microsoft SQL Server backup specification file for the backup. The Microsoft SQL Server backup specification contains the Microsoft SQL Server objects to be backed up.

`-mssps_list ListName`

Specifies the name of the Microsoft SharePoint Portal Server backup specification file for the backup. The Microsoft SharePoint Portal Server backup specification contains the Microsoft SharePoint Portal Server objects to be backed up.

`-msese_list ListName`

Specifies the name of the Microsoft Exchange Server backup specification file for the backup. The Microsoft Exchange Server backup specification contains the Microsoft Exchange Server objects to be backed up.

`-mbx_list ListName`

Specifies the name of the Microsoft Exchange Server single mailbox backup specification file for the backup. The Microsoft Exchange Server single mailbox backup specification contains single mailboxes to be backed up.

`-lotus_list ListName`

Specifies the name of the Lotus Notes/Domino Server backup specification file for the backup. The Lotus Notes/Domino Server backup specification contains the Lotus database objects to be backed up.

`-msvssw_list ListName`

Specifies the name of the Microsoft VSS backup specification file for the backup. The Microsoft VSS backup specification contains the Microsoft VSS objects to be backed up.

`-db2_list ListName`

Specifies the name of the IBM DB2 UDB backup specification file for the backup. The IBM DB2 UDB backup specification contains the IBM DB2 UDB objects to be backed up.

`-device BackupDevice`

Specifies the backup device to be used for the backup.

`-public`

If you use this option, you allow other users to see and restore your data. By default for filesystem backups, only the Data Protector administrator and the user who created a backup can see and restore the data.

MIRROR_OPTIONS

`-mirror BackupDevice`

Specifies one or several backup devices to be used for object mirroring. Different backup devices should be specified for the backup and for each mirror.

`-pool MediaPool`

Instructs the Session Manager to use an alternate media pool for object mirroring. By default, the default media pool for the backup device is used.

`-prealloc MediaList`

Specifies a list of media to be used for object mirroring. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt

is issued. Note: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

GENERAL_OPTIONS

-preview

Checks the backup objects, backup devices and options you selected, without performing the backup. The check includes: backup objects, status of the backup device, available media, and the approximate amount of data which will be backed up.

-pool MediaPool

Instructs the Session Manager to use an alternate media pool for the backup. By default, the default media pool for the backup device is used.

-prealloc MediaList

Specifies a list of media to be used for the backup. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt is issued. Note: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

*-protect{none | weeks *n* | days *n* | until *Date* | permanent}*

Sets the level of protection for the backup session. The media containing this backup session cannot be overwritten until the protection expires. By default, the protection is permanent.

-report{warning | minor | major | critical}

Sets the level of error notification for the session. Errors are classified (in ascending order) as: warning, minor, major and critical. When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if major is selected, only major and critical errors are reported. By default, all errors are reported.

-pre_exec Pathname

Instructs the Session Manager to execute this command before starting the backup session. The complete *Pathname* of the command should be specified. The command is executed on the Session Manager system.

-post_exec Pathname

Instructs the Session Manager to execute this command after the backup session. The complete *Pathname* of the command should be specified. The command is executed on the Session Manager system.

-compress

Instructs the General Media Agent to write data to media in the compressed format.

This option is not supported on Novell NetWare. However, it is possible to uncompress files that were compressed with this option using older versions of Data Protector.

`-encode [aes256]`

Instructs the General Disk Agent to write data to media in encoded format.

If the `aes256` option is specified, data is written to media in encrypted format, using the Advanced Encryption Standard (AES) algorithm.

`-load{low | medium | high}`

Specifies the level of network traffic generated by a session during a time period. High level generates as much traffic as allowed by the network, resulting in a faster backup. Low level has less impact on the network performance, but results in a slower backup. By default, this option is set to `high`.

`-crc`

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the `omniver` command.

`-no_monitor`

By default, the command monitors the session and displays the status of the session during the session. If this option is used, the SessionKey is displayed and the command is disconnected from the session.

`-keepcatalog{weeks n | days n | until Date}`

This option specifies file catalog retention time. If you do not want to save the file catalog at all, use the `-no_log` option. By default, this option is set to the same value as specified by the `protection` option.

`-variable VariableName VariableValue`

This option lets you specify a variable name and its value for proper operation of some platforms and integrations, for example, for backing up and restoring data on MPE/iX System. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

FILESYSTEM_OPTIONS

`-trees TreeList`

Specifies the trees to be included in the backup. If this option is not used, the filesystem is backed up from the mount point level downwards. When specifying several trees, separate each *Tree* with a space. *Tree* must start with a /. Note that when specifying trees on UNIX systems, the complete tree must be specified including the mountpoint, whereas on Windows systems, trees must be specified

without volumes (drives). For example: `-tree /usr/temp` (UNIX system) or `-tree \temp` (Windows system). This option is not supported with Data Protector NDMP server integration.

`-only MatchPattern`

Specifies that only files that match the *MatchPattern* will be backed up. This option is not supported with Data Protector NDMP server integration.

`-exclude TreeList`

Specifies trees not to be backed up. This option is not supported with Data Protector NDMP server integration.

`-skip MatchPattern`

Specifies that files matching the *MatchPattern* will not be backed up. This option is not supported with the Data Protector NDMP server integration.

`-lock`

Instructs the Disk Agent to lock each file before backing it up. If the file is in use (and cannot be locked), the session manager displays a warning that this file can not be locked and backs up the file anyway. This warning is also logged to the catalog database. By default, files are not locked at backup.

`-no_log`

Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log`

The default option. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the Data Protector internal database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

`-log_dirs`

If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log_file`

All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector internal database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape. It also does not take much space since some information on file details (file attributes) is not logged to the database.

`-mode{Full | Incremental[1-9]}`

Specifies the mode for the backup session. `Full` mode backs up all specified files. `Incremental[1-9]` backs up only a subset of the specified files, based on whether or not the files were modified since the last `Full` or lower-level `Incremental` backup. Default is the `Full` mode. The level of incremental backup is based on the level number which is specified. For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 or lower backup.

`-touch`

Whenever a file is opened, read, or locked, which happens during backup, the file's access time attribute changes. By default, after backup, Data Protector resets the file's access time attribute to the value it had before backup. However, on UNIX, this resetting of the access time attribute modifies the file's change time.

If the `-touch` option is specified, Data Protector does not reset access time attributes. Then, on UNIX, Data Protector can also use the file's change time (inode modification time) as an incremental backup criterion. As a result, files with a changed name, location, or attributes are backed up in an incremental backup.

This option is not supported on Novell NetWare.

`-no_hlink`

If this option is specified, then hardlink detection is disabled and hard links are backed up as normal files. This speeds up the first traversal of the filesystem.

`-enh_incr`

This option enables enhanced incremental backup. Unlike conventional incremental backup, enhanced incremental backup reliably detects and backs up files with changes in name, location, and attributes. It is also a prerequisite for subsequent object consolidation (synthetic backup).

NOTE: After you select this option, incremental backup will run in the enhanced mode only after a full backup is performed.

`-clp`

This option, used together with the `-enh_incr` option, enables enhanced incremental backups using the Windows NTFS Change Log Provider. A list of files to be backed up will be generated by querying the Change Journal rather than performing a file tree walk.

`-size FromRange ToRange`

Limits backup to those files only, of which sizes are in the specified range. The sizes are set in KB. If you set `ToRange` to 0, all files larger than `FromRange` will be backed up.

`WINFS_OPTIONS`

`-no_share[_info]`

If this option is specified, share information for directories on Windows systems is *not* backed up. By default, if a directory was shared on the network when a backup was run, the share information for directory is backed up, unless the `-no_share[_info]` option is specified.

Backing up share information for shared directories enables you to automatically share such directories after restore.

`-[no_]nthlinks`

If this option is specified then NTFS hardlink detection is disabled and NTFS hard links are backed up as normal files. This speeds up the first traversal of the filesystem.

`-[no_]archatt`

By default, Data Protector uses the archive attribute as an incremental backup criterion and also clears the file's archive attribute after the file is backed up. The archive attribute is automatically set by the system when the file's content, properties, name, or location changes.

If archive attributes cannot be cleared, an error is reported. This affects future incremental backups, so that the files are backed up, although they have not changed. This may happen when backing up removable media with write protection.

In the case of ZDB, archive attributes are cleared on the replica and this is not reflected on the source volume. As a result, in the next incremental ZDB session, when a new replica is created, the archive attributes appear again and the corresponding files are backed up although they may not have changed. To enhance the incremental ZDB behavior, specify the `-[no_]archatt` option.

If the `-[no_]archatt` option is specified, Data Protector ignores archive attributes and detects changed files using other criteria, such as the file's modification time.

`-vss [fallback]`

If the `-vss` option is specified, the VSS filesystem backup is performed. If the shadow copy creation on the system where the VSS filesystem backup is running, fails, the backup also fails by default. However, you can avoid backup failure by specifying the `fallback` option. In this case, the backup will continue as the normal filesystem backup.

`-async`

If this option is specified, Disk Agent performs asynchronous reading from the disk without using Windows cache manager. Concurrent reads of the same file are started simultaneously. If this option is not specified, synchronous reading from the disk is performed.

BACKUP_SPECIFICATION_OPTIONS

-select SelectList

Specifies which objects (of those in the backup specification) to back up. The *SelectList* is the list of objects to be backed up.

-mode{Full | Incremental[1-9]}

Specifies the Mode for the backup session. *Full* mode backs up all specified files. *Incremental[1-9]* backs up only a subset of the specified files, based on whether or not the files were modified since the last *Full* or lower-level *Incremental* backup. Default is the *Full* mode. The level of incremental backup is based on the level number which is specified. For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 (or lower) backup. Use incremental level 1 to back up files that were changed since last full backup only. The *Incremental* without level will back up the files that changed since the last backup only (regardless whether it was full or incremental of any level).

-preview

Checks the backup objects, backup devices and options you selected, without performing the backup. The check includes: objects due for backup, status of the backup device, available media, and approximate amount of data which will be backed up.

-disk_only

A ZDB related option. It instructs Data Protector to perform a ZDB-to-disk session rather than a ZDB-to-tape or ZDB-to-disk+tape session. With ZDB, if the option is not specified, a ZDB-to-tape or ZDB-to-disk+tape session is performed.

-crc

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the *omnimver* command.

-no_monitor

By default, the command monitors the session and displays the status of the session during the session. If this option is used only the SessionKey is displayed and the command is disconnected from the session.

LIST_OPTIONS

-barcmd Command

Specifies the command that will be used instead of the command specified with *exec* option in the backup specification. The command should reside in the */opt/omni/sbin* directory.

-barmode SapMode

For SAP R/3 objects, the possible modes are `full` and `incremental`. The default value for this option is `full`.

`-barmode SapdbMode`

For SAP DB/MaxDB objects, the possible modes are `full`, `diff` and `trans`. The `full` option triggers a full backup of the SAP DB/MaxDB instance, the `diff` option triggers a differential backup, and the `trans` option triggers an archive logs backup. The default value for this option is `full`.

`-barmode InformixMode`

For Informix Server objects you can specify the following modes:

`full`: full backup of dbspaces specified during the backup specification creation time,

`inf_incr1`: first incremental backup,

`inf_incr2`: second incremental backup.

The default value for this option is `full`.

`-barmode Oracle8Mode`

For Oracle objects you can specify `-full` for full backup or `-incr1` to `-incr4` for incremental backups.

`-barmode VMwareMode`

For VMware Virtual Infrastructure objects, the possible modes are `full`, `diff` and `incr`. The `full` option triggers a full backup, the `diff` option triggers a differential backup, and the `incr` option triggers an incremental backup. The default value for this option is `full`.

`-barmode SybaseMode`

For Sybase objects you can specify `full` for full database backup or `trans` for transaction backup. The default value for this option is `full`.

`-barmode MSSQLMode`

For Microsoft SQL Server objects you can specify `full` for full database backup, `diff` for differential database backup or `trans` for transaction log backup. The default value for this option is `full`.

`-barmode MSSPSMode`

For Microsoft SharePoint Portal Server objects you can specify the following modes:

`full`: full backup,

`diff`: differential database backup of Microsoft SQL Server databases and full backup of other Microsoft SharePoint Portal Server objects,

`trans`: transaction log backup of Microsoft SQL Server databases and full backup of other Microsoft SharePoint Portal Server objects.

The default value for this option is `full`.

`-barmode MSExchangeMode`

For Microsoft Exchange Server objects you can specify `full` for full database and log files backup or `incr` for incremental backup of log files. The default value for this option is `full`.

`-barmode MSMailboxMode`

For Microsoft Exchange Server single mailboxes, you can specify `-full` for a full mailbox backup, `-incr` for an incremental mailbox backup, or `-incr1` for an incremental1 mailbox backup. The default value for this option is `-full`.

`-barmode LotusMode`

For Lotus Notes/Domino Server objects you can specify `full` for full database backup or `incr` for a full backup of selected Lotus Notes/Domino objects, if the amount of data changed from the last backup is bigger than specified by the `-need_bck` barlist option. In case that transaction logging is enabled, the full backup of all archived transaction logs is also performed. The default value for this option is `full`.

`-barmode VSSMode`

The available backup modes for VSS Writer objects depend on the writer: some writers support several modes (for example `full`, `copy`, `incr`, `diff` with Microsoft Exchange Server 2003 writer), others may support only `full`. See the *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*.

`-barmode DB2Mode`

For IBM DB2 UDB objects you can specify `-full` for full database backup, `-incr` for incremental database backup or `-delta` for delta database backup. The default value for this option is `-full`.

`-crc`

Instructs the General Media Agent to write a CRC checksum at the end of every block on the medium. If this option is used, you can later verify the CRC checksum on the medium by using the `omnimver` command.

`-no_monitor`

By default, the command monitors the session and displays the status of the session during the session. If this option is used, only the SessionKey is displayed, and the command is disconnected from the session.

`-test_bar`

Enables preview mode for integrations. This option is supported only for Oracle, SAP R/3, SAP DB/MaxDB, Microsoft Exchange Server single mailbox, Lotus Notes/Domino Server, DB2, Informix Server and Sybase. ZDB is not supported.

The option checks the backup objects, backup devices and options you selected, without doing the backup. The check includes: objects due for backup, status of the backup device, available media, and the approximate amount of data which will be backed up.

`-disk_only`

A ZDB related option. It instructs Data Protector to perform a ZDB-to-disk session rather than a ZDB-to-tape or ZDB-to-disk+tape session. With ZDB, if the option is not specified, a ZDB-to-tape or ZDB-to-disk+tape session is performed.

NETWARE_OPTION

`-NWuncompress`

By default, Data Protector backs up Novell NetWare compressed files in their compressed format. Though this approach speeds up the backup process, it makes it impossible to restore the Novell NetWare compressed files to a non-compressed Novell NetWare volume. When this option is set to `NWuncompress`, Novell NetWare compressed files are uncompressed before being backed up. Files backed up in this form can be restored to non-compressed Novell NetWare volume.

NDMP_OPTIONS

`-ndmp_user UserName`

Sets the username that is used by Data Protector to establish the connection to the NDMP server.

`-ndmp_passwd Password`

Sets the password for the username that is used by Data Protector to establish the connection to the NDMP server.

`-ndmp_env FileName`

Specifies the filename of file with NDMP environment variables for specific NDMP implementations.

`-no_log`

Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log`

The default option. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the Data Protector internal database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

`-log_dirs`

If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log_file`

All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector internal database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape. It also does not take much space since some information on file details (file attributes) is not logged to the database.

`-mode{Full| Incremental[1-9]}`

Specifies the mode for the backup session. Full mode backs up all specified files. `Incremental[1-9]` backs up only a subset of the specified files, based on whether or not the files were modified since the last `Full` or lower-level `Incremental` backup. Default is the `Full` mode. The level of incremental backup is based on the level number which is specified. For example, an incremental level 3 backs up only those files (of the specified files) which were modified since the last incremental level 2 or lower backup.

`-pool MediaPool`

Instructs the Session Manager to use an alternate media pool for the backup. By default, the default media pool for the backup device is used.

`-prealloc MediaList`

Specifies a list of media to be used for the backup. If the Media Allocation policy for the pool is set to "strict", the media in the Prealloc list are used in the sequence shown in the list. If one of these media is unavailable, a mount prompt is issued. Note: If the Media Allocation Policy is "strict", you must specify a Prealloc list.

`-protect{none | weeks n | days n | until Date | permanent}`

Sets the level of error notification for the session. Errors are classified (in ascending order) as: `warning`, `minor`, `major` and `critical`. When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if `major` is selected, only `major` and `critical` errors are reported. By default, all errors are reported.

`-variable VariableName VariableValue`

This option lets you specify a variable name and its value for proper operation of some platforms and integrations, for example, for backing up and restoring data on MPE/iX System. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omnib` command are:

- | | |
|----|--|
| 10 | There was an error while backing up some files. All agents completed successfully. |
| 11 | One or more agents failed, or there was a database error. |
| 12 | None of the agents completed the operation; session was aborted by Data Protector. |
| 13 | Session was aborted by user. |

EXAMPLES

The following examples illustrate how the `omnib` command works:

1. To do a backup of a tree `/usr` of filesystem `senna` with the label `work`, using the compress option, to the backup device `DAT`, run:

```
omnib -device DAT -filesystem senna:/ work -tree /usr -compress
```
2. To back up the Data Protector internal database (IDB) on the client `geronimo` with the label `newDB` to the backup device `ADIC3` and to create two mirrors of this backup to the backup devices `LTO1` and `LTO2`, run:

```
omnib -omnidb geronimo:/ newDB -device ADIC3 -mirror LTO1 -mirror LTO2
```
3. To perform an incremental backup using the backup specification `OMNIGROUP`, run:

```
omnib -datalist OMNIGROUP -mode Incremental
```
4. To preview a backup of the tree `/Amt3` of the filesystem `Munich`, skipping the files with the `.fin` extension, run:

```
omnib -preview -filesystem Munich:/ -tree /Amt3 -skip "*.fin"
```
5. To run a disk image backup of the section `/dev/rdisk/c201d1s0` on the client `xanadu` to the backup device `Exa` and protecting the session against overwrite for 4 weeks:

```
omnib -rawdisk xanadu section /dev/rdisk/c201d1s0 -dev Exa  
-protect weeks 4
```

6. To run a full Lotus backup using the "test2" backup specification with the high network load and permanent protection set:

```
omnib -lotus_list test2 -barmode full -protect permanent  
-load high
```

7. To start a full backup using an existing IBM DB2 UDB backup specification called "TEST", and to set data protection to 10 weeks, run:

```
omnib -db2_list TEST -barmode -full -protect weeks 10
```

8. To start a differential backup using an existing SAP DB/MaxDB backup specification called "test", and write a CRC checksum at the end of every block on the medium, run:

```
omnib -sapdb_list test -barmode diff -crc
```

9. To perform an encrypted backup of a tree "/usr" of filesystem "alpha.hp.com" with the label "work", using the encode aes256 option, to the backup device "ENC1", run:

```
omnib -filesystem alpha.hp.com:/work -device ENC1 -tree  
/usr -encode aes256 -mode full
```

SEE ALSO

omnikeymigrate(1M), omnikeytool(1M), omniobjconsolidate(1), omniobjcopy(1), omniobjverify(1), omnir(1)

omnicc

handles the Data Protector licensing, reports the number of configured and available Data Protector licenses, installs the licenses, imports and exports Data Protector clients, and manages access to secured clients
(this command is available on systems with any Data Protector component installed)

omnicc

SYNOPSIS

```
omnicc -version | -help
omnicc -redistribute
omnicc -import_host ClientName [-virtual]
omnicc -import_vls ClientName -port Port -user UserName -passwd Password
omnicc -import_ndmp ClientName -type NdmpType -port Port -user UserName -passwd Password
omnicc -import_is ClientName
omnicc -export_is ClientName
omnicc -update_host ClientName
omnicc -update_all [-force_cs]
omnicc -export_host ClientName
omnicc -list_authorities ClientName
omnicc -secure_client ClientName -authorities ClientName1 [ClientName2]
omnicc -unsecure_client ClientName
omnicc -install_license password
omnicc -password_info
omnicc -confirm_mom_clients
omnicc -update_mom_server
omnicc -check_licenses [-detail]
omnicc [-query]
```

NdmpType

Generic | NetApp | Celerra

DESCRIPTION

The `omnicc` command is used for licensing, importing, and exporting clients, and for managing secured clients.

OPTIONS

`-version`

Displays the version of the `omnicc` command.

`-help`

Displays the usage synopsis for the `omnicc` command.

`-check_licenses [-detail]`

Reports licensing related information from the cell.

If the `-detail` option is not specified, the command returns information on whether the Data Protector licensing is covered or not.

If the `-detail` option is specified, a detailed report is produced. The following information is returned for every license, except for the Encryption Extension for one client system licence, in the cell: license name, licenses installed, licenses used, and licenses required.

In a MoM environment with the CMMDB configured, when producing a license report for the items that are subject to libraries and devices related licenses, such as media (including advanced file device media), backup devices, drives and slots, the `omnicc` command must be run on the Cell Manager with the CMMDB installed.

`-query`

Displays information about the number of available licenses.

`-redistribute`

Displays licensing information for multicell environments. The first part shows the number of allocated licenses and the second shows the number of licenses actually used per server.

`-import_host ClientName [-virtual]`

Imports the specified client into a cell. This allows you to move a client between two cells without reinstalling the Data Protector modules.

When you import the next one among multiple network names (clusters, service guards), use the `-virtual` option. This way you keep Data Protector from assigning licenses to all the network names of the same system.

`-import_is ClientName`

Imports an already installed Installation Server into the cell.

`-export_is ClientName`

Exports an already installed Installation Server from the cell.

`-import_vls ClientName`

Imports the specified VLS Device into the cell.

`-port Port`
 Sets the TCP/IP port number for the VLS Device.

`-user UserName`
 Sets the username that is used by Data Protector to establish the connection to the VLS Device.

`-passwd Password`
 Sets the password for the above specified username.

`-import_ndmp ClientName`
 Imports the specified NDMP server into the cell.

`-type Ndmptype`
 Sets the NDMP data format when importing an NDMP server into a cell.

`-port Port`
 Sets the TCP/IP port number of the NDMP server when importing an NDMP server into a cell.

`-user UserName`
 Sets the username that is used by Data Protector to establish the connection to the NDMP server when importing an NDMP server into a cell.

`-passwd Password`
 Sets the password for the username that is used by Data Protector to establish the connection to the NDMP server when importing an NDMP server into a cell.

`-update_host ClientName`
 Updates the version information and installed packages information in the Cell Manager configuration file for the specified client. Useful when automatic update fails due to any reason.

`-update_all [-force_cs]`
 Updates the version information and installed packages information in the Cell Manager configuration file for all clients in the cell. Useful when automatic update fails due to any reason.
 If the `-force_cs` option is specified, it checks if the clients belong to the current cell. If not, the command will change the cell to the current cell.

`-export_host ClientName`
 Exports the specified client from the cell. This enables you to remove a client from the cell without uninstalling its Data Protector modules.

`-list_authorities ClientName`
 Lists systems from which the specified client accepts requests on the Data Protector port (by default 5555).

`-secure_client ClientName`
 Specifies the client to be secured.

`-authorities ClientName [ClientName2...]`
 Specifies systems from which the specified client accepts requests on the Data Protector port (by default 5555). Consequently, other computers will not be able to access this client. For tasks like backup and restore, starting pre- or post-execution scripts, or importing and exporting clients, the client checks whether the computer which triggers one of these tasks via the Data Protector port is allowed to do so. This security mechanism instructs the client to accept such actions only from the systems specified by this option.

`-unsecure_client ClientName`
 Specifies the client from which you want to remove security. Such a client will enable access to all systems in the cell.

`-install_license password`
 Installs an encrypted Data Protector license. The password must be formatted as a single line and must not contain any embedded carriage returns. The password must be in quotes. If the password includes also a description in quotes, the quotes in this description must be preceded with backslashes.

`-confirm_mom_clients`
 Collects `cell_info` files from MoM clients
 (`Data_Protector_program_data\Config\Server\cell\mom_info` on Windows Server 2008 clients,
`Data_Protector_home\Config\Server\cell\mom_info` on other Windows clients, or `/etc/opt/omni/server/cell/mom_info` on UNIX clients) and stores them on the MoM Manager into the directory
`Data_Protector_program_data\Config\Server\mom\cell_info` (Windows Server 2008),
`Data_Protector_home\Config\Server\mom\cell_info` (other Windows systems), or `/etc/opt/omni/server/mom/cell_info` (UNIX systems) under client Cell Manager name. Use this command when switching MoM clients to CMMDB mode. `Omnicc` with this option specified has to be executed on the MoM Manager.

`-update_mom_server`
 Pushes `mom_info` file located in the directory
`Data_Protector_program_data\Config\Server\cell` (Windows Server 2008), `Data_Protector_home\Config\Server\cell` (other Windows systems), or `/etc/opt/omni/server/cell` (UNIX systems) to MoM and CMMDB server to MoM into the directory
`Data_Protector_program_data\Config\Server\mom\cell_info`

(Windows Server 2008),

Data_Protector_home\Config\Server\mom\cell_info (other Windows systems), or */etc/opt/omni/server/mom/cell_info* (UNIX systems) under client Cell Manager name. Use this command when switching to CMMDB mode.

Omnicc with this option specified has to be executed on the client Cell Manager.

`-password_info`

Displays information about installed license passwords.

EXAMPLE

The following example illustrates how the `omnicc` command works.

To install the zero downtime backup EVA 10TB license key "4TRV E9ES LW3U YST7 KQZ3 G5NK ABA7 MQDB "EVA 10TB"", where "EVA 10TB" is description, run:

```
omnicc -install_licence "4TRV E9ES LW3U YST7 KQZ3 G5NK ABA7  
MQDB \"EVA 10TB\""
```

Note that the whole command should be provided without a carriage return.

SEE ALSO

`omnicellinfo(1)`, `omnicheck(1M)`, `omnidlc(1M)`, `omniinstlic(1M)`, `omnisv(1M)`

omnicellinfo

displays configuration information about the Data Protector cell
(this command is available on systems with the Data Protector User Interface component installed)

omnicellinfo

SYNOPSIS

```
omnicellinfo -version | -help
omnicellinfo -servers
omnicellinfo -group
omnicellinfo -object [schedule | no_schedule] -group Group | -db
omnicellinfo {-mm | -dev} [-detail]
omnicellinfo {-dlinfo [-group Group]] | -cell [brief] {-schinfo
[Backup_Specification | -days NumberDays | -group Group]] | {-dlobj
[-group Group]] | {-trees [-group Group]] | -allbdf | -acl
```

DESCRIPTION

The `omnicellinfo` command displays information about data objects, media pools, devices, clients, database, backup specifications and backup specification groups in the cell. It can be also used to display the cell servers in multicell environments.

Some options recognized by `omnicellinfo` are intended primarily for generating reports by shell/awk/perl scripts. Information produced is formatted in records with a newline as field separator and a blank line as record separator. Those options are: `-dlinfo`, `-schinfo`, `-dlobj`, `-trees` and `-allbdf`.

OPTIONS

`-version`

Displays the version of the `omnicellinfo` command.

`-help`

Displays the usage synopsis for the `omnicellinfo` command.

`-servers`

Displays the list of cell servers that are included in the multicell environment.

`-group`

Displays the backup specification groups that contain backup specifications. Note that the backup specification group named `Default` is not displayed.

`-object[schedule | no_schedule]`

Displays information about objects (filesystems, databases and disk images) in the cell. The report shows: Object (object type, client name, and mountpoint), Label, and Next Scheduled Backup Date. When you use the `schedule` option, the report only shows those objects which are scheduled for backup. When you use the `-no_schedule` option, the report only shows those objects which are not scheduled for backup. By default, all objects (scheduled and unscheduled) are listed.

`-mm`

Displays information about the media and media pools in the cell. The report shows for each pool: the Pool Name, Media Class, Media Usage Policy, Media Allocation Policy, and Amount of Free Space in the pool.

`-dev`

Displays information about the backup devices in the cell. The report shows for each device: the Device Name, Client Name, Device Type and Media Pool.

`-db`

Displays information about the Data Protector internal database (IDB). The database is divided in logical structures, for each of these structures the report shows: Disk Space Used, Records Used and Records Total.

`-cell`

Displays information about the configured clients in the cell. The report shows for each client: client name, operating system, cell console version, Disk Agent version, Media Agent version, GUI version, and all installed Data Protector integrations versions. There is also a short summary which shows the total number of clients and, if the `brief` suboption was not specified, all possible Data Protector software components, together with the total number of every software component in the cell. If the `brief` suboption was specified, only the installed Data Protector software components together with the total number of every software component in the cell is listed.

`-detail`

The `-detail` option can be used in combination with the `-dev` and `-mm` options to produce a more detailed report.

`-dlinfo`

Shows information about backup specifications. For each backup specifications it lists the name of the backup specification, session owner, pre-exec and post-exec script. Session owner is in format `USER.GROUP@CLIENT`.

`-schinfo[Backup_Specification | -days NumberDays]`

Shows information about backup specification scheduling. If `Backup_Specification` and `-days` option are not specified, the command

displays the next schedule time for each backup specification. If backup specification is specified the command lists all schedules in the next year for the specified backup specification. Option `-days` can be used to display schedules of all backup specifications for a specified number of days.

`-dlobj`

Shows information about all objects in backup specifications. For each object it lists object type, object name (in format *ClientName:PathName*), description, and the name of the backup specification. After this, the device and poolname fields are listed for each device used in the backup specification making the size of the records variable.

`-trees`

Shows information about all defined trees in backup specifications. For each tree, it lists filesystem name (in format *ClientName:Pathname*), tree, description, backup device, media pool and name of the backup specification.

`-acl`

Displays all Data Protector access permissions that the user running the command has.

`-group Group`

This option allows you to limit the output of the command to single backup specification group. The following options support this: `-dlinfo`, `-schinfo`, `-dlobj`, `-trees` and `-object`.

EXAMPLES

The following examples illustrate how the `omnicellinfo` command works.

1. To list detailed information about the selected objects, run:
`omnicellinfo -object schedule`
2. To list detailed information about the configured devices, run:
`omnicellinfo -dev -detail`

SEE ALSO

`omnicc(1)`, `omnicheck(1M)`, `omnidlc(1M)`, `omniinstlic(1M)`, `omnisv(1M)`

omniclus

manages load balancing in a cluster environment in the event of an application (Data Protector or other) failover

(this command is available on systems with the Data Protector MS Cluster Support component installed (Windows systems) and on the Data Protector Cell Manager (UNIX systems))

omniclus

SYNOPSIS

```
omnir -version | -help
omniclus -clus cluster_name -session {* | backup_specification}
-abortsess [-abortid {== | !=}application_id]
omniclus -clus cluster_name -inhibit {* | 0 | minutes}
omniclus -clus cluster_name -session {* | backup_specification}
-symlink {split | active}
```

NOTE: On UNIX systems replace the *** wildcard with *'*'*

Under Windows, the *-noclus* option can be specified directly after *-clus* to prevent loading of the cluster dynamic library

DESCRIPTION

The *omniclus* command, that is common to all platforms (UNIX and Windows) allows the user to send the Data Protector Cell Manager special events that in some way control the behavior of the Cell Manager and the backup sessions in a cluster environment. *omniclus* allows balance loading by offering additional (CLI) control of the Cell Manager in the cluster environment:

- abort sessions
- temporarily disabling the Cell Manager for backups
- specify the state of EMC/Symmetrix links after an application failover

Note: that the *cluster_name* specified with the *-clus* switch must be a cluster-aware Data Protector Cell Manager.

OPTIONS

-version

Displays the version of the *omniclus* command

`-help`
 Displays the usage synopsis for the `omniclus` command.

`-clus cluster_name`
 Specifies the cluster-aware Cell Manager.

`-session* | backup_specification`
 Specifies the session(s) to which the abort message should be sent.

`-abortsess`
 Specifies the abort session command.

`-abortid{== | !=} application_id`
 Specifies the application identification.

`-inhibit{* | 0 | minutes}`
 Specifies the number of minutes for Cell Manager backup inactivity, where `*` means forever and `0` means activate now.

`-symlink{active | split}`
 Specifies the state of the EMC/Symmetrix links upon application failover if a backup is running.

NOTE

The command can only be used in the cluster environment.

EXAMPLES

Following example illustrates how the `omniclus` command works.

1. Abort all running sessions

```
omniclus -clus cluster.domain.com -session * -abortsess
```

Note: On UNIX systems replace the `*` wildcard with `'*'`.

The utility will connect to all running sessions and will send them abort messages. The state of the sessions can be then checked with the Data Protector `omnistat` utility.

2. Abort specific running sessions

```
omniclus -clus cluster.domain.com -session mybackup  
-abortsess
```

The utility will connect to backup session managers issuing abort messages and sending them additional information - the backup specification name. Each

backup session manager checks whether the command addresses it and if this is the case it aborts.

3. Abort sessions (all or specific) with application identifications

```
omniclus -clus obvs.hermes.com -session * -abortsess  
-abortid != 10
```

Note: On UNIX systems replace the * wildcard with '*'.

This way the user can define groups of sessions and abort only the ones that are actually related to the application that failed over. For example a backup session that performs a normal filesystem backup of a remote client is not aborted because an application server switches, while the application server backup can be aborted.

4. Temporarily disabling the Data Protector cell

The following command will inhibit backup sessions for twenty minutes:

```
omniclus -clus cluster.domain.com -inhibit 20
```

The following command will inhibit backup sessions forever:

```
omniclus -clus cluster.domain.com -inhibit *
```

Note: On UNIX systems replace the * wildcard with '*'.

The following command will re-activate backup sessions immediately:

```
omniclus -clus cluster.domain.com -inhibit 0
```

5. EMC/Symmetrix links

The following syntax will connect to specific (running) backup session managers and inform them to left the EMC/Symmetrix links split:

```
omniclus -clus cluster.domain.com -session * -symlink split
```

Note: On UNIX systems replace the * wildcard with '*'.

The following syntax will connect to specific (running) backup session managers and inform them to left the EMC/Symmetrix links active (established):

```
omniclus -clus cluster.domain.com -session * -symlink  
active
```

Note: On UNIX systems replace the * wildcard with '*'.

SEE ALSO

omnirsh(1M)

omnicreatedl

creates a filesystem backup specification file (datalist); or an HP StorageWorks Disk Array XP, HP StorageWorks Virtual Array, or HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB backup specification file (datalist)
(this command is available on systems with the Data Protector User Interface component installed)

omnicreatedl

SYNOPSIS

omnicreatedl -version | -help

FILESYSTEM BACKUP SPECIFICATION

omnicreatedl [-datalist *Name*] [-host *HostName1* [*HostName2...*]]
[-device *BackupDevice*]

MS EXCHANGE ZDB BACKUP SPECIFICATION

omnicreatedl -ex2000 -datalist *Name* [-device *Name*] {*DISK_ARRAY_XP_OPTIONS* | *VIRTUAL_ARRAY_OPTIONS* | *ENTERPRISE_VIRTUAL_ARRAY_OPTIONS*} *EXCHANGE_OPTIONS* [-force] [-virtualSrv *Name*]

DISK_ARRAY_XP_OPTIONS

1. ZDB-to-disk or ZDB-to-disk+tape session

-split_mirror -sse -local *app_sys bck_sys* [-mirrors *MU_Numbers*]
-instant_restore [-leave_enabled_bs] [-split | -establish]

2. ZDB-to-tape session

-split_mirror -sse -local *app_sys bck_sys* [-mirrors *MU_Numbers*]
[-keep_version [-leave_enabled_bs]] [-split | -establish]
-split_mirror -sse {-remote *app_sys bck_sys* | -combined *app_sys bck_sys*}
[-keep_version [-leave_enabled_bs]] [-split | -establish]

VIRTUAL_ARRAY_OPTIONS

1. ZDB-to-disk or ZDB-to-disk+tape session

-snapshot -va *app_sys bck_sys* -instant_recovery [-snapshots *number*]
[-leave_enabled_bs] [-lun_security]

2. ZDB-to-tape session

-snapshot -va *app_sys bck_sys* [-use_existing_snapshot]
[-leave_version [-leave_enabled_bs]] [-lun_security]

ENTERPRISE_VIRTUAL_ARRAY_OPTIONS

1. ZDB-to-disk session

```
-snapshot -smis app_sys bck_sys -instant_recovery [-snapshots  
number]
```

2. ZDB-to-disk+tape session

```
-snapshot -smis app_sys bck_sys -instant_recovery [-snapshots  
number] [-wait_clonecopy number]
```

3. ZDB-to-tape session

```
-snapshot -smis app_sys bck_sys -snapshot_type {standard | vsnap  
| clone [-wait_clonecopy number]} -snapshot_policy {strict | loose}  
-replica_conf {local | combined [-ca_failover_option {follow_rep-  
lica_direction | maintain_replica_location}]}
```

EXCHANGE_OPTIONS

```
-annotation {MIS | SRS | KMS}  
{-all_storage_groups | -storage_group Storage_Group_Name1 [-store  
Store1 [Store2...]] [-storage_group Storage_Group_Name2 [-store  
Store1 [Store2... ]]]...}
```

DESCRIPTION

FILESYSTEM BACKUP SPECIFICATION

The `omnicreatedl` command creates a filesystem backup specification file (datalist). It searches all specified clients for local mount points and puts them in the backup specification or on the `stdout` if no backup specification name is specified. If no client is specified, all clients in the cell are searched.

MICROSOFT EXCHANGE SERVER ZDB BACKUP SPECIFICATION

The `omnicreatedl` command is also used to create an Exchange ZDB backup specification file for the following disk arrays:

HP StorageWorks Disk Array XP

HP StorageWorks Virtual Array

HP StorageWorks Enterprise Virtual Array

When creating an Exchange ZDB backup specification file, if the circular logging is disabled for any storage group, an Exchange ZDB transaction logs backup

specification file for each such storage group specified in the Exchange ZDB backup specification file is additionally created.

An Exchange ZDB backup specification file includes the stop/ quiesce the application and restart the application scripts (`omniEx2000.exe`) sections for dismounting/ mounting backed up stores and checking their consistency. A backup specification can be edited later using the Data Protector GUI to modify backup devices, ZDB options, schedule, etc.

For a Microsoft Exchange Server ZDB, the *final* decision on whether the created backup specification will start a ZDB-to-disk, ZDB-to-disk+tape or ZDB-to-tape session depends on the Data Protector `omnib` command options selection.

OPTIONS

`-version`

Displays the version of the `omnicreatedl` command

`-help`

Displays the usage synopsis for the `omnicreatedl` command

FILESYSTEM BACKUP SPECIFICATION

`-datalist Name`

Specifies the name of the backup specification file (`datalist`) for filesystem backup. The backup specification file is created on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\datalists` (Windows Server 2008), `Data_Protector_home\Config\Server\datalists` (other Windows systems), or `/etc/opt/omni/server/datalists` (HP-UX or Solaris systems). If this option is not specified, backup specification objects are written to stdout.

`-host HostName1 [HostName2]`

List of all clients whose filesystems will be included in the backup specification. If this option is not specified, all clients from the cell are used.

`-device BackupDevice`

Specifies the backup device to be used for backup. If this option is not used, the backup device must be specified using the Data Protector GUI.

MICROSOFT EXCHANGE SERVER ZDB BACKUP SPECIFICATION

`-ex2000`

Instructs the `omnicreatedl` command to create a Disk Array XP Microsoft Exchange Server ZDB backup specification file and, if circular logging is disabled

for any storage group specified, a Disk Array XP Microsoft Exchange Server ZDB transaction logs backup specification file(s) for every such storage group.

`-datalist Name`

Specifies the name of the Microsoft Exchange Server ZDB backup specification file (datalist) for the Microsoft Exchange Server ZDB. The datalist is created on the Cell Manager in the directory

Data_Protector_program_data\Config\Server\datalists (Windows Server 2008), *Data_Protector_home*\Config\Server\datalists (other Windows systems), or /etc/opt/omni/server/datalists (HP-UX or Solaris systems).

The corresponding datalist(s) for Microsoft Exchange Server logs for every storage group specified that has the circular logging disabled is/are also created in the same directory with the file name *Storage_Group_Name* (LOGS) *app_sys*.

If any of the thus created backup specification files (datalists) has a name that already exists, the `omnicreatedl` command issues a warning and, depending on whether the `-force` option is set or not, overwrites the existing backup specification files with the same name or aborts the action.

`-force`

Forces overwriting of an existing backup specification file with the same name.

`-virtualSrv Name`

The name of the Microsoft Exchange Server virtual server. This option is obligatory and used only in cluster configurations.

DISK_ARRAY_XP_OPTIONS

`-split_mirror -sse`

Instructs the `omnicreatedl` command to create a Disk Array XP Microsoft Exchange Server ZDB backup specification file.

`-local app_sys bck_sys`

Selects the Business Copy XP (BC) configuration, with the application system *app_sys* and the backup system *bck_sys*.

`-remote app_sys bck_sys`

Selects the Continuous Access XP (CA) configuration, with the application system *app_sys* and the backup system *bck_sys*.

`-combined app_sys bck_sys`

Selects the Combined (Continuous Access XP + Business Copy XP) configuration, with the application system *app_sys* and the backup system *bck_sys*.

`-mirrors MU_numbers`

Specifies a specific replica or a replica set to be used in the backup session to define a replica set from which the integration, according to the replica set rotation, selects one replica to be used in the backup session. If this option is not specified, the *MU# 0* is set.

Enter an integer number from 0 to 2, any range of integer numbers from 0 to 2, or any combination of integer numbers from 0 to 2 separated by a comma. For example:

1

1-2

2, 0, 1

If the sequence is specified, it does not set the order in which the replicas are used. They are used according to the replica set rotation.

If a range is entered, it must be specified in ascending order.

`-instant_restore`

When this option is specified, the `omnicreated1` command automatically sets the `-keep_version` option. Specify the `-instant_restore` option to enable ZDB to disk or ZDB to disk+tape and instant recovery from the replica. If this option is not specified, it is not possible to perform ZDB to disk or ZDB to disk+tape and instant recovery from the replica. However, this option does not influence the replica set rotation.

`-keep_version`

If this option is specified, the pairs involved in the backup session will remain split after the backup session, enabling you to restore from the replica if an instant recovery is needed. If this option is not specified, the disks involved in the backup session are resynchronized after the backup session, only if one or no replica is set by the `-mirrors` option. If more than one replica is set by the `-mirrors` option, the disks involved in the backup session will remain split after the backup session. If this option is not specified, it is not possible to specify the `-leave_enabled_bs` option.

`-leave_enabled_bs`

To specify this option, the `-keep_version` option has to be specified. By default, Data Protector dismounts the filesystems on the backup system after each backup. If this option is specified, the filesystems remain mounted after the backup. Thus, you can use the backup system for some data warehouse activity afterwards, but not for instant recovery.

`-split`

If this option is specified, the mirrored disks in the replica selected for the current backup session are resynchronized with the P-VOLs at the start of the current

backup session. If neither the `-split` nor the `-establish` option is specified, the `-establish` option is set automatically.

`-establish`

If this option is specified and the replica for the next backup is not synchronized, a resync will be initiated before the next backup. If neither the `-split` nor the `-establish` option is specified, the `-establish` option is set automatically.

VIRTUAL_ARRAY_OPTIONS

`-snapshot -va app_sys bck_sys`

Sets the application system *app_sys* and the backup system *bck_sys* and instructs the `omnicreatedl` command to create an HP StorageWorks Virtual Array snapshot datalist.

`-instant_recovery`

Specify this option if you want to perform either a ZDB to disk or a ZDB to disk+tape and leave the replica on a disk array (after the backup session) to use it in future for instant recovery. If this option is not set, it is not possible to perform instant recovery from the replica created or reused in this backup session.

If this option is specified, you should also set the `-snapshots` option.

Note that when this option is selected, the options `-use_existing_snapshot` and `-leave_version` are automatically set by Data Protector.

`-snapshots number`

Specify the number of replicas you want to keep on a disk array. During every backup session, Data Protector creates a new replica and leaves it on a disk array as long as the specified number is not reached. When the specified number is reached, Data Protector reuses the oldest replica.

This option sets the number of replicas in the replica set for a backup specification.

You need to specify this number, if you have selected the `-instant_recovery` option.

If the option is not specified, it is set to 1. The maximum is 1024.

`-use_existing_snapshot`

By default, Data Protector automatically sets this option if the `-instant_recovery` option is specified.

If configuring a ZDB-to-tape session, select this option if you want to reuse an existing replica.

Data Protector can reuse a replica only if the following condition is met, otherwise the backup session will fail:

On a disk array, there must already exist a replica that can be reused. Only replicas that are not marked for instant recovery (are not part of the replica set) or include no snapshots that are listed in the VA LUN exclude file can be reused. Any replica which is not marked for instant recovery or includes no snapshots which are listed in the VA LUN exclude file can be reused.

`-leave_version`

By default, Data Protector automatically sets this option if the `-instant_recovery` option is specified.

If configuring a ZDB-to-tape session (the `-instant_restore` option is not specified), specify this option if you wish to keep the replica on a disk array after the ZDB-to-tape session is completed. In this case, the replica will not be available for instant recovery, but can be reused in future backup sessions using the same backup specification with the option `-use_existing_snapshot` specified.

If this option is not specified, the replica is deleted after the backup session is completed.

`-leave_enabled_bs`

To specify this option, the `-leave_version` option has to be specified. By default, Data Protector dismounts the filesystems on the backup system after each backup. If this option is specified, the filesystems remain mounted after the backup is finished.

Thus, you can use the backup system for some data warehouse activity afterwards, but not for instant recovery.

By default, this option is not selected.

`-lun_security`

Specify this option if you want to apply the LUN security to the child LUNs (target volumes or snapshots) that the integration creates.

If Secure Manager is activated on HP StorageWorks Virtual Array, you must specify this option and configure passwords correctly, otherwise the backup sessions will fail.

The LUN security is set using the `omnidbva` command.

By default, this option is not selected.

`ENTERPRISE_VIRTUAL_ARRAY_OPTIONS`

`-snapshot-smis app_sys bck_sys`

Instructs the `omnicreated1` command to create an HP StorageWorks Enterprise Virtual Array snapshot backup specification file and sets the application system `app_sys` and the backup system `bck_sys`.

`-instant_recovery`

This parameter is optional. Specify this option, if you want to perform either a ZDB to disk or a ZDB to disk+tape and leave the replica on a disk array (after the backup session) to use it in future for instant recovery. If this option is not set, it is not possible to perform instant recovery from the replica created in this backup session.

Note that when this option is selected, the options `-snapshot_type clone` and `-snapshot_policy strict` are automatically set by Data Protector. If the option `-snapshots number` is not specified, it is set to 1.

`-snapshots number`

This parameter is optional. By default, Data Protector automatically sets this option to 1 if the `-instant_recovery` option is specified.

Specify this option if you wish to keep the replica on a disk array after a backup session is completed. With *number*, specify the number of replicas you want to keep on a disk array. During every backup session, Data Protector creates a new replica and leaves it on a disk array as long as the specified number is not reached. When the specified number is reached, Data Protector deletes the oldest replica and creates a new one.

The maximum number for vsnaps and standard snapshots is 7. Data Protector does not limit the number of replicas rotated, but the session will fail if the limit is exceeded.

Note that this option sets the number of replicas in the replica set for a backup specification.

`-snapshot_type{standard | vsnap | clone}`

This option instructs Data Protector to create one of the two types of HP StorageWorks Enterprise Virtual Array snapshots during the backup session.

Setting `standard` creates snapshots with the pre-allocation of disk space.

Setting `vsnap` creates snapshots without the pre-allocation of disk space.

Setting `clone` creates a clone of an original virtual disk.

`-snapshot_policy{strict | loose}`

Specifies how Data Protector creates snapshots with regard to types of already existing snapshots for the same original virtual disk.

When `strict` is set, Data Protector attempts to create snapshots of the type selected by the `-snapshot_type` option. If some of the original virtual disks used in the backup session already have existing snapshots of different type, the selected type of snapshots cannot be used. Such a backup session will be aborted.

When `loose` is set, Data Protector creates snapshots of different type than specified by the `-snapshot_type` option, when this would help to make a successful session. For example, if you select standard snapshots to be created, but Data Protector detects that standard snapshots cannot be created because

some vsnaps or snapclones of the source volumes already exist in a replica set, the following happens: with the loose option selected, Data Protector creates either vsnaps (if vsnaps already exist) or snapclones (if snapclones already exist) instead of standard snapshots. Note that Data Protector can use only one type of snapshots in the backup session. In case when some of the original virtual disks used in the backup session have existing standard snapshots and some of them existing vsnaps, the backup session will be aborted.

`-wait_clonecopy number`

This parameter is optional and can be selected only if the `-snapshot_type clone` option is selected.

In the case of a ZDB to tape or a ZDB to disk+tape, specify this option if you want to delay moving data to tape media until the cloning process is completed. By *number*, specify the maximum waiting time in minutes. After the specified number of minutes, the backup to tape will start even if the cloning process is not finished yet.

With this option, you prevent degradation of the application data access times during the phase of backup to tape.

`-replica_conf{local | combined}`

Select the EVA configuration. Specify `local` to configure a backup specification for ZDB in Business Copy (BC) EVA environments. Specify `combined` to configure a backup specification for ZDB in combined Continuous Access + Business Copy (CA+BC) EVA environments.

`-ca_failover_option{follow_replica_direction | maintain_replica_location}`

This parameter is optional and is available only if the `combined` replica configuration is selected. Specify this option to control the replication direction after a failover.

Select `follow_replica_direction` to follow the replication direction and create replicas on the array remote to current source. A failover reverses the replication direction and the replicas are created on the array that was originally a source EVA.

Select `maintain_replica_location` to maintain the replica location and create replicas on the array remote to home. After a failover, replicas continue to be created on the destination array that has also become a source EVA.

Note that when `-ca_failover_option` option is selected, `follow_replica_direction` is set as default.

EXCHANGE_OPTIONS

`-annotation{MIS | SRS | KMS}`

This option specifies the possible Microsoft Exchange Server annotations: Microsoft Information Store (MIS), Site Replication Service (SRS), and Key Management Service (KMS). MIS is the default setting and does not need to be specified in case when the MIS will be backed up.

`-all_storage_groups`

This option creates a backup specification for all databases relating to Microsoft Exchange Server Microsoft Information Store. It must be specified by the `-annotation MIS` parameter.

`-storage_group storage_group_name`

This option creates a backup specification for all stores relating to the specified storage group. Multiple declarations of the `-storage_group` parameter are possible to create a backup specification for the selected storage groups.

Logical storage group names can be obtained by using the Exchange System Administrator tool, which is a part of Microsoft Exchange Server.

`-store Store1 [Store2...]`

When the `-store` parameter is specified, backup specification is created only for specified store(s) inside the storage group. List of stores can be specified after the `-store` parameter to create a backup specification for many stores.

Store names can be obtained by using Exchange System Administrator tool, which is a part of Microsoft Exchange Server.

EXAMPLES

The following examples show how the `omnicreatedl` command works:

1. To create an HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server running on client "computer1.company.com" with the backup system "computer2.company.com", to back up all storage groups relating to Microsoft Information Store, run:

```
omnicreatedl -ex2000 -datalist Exchange_example  
-all_storage_groups -split_mirror -sse -local  
computer1.company.com computer2.company.com
```

The `omnicreatedl` command creates the HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" and additional HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB transaction logs backup specification files (in case they do not already exist) for each storage group with disabled circular logging option.

2. To create an HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server running on client "computer1.company.com" with the backup system "computer2.company.com", to back up entire First Storage Group and Test Storage Group (both have circular logging disabled), run:

```
omnicreatedl -ex2000 -datalist Exchange_example  
-storage_group "First Storage Group" -storage_group "Test  
Storage Group" -split_mirror -sse -local  
computer1.company.com computer2.company.com
```

The `omnicreatedl` command creates the HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file (datalist) named "Exchange_example" and two additional HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB transaction logs backup specification files (if they do not already exist) named: "First Storage Group (LOGS) computer1.company.com" for First Storage Group log files backup and "Test Storage Group (LOGS) computer1.company.com" for Test Storage Group log files backup.

3. To create an HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" for a Microsoft Exchange Server running on "computer1.company.com" with the backup system "computer2.company.com", overwriting the possible already existent backup specification files with the same name to back up First Mailbox Store, Public Folder Store, part of First Storage group and Test Mailbox Store, part of Test Storage Group, run:

```
omnicreatedl -ex2000 -datalist Exchange_example  
-storage_group "First Storage Group" -store "First Mailbox  
Store" "Public Folder Store" -storage_group "Test Storage  
Group" -store "Test Mailbox Store" -split_mirror -sse  
-local computer1.company.com computer2.company.com -force
```

The `omnicreatedl` command creates the HP StorageWorks Disk Array XP Microsoft Exchange Server ZDB-to-tape backup specification file (datalist) "Exchange_example" and two additional HP StorageWorks Disk Array XPP Microsoft Exchange Server ZDB transaction logs backup specification files if circular logging option is disabled for a particular storage group: "First Storage Group (LOGS) computer1.company.com" for First Storage Group log files backup and "Test Storage Group (LOGS) computer1.company.com" for Test Storage Group log files backup. Any possible already existent backup specification file with the same name is overwritten.

4. To create an HP StorageWorks Virtual Array Microsoft Exchange Server ZDB-to-tape backup specification file (datalist) "Exchange_example", to back up Site Replication Service on "dev1" device, run:

```
omnicreatedl -ex2000 -datalist Exchange_example -device  
dev1 -annotation SRS -snapshot -va computer1.company.com  
computer2.company.com
```

The `omnicreatedl` command creates an HP StorageWorks Virtual Array Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" and HP StorageWorks Virtual Array Microsoft Exchange Server ZDB transaction logs backup specification file in case it does not already exist: "SRS (LOGS) computer1.company.com" for Site Replication Service log files backup if the circular logging is disabled.

5. To create an HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB-to-tape backup specification file (datalist) "Exchange_example", to back up Site Replication Service on "dev1" device, using the `vsnap` type of snapshot and the strict snapshot policy, run:

```
omnicreatedl -ex2000 -datalist Exchange_example -device  
dev1 -annotation SRS -snapshot -smis computer1.company.com  
computer2.company.com -snapshot_type vsnap -snapshot_policy  
strict
```

The `omnicreatedl` command creates an HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB-to-tape backup specification file named "Exchange_example" and an HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB transaction logs backup specification file in case it does not already exist: "SRS (LOGS) computer1.company.com" for Site Replication Service log files backup if the circular logging is disabled. When the `omnib` command or Data Protector GUI is used to start the created backup specification, Data Protector tries to create the `vsnap` type of snapshots if they cannot be created, the session aborts.

6. To create an HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB-to-disk backup specification file (datalist) "Exchange_example", to back up Site Replication Service on the backup device "dev1", using the replica set with "5" replicas, run:

```
omnicreatedl -ex2000 -datalist Exchange_example -device  
dev1 -snapshot -smis computer1.company.com  
computer2.company.com -instant_recovery -snapshots 5  
-annotation SRS
```

In case it does not already exist, `omnicreatedl` creates an EVA Microsoft Exchange Server transaction logs backup specification file "SRS (LOGS) computer1.company.com" for Site Replication Service log files backup (the circular logging must be disabled). When the `omnib` command or Data Protector GUI is used to start the created backup specification, you must choose the ZDB-to-disk session. Data Protector tries to create the `snapclone` type of snapshots;

if they cannot be created, the session aborts. After the backup session, the created replica is retained on a disk array and can be used for instant recovery.

7. To create an HP StorageWorks Enterprise Virtual Array Microsoft Exchange Server ZDB-to-disk+tape backup specification file (datalist) "Exchange_example", to back up Site Replication Service on the backup device "dev1", using the replica set with "3" replicas and to delay the backup to tape for the maximum of "50" minutes, run:

```
omnicreatedl -ex2000 -datalist Exchange_example -device  
dev1 -snapshot -smis computer1.company.com  
computer2.company.com -instant_recovery -snapshots 3  
-wait_clonecopy 50 -annotation SRS
```

In case it does not already exist, `omnicreatedl` creates an EVA Microsoft Exchange Server transaction logs backup specification file "SRS (LOGS) computer1.company.com" for Site Replication Service log files backup (the circular logging must be disabled). When the `omnib` command or Data Protector GUI is used to start the created backup specification, you must choose the ZDB-to-disk+tape session. Data Protector tries to create the snapclone type of snapshots; if they cannot be created, the session aborts. The backup to tape will start after the snapclones are fully created or after 50 minutes. After the backup session, the created replica is retained on a disk array and can be used for instant recovery.

SEE ALSO

`omnib(1)`, `omniintconfig.pl(1M)`, `util_cmd(1M)`, `util_oracle8.pl(1M)`,
`util_vmware.exe(1M)`

omnidb

queries the Data Protector internal database (IDB)
(this command is available on systems with the Data Protector User Interface component installed)

omnidb

SYNOPSIS

```
omnidb -version | -help
omnidb -session [-datalist Datalist] [-type {restore | backup |
verification}] [-user User] [[[-since Date] [-until Date]] | [-last
Number] | [-latest] | [-wo start duration]] [-detail]
omnidb -filesearch [-n N]Client Directory FileName
omnidb Object [-session SessionID] [-copyid CopyID] -listdir Dir-
ectory
omnidb -list_folders -session SessionID [-mailbox MailboxName...]
omnidb -rpt [SessionID | -latest] [-detail]
omnidb -rpt [-wo start duration]
omnidb -session SessionID [{-report Report | -detail | -encryption-
info | -strip | -purge | -change_protection Protection |
-change_catprotection Protection | -media [-detail]]}]
omnidb -object [{-detail | -encryptioninfo}]
omnidb [-noexpand] {-filesystem | -winfs | -vbfs} Client:Mount-
PointLabel [-file FileName] [{-detail | -encryptioninfo}]
omnidb Object [ -since Date [-until Date] | -last NumberOfDays |
-latest] [-change_protection Protection] [-change_catprotection
Protection]
omnidb Object [{-since Date] [-until Date] | -last NumberOfDays}
[-latest] [{-detail | -encryptioninfo}]
omnidb Object -strip NumberOfDays
omnidb -strip
omnidb -change_protection Protection
omnidb -change_catprotection Protection
omnidb [-noexpand] {-filesystem | -winfs | -netware} Client:Mount-
Point Label -fileversions FileName [{-detail | -encryptioninfo}]
omnidb Object [{-detail | -encryptioninfo}]
omnidb Object [-noexpand] -session SessionID [-copyid CopyID]
[-report [Report] | -catalog | -change_protection Protection |
-change_catprotection Protection | -strip | -encryptioninfo]
omnidb Object -session SessionID [-copyid CopyID] -media [-detail]
```

```

omnidb Object [-session SessionID [-copyid CopyID] -listcopies
[{-detail | -encryptioninfo}]
omnidb -auditing [-timeframe StartDate EndDate | -since Date
[-until Date] | -last NumberOfDays] [-detail]

Object

[-noexpand]
{-filesystem [Client:MountPoint Label] |
-winfs [Client:MountPoint Label] |
-netware [Client:MountPoint Label] |
-omnidb [Client:MountPoint Label] |
-rawdisk [Client Label] |
-sap [Client:Set] |
-sapdb [Client:Set] |
-stream [Client:Set] |
-oracle8 [Client:Set] |
-vmware [Client:Set] |
-mssql [Client:Set] |
-mssps [Client:Set] |
-msexchange [Client:Set] |
-mbx [Client:Set] |
-informix [Client:Set] |
-sybase [Client:Set] |
-lotus [Client:Set] |
-vss [Client:Set] [|]
-db2 [Client:Set]}
```

Protection

```

none | days n | weeks n | until Date | permanent
```

Report

```

warning | minor | major | critical
```

Date

```

[YY]YY/MM/DD (1969 < [YY]YY < 2038)
```

DESCRIPTION

The `omnidb` command is used to query the IDB Log database.

This command can be used to:

- list sessions and their summary reports
- list backed up objects and their details (for example: client name, mountpoint, label, object type, object status, backup type, etc.), message logs, and media location
- search for all occurrences of a pathname pattern

The `omnidb` command performs basic IDB queries.

OPTIONS

`-version`

Displays the version of the `omnidb` command

`-help`

Displays the usage synopsis for the `omnidb` command

`-datalist IntegrationName BackupSpecificationName`

Lists the sessions resulting from backup specification backups created using this *BackupSpecificationName*.

NOTE: For non-filesystem backup specification (Microsoft Exchange Server, Microsoft SQL Server, Informix Server, etc.)

IntegrationName must be specified in front of *BackupSpecificationName*. Both must be in double quotes.

`-type {restore | backup | verification}`

If no *SessionID* is specified, the command lists either backup, restore, or verification sessions. If *SessionID* is specified for backup sessions, the command lists the objects created for that backup session.

`-user User`

Lists only the sessions belonging to the specified user.

`-since Date`

Lists sessions since the given *Date*.

`-until Date`

Lists sessions until the given *Date*.

`-last n`

Lists sessions that occurred within the last *n* days.

`-latest`

Lists the last active Data Protector session.

`-wo start duration`

Lists the sessions that started within a specified timeframe. *Start* defines the start of the timeframe. *Duration* is the duration of the timeframe in seconds.

`-detail`

Displays detailed information about the selected query, such as backup type, protection, whether or not encrypted.

`-encryptioninfo`

Displays detailed encryption information for objects meeting the query criteria.

`-session SessionID`

Displays session information. If no *SessionID* is specified, all sessions are shown. The report shows for each session: the ID, type, status and user (UNIX login, UNIX group and client). If a *sessionID* is specified, then objects that are backed up within this session are shown. This information includes: client name, mountpoint, label, object type and object status.

If the `-detail` option is specified, more information is shown, such as the backup type (full, incr, ...), protection status, encryption status, and so on. For integration objects, also the backup ID is shown.

If the `-encryption` option is specified, the Encryption KeyID-StoreID is displayed for each encrypted object created during the specified session. *SessionID* is mandatory in this case.

`-auditing`

Lists auditing related information from the cell. The following information is listed for each backup session: name, specification, completion status, backup type, start time, end time, and owner.

If the `-detail` option is specified, the command also lists used media and objects.

`-copyid CopyID`

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option is obligatory. It selects a specific copy.

`-filesearch[-n N] Client Directory FileName`

Lists all the backed up files and directories that match the selection criteria set by the *Client Directory FileName* parameters. Wildcards can be used. The list can be limited to a certain number of displayed objects by setting the `-n` suboption, where *N* is the number of objects to be displayed. The following information is displayed about each object: object type, object name, object description, pathname.

`-listdir Directory`

Lists all the backed up objects in the specified directory.

`-list_folders`

Microsoft Exchange Server single mailbox restore only: displays a list of all single mailbox folders (including their subfolders) backed up within a particular session.

`-mailbox MailboxName`

Microsoft Exchange Server single mailbox restore only: displays mailbox folders for a particular mailbox only. If the option is not specified, folders of all backed up mailboxes are listed.

`-listcopies`

Lists details on all existing object or mirror copies of the specified object for the specified session. The SessionID, the CopyID, the time and the status of object copy or mirror sessions for the specified object are listed.

`-rpt SessionID`

Displays session information in a form specially suited for further use of awk, grep or perl. Records are separated with blank lines and line feed is the field separator. If no *SessionID* is specified, all backup sessions are shown. Each record contains the following fields: the ID, backup specification name, status, start time in format *HH:MM* and duration in hours as a floating point number.

`-report Report`

Lists all messages (of specified report level and higher) which were generated by the specified session. Messages are classified (in ascending order) as: warning, minor, major and critical. For example, if major is selected, only major and critical messages are reported. By default, all messages are reported.

`-object`

Displays information on all data objects. The report shows the client name, label, and object type.

If the `-detail` option is specified, more detailed information is displayed for each object, such as each session for which object versions were created, together with protection status, encryption status, etc.

If the `-encryptioninfo` option is specified, for each object, the Encryption KeyID-StoreID is displayed for each session in which object versions were created.

`-filesystem[Client:MountPoint Label]`

Displays information on all filesystem objects (displays the *Client:MountPoint Label* string for every filesystem object in the IDB). If a *Client:MountPoint Label* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-winfs[Client:MountPoint Label]`

Displays information on all Windows filesystem objects (displays the *Client:MountPoint Label* string for every Windows filesystem object in the IDB). If a *Client:MountPoint Label* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-vbfs[Client:MountPoint Label]`

Displays information on all Windows filesystem objects (displays the *Client:MountPoint Label* string for every Windows filesystem object in the IDB). If a *Client:MountPoint Label* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-omnidb[Client:MountPoint Label]`

Displays information on IDB object (displays the *Client:MountPoint Label* string for every IDB object in the IDB). If a *Client:MountPoint Label* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-rawdisk[Client Label]`

Displays information on disk image objects (displays the *Client Label* string for every rawdisk object in the IDB). If a *Client Label* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-sap[Client:Set]`

Displays information on SAP R/3 data objects (displays the *Client:Set* string for every SAP R/3 object in the IDB). If *Client:Set* is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-sapdb[Client:Set]`

Displays information on SAP DB/MaxDB data objects (displays the *Client:Set* string for every SAP DB/MaxDB object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-stream[Client:Set]`

Displays information on stream objects (displays the *Client:Set* string for every stream object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-oracle8[Client:Set]`

Displays information on Oracle objects (displays the *Client:Set* string for every Oracle object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the status, size of object and the number of errors for the session.

`-vmware[Client:Set]`

Displays information on VMware Virtual Infrastructure objects (displays the *Client:Set* string for every VMware Virtual Infrastructure object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the status, size of object and the number of errors for the session.

`-mssql[Client:Set]`

Displays information on Microsoft SQL Server objects (displays the *Client:Set* string for every Microsoft SQL Server object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-mssps[Client:Set]`

Displays information on Microsoft SharePoint Portal Server objects (displays the *Client:Set* string for every Microsoft SharePoint Portal Server object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-msexchange[Client:Set]`

Displays information on Microsoft Exchange Server objects (displays the *Client:Set* string for every Microsoft Exchange Server object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-mbx[Client:Set]`

Displays information on Microsoft Exchange Server objects - single mailboxes (displays the *Client:Set* string for every Microsoft Exchange Server object - single mailboxes in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-informix [Client:Set]`

Displays information on Informix Server objects (displays the *Client:Set* string for every Informix Server object in the IDB). If an *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-sybase[Client:Set]`

Displays information on Sybase objects (displays the *Client:Set* string for every Sybase object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-lotus[Client:Set]`

Displays information on Lotus Notes/Domino objects (displays the *Client:Set* string for every Lotus Notes/Domino object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-vss[Client:Set]`

Displays information on Microsoft Volume Shadow Copy (VSS) objects (displays the *Client:Set* string for every VSS object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-db2[Client:Set]`

Displays information on IBM DB2 UDB objects (displays the *Client:Set* string for every IBM DB2 UDB object in the IDB). If a *Client:Set* string is specified, the backup sessions containing the object specified by this string are listed. For each backup session, the report shows: the SessionID, start time, session duration, object status, size of object and the number of errors for the session.

`-noexpand`

Do not expand client names. Use this option if object was backed up with different client name resolution as when using this option.

`-strip`

This option works in three different ways. If `sessionID` is specified it strips the detail catalogs for all objects of session with specified `SessionID`. If both `SessionID` and `ObjectName` are specified it strips the detail catalog of the object identified by `ObjectName` for the session with specified `SessionID`. If no option is specified, it strips catalogs on all data objects that are no longer protected.

`-strip NumberOfDays`

This option can be used with `ObjectName` to strip the detail catalogs for all versions of specified object that are older than *NumberOfDays* days.

`-fileversions FileName`

Displays information on all sessions which contain the filesystem with specified file *FileName*, session ID, mode, date modified, size and type.

`-media`

Shows list of the media used in the backup session. If object is also specified then it only shows list of media containing that object.

`-user_location`

This option changes the output of media related reports to print out user defined location instead of physical location used by default.

`-change_protection Protection`

Changes the current protection of the object versions identified by `ObjectName` and/or `SessionID` to the new protection defined as *Protection*. If it is specified without any other option then it changes protection for all Failed/Aborted objects. Protection can be none, permanent, until a specific date, or for a time interval. When the protection is until a specified date or for a time interval, you must specify the value. The Date form is [YY]YY/MM/DD. In the first case the value is the date until which the data is protected. In the second case the time interval is the number of days (after today) during which the data can not be overwritten.

`-change_catprotection Protection`

Changes the current protection of the catalog retention time. *Protection* can be none, `same_as_data_protection`, until a specific date, or for a time interval. `same_as_data_protection` means that catalog will stay until data is overwritten/exported. When the protection is until a specified date or for a time interval, you must specify the value. The Date form is [YY]YY/MM/DD. In the first case the value is the date until which the data is protected. In the second case the time interval is the number of days (after today) during which the data can not be overwritten.

`-catalog`

Displays the detail catalog of a specified object - session combination. Use an object option (for example `-filesystem`) to specify the object and use the `-session` (and *sessionID*) to specify the session.

`-purge`

This option removes the session from the session list. All objects within the session become unprotected. It is still possible to make a restore from this session.

`-timeframe StartDate EndDate`

Lists the sessions that started within a specified timeframe.

NOTES

With clustered objects, the *Client* argument must be specified as the virtual hostname.

EXAMPLES

The following examples illustrate how the `omnidb` command works.

1. To see details for the backup sessions started by user "root" in last three days, run:
`omnidb -session -user root -last 3 -type backup -detail`
2. To see critical errors for the session with the sessionID "2008/05/14-17", run:
`omnidb -session 2008/05/14-17 -report critical`
3. To see all objects of the type filesystem, run:
`omnidb -filesystem`
4. To see encryption information for all Windows filesystem objects, run:
`omnidb -winfs -encryptioninfo`
5. To see encryption information for objects created in session "2009/03/23-2" run:
`omnidb -session 2009/03/23-2 -encryptioninfo`
6. To see details for the filesystem "hpuljum.hermes.com:/ Label44" in the latest session, run:
`omnidb -filesystem hpuljum.hermes.com:/ Label44 -latest -detail`
7. To see catalog for the filesystem "bob:/" in the session "2008/07/14-6", run:

```
omnidb -filesystem bob:/ -session 2008/07/14-6 -catalog
```

8. To see details for the Microsoft Exchange Server backup specification "TEST" backup sessions, run:

```
omnidb -session -datalist "MSEExchange TEST" -details
```

9. To list all Microsoft Exchange Server mailbox folders in the mailbox "User 2", backed up in the session "2008/03/16-5", run:

```
omnidb -mbx -list_folders -session 2008/03/16-5 -mailbox  
"User 2"
```

10. To see information on Lotus Notes/Domino Server objects:

```
omnidb -lotus
```

11. To see which Lotus Notes/Domino Server files are contained in the Lotus Notes/Domino Server object "computer.company.com:DREAM::Databases:5" from the session "2007/10/26-2", run:

```
omnidb -lotus computer.company.com:DREAM::Databases:5  
-session 2007/10/26-2 -catalog
```

12. To see information on the SAP DB/MaxDB object "machine.company.com:/instance1/Config/1", run:

```
omnidb -sapdb machine.company.com:/instance1/Config/1
```

13. To see detailed information on media used for the Windows filesystem object "system.company.com:/C" with the label "DTS_T" in the session "2008/07/14-17", with CopyID "1280", run:

```
omnidb -winfs system.company.com:/C "DTS_T" -session  
2008/07/14-17 -copyid 1280 -media -detail
```

14. To see detailed information on all existing object or mirror copies of the Windows filesystem object "system.company.com:/D" with the label "D1" with the sessionID "2008/05/01-12", run:

```
omnidb -winfs system.company.com:/D "D1" -session  
2008/05/01-12 -listcopies -detail
```

SEE ALSO

omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1),
omnidbupgrade(1M), omnidbutil(1M), omnidbva(1), omnidbvss(1), omnidbvp(1)

omnidbsmis

executes administrative tasks required for managing the HP StorageWorks SMI-S EVA provider

(this command is available on systems with the Data Protector User Interface component installed)

omnidbsmis

SYNOPSIS

```
omnidbsmis -version | -help
omnidbsmis -ompasswd -add hostname [-ssl] [-port port] [-namespace namespace] [-user username] [-passwd password]
omnidbsmis -ompasswd -remove hostname [-port port] [-namespace namespace] [-user username] [-passwd password]
omnidbsmis -ompasswd [-list [hostname]]
omnidbsmis -ompasswd [-check [-host hostname]]
omnidbsmis -dgrules {-init | -put filename | -get filename | -check EVA_WWN DG_name}
omnidbsmis -caconf {-init | -put filename | -get filename | -list EVA_Name | -check DR_Group_Name}
omnidbsmis [-list] {-session [-ir] [-excluded] [-original] | -datalist}
omnidbsmis [-show] {-session sessionID | -datalist DatalistName}
omnidbsmis -list -purge
omnidbsmis -purge [-force] [-host hostname]
omnidbsmis -delete {-session SessionID | -datalist DatalistName} [-preview] [-force] [-host hostname]
omnidbsmis -sync [-preview] [-force] [-host hostname]
```

DESCRIPTION

The following tasks can be performed using the `omnidbsmis` command:

SETTING, DELETING, LISTING, AND CHECKING THE LOGIN INFORMATION FOR SMI-S EVA PROVIDER

The `omnidbsmis` command can be used to set, delete, and list the login information for SMI-S EVA provider. The systems with SMI-S EVA provider installed are referred to as management systems.

The `omnidbsmis` options used for manipulating the login information for SMI-S EVA provider, which should be used together with the `-ompasswd` option, are: `-add`, `-remove`, `-list`, `-ssl`, `-port`, `-namespace`, `-user`, `-passwd`.

SETTING THE DISK GROUP PAIRS CONFIGURATION FILE

The `omnidbsmis` command can be used to manipulate the EVA disk group pairs configuration file.

By default, the snapclones are created in the same disk group as the source volumes. However, you can define the allocation of snapclones and allocate them to a disk group other than the one used for the source volumes.

The `omnidbsmis` options used for manipulating the EVA disk group pairs configuration file, which should be used together with the `-dgrules` option, are: `-init`, `-put`, `-get`, `-check`.

SETTING UP EVA HOME CONFIGURATION FILE

The `omnidbsmis` command can be used to manipulate the home EVA storage system configuration file. You can create a new home configuration file template and store it in its default configuration directory, download the file for editing and upload it back in the SMISDB. You can also list the data replication (DR) groups with a specified EVA acting as home and check if a specified DR group is part of CA+BC configuration.

The `omnidbsmis` options used for manipulating the home EVA configuration file are: `-caconf`, `-init`, `-get`, `-put`, `-list`, `-check`.

QUERYING THE INFORMATION ON THE BACKUP OBJECTS

The `omnidbsmis` command can be used to query the SMISDB for the information on the backup sessions (the product of every successful backup session is a replica) and the backup specifications (a group of replicas, created using the same backup specification, is a replica set).

Using the `omnidbsmis` command to query the SMISDB, you can:

1. Get detailed information on a specific backup session (replica).
2. Get detailed information on all backup sessions created using a specific backup specification (replica set).
3. Get a list of all backup sessions created using the same backup specification.
4. Get a list of all backup sessions available for instant recovery.
5. Get a list of all backup specifications that have a replica created.
6. Get a list of replicas to be deleted (having the purge flag).

Note that session details are only displayed for the sessions that have the `Keep the replica after the backup` option selected in the backup specification. ZDB-to-tape sessions without this option set are deleted from the SMISDB after each such backup.

The `omnidbsmis` options used for querying the SMISDB are: `-list`, `-session`, `-ir`, `-datalist`, `-purge`, `-show`.

PURGING THE SMISDB

The `omnidbsmis` command can be used to run the purge operation that checks the SMISDB for the virtual disks with the purge flag and, in case of finding such disks, attempts to delete these objects.

The `omnidbsmis` options used for purging replicas and their entries in the SMISDB are: `-purge`, `-force`, `-host`.

DELETING A SPECIFIC BACKUP SESSION (REPLICA) OR ALL BACKUP SESSIONS BASED ON A SPECIFIC BACKUP SPECIFICATION (REPLICA SET) FROM THE DISK ARRAY AND FROM SMISDB

The `omnidbsmis` command can be used to delete volumes of specific backup sessions (replicas or replica sets) from the disk array and information about them from SMISDB. It can perform deletion only for a specific backup session (replica), identified by the backup session ID, or for all backup sessions based on a specific backup specification (replica set), identified by the backup specification name.

Note that it is not possible to perform instant recovery from the deleted replica/replica set.

The `omnidbsmis` options to be used for deleting replicas and SMISDB entries, or only SMISDB entries, which should be used together with the `-delete` option, are: `-session`, `-datalist`, `-preview`, `-force`, `-host`.

SYNCHRONIZING THE SMISDB

The `omnidbsmis` command can be used to run the sync operation on the backup system. During this operation, the EVA SMI-S Agent checks if any target volumes in a replica logged in the SMISDB are missing on the EVA storage system. If a target volume is missing, the whole backup session that created the replica with a missing target volume is deleted from the SMISDB. The check is performed for all replica sets.

The `omnidbsmis` options used for synchronizing the SMISDB are: `-sync`, `-preview`, `-force`, `-host`.

OPTIONS

`-version`

Displays the version of the `omnidbsmis` command.

`-help`

Displays the usage synopsis for the `omnidbsmis` command.

`-ompasswd -add hostname`

Stores the login information for the system with the name *hostname*, on which SMI-S EVA provider is installed, in the SMISDB.

The `-ssl` option specifies that HP StorageWorks EVA SMI-S Provider is SSL-enabled. In this case, the SMI-S Agent uses an SSL-based client connection to communicate with the SMI-S provider.

The `-port port` option specifies the port number on which SMI-S EVA provider listens to requests. The default port number for SMI-S EVA Provider is 5988 (the `-ssl` option is not selected) or 5989 (the `-ssl` option is selected). If your SMI-S EVA Provider is configured to use a different port number, set it using this option.

The `-namespace namespace` parameter is used to specify the namespace that contains the CIMOM configuration for the EVA. The default namespace is `root/eva`.

The `-user username` option sets the user of SMI-S EVA provider. The default user is `administrator`.

The `-passwd password` option sets the password that will be used for logging in to SMI-S EVA provider. If you omit this parameter, the command will ask for a password interactively.

`-ompasswd {-remove hostname | -delete hostname}`

Removes a system with SMI-S EVA provider installed (together with the login and port number information), which has a name *hostname*, from the SMISDB. The `-delete` option is only an alias for `-remove`.

Used together with the `-port port` option, the command will only remove the entries for the specified port. Use this option if you have more than one port configured on the same system, and you want to delete only one port from the configuration.

If the `-namespace namespace` option is specified, the command will only remove the entries for the specified namespace. Use this option if you have more than one namespace configured on the same system, and you want to delete only one namespace from the configuration.

If the `-user username` option is specified, the command will only remove the entries for the specified user. Use this option if you have more than one user configured on the same system, and you want to delete only one user from the configuration.

`-ompasswd -list hostname`

Lists all systems that have SMI-S EVA provider installed, together with the port numbers, on which SMI-S EVA providers listen to requests. The *hostname* value is optional: if you enter a name of the host, only the SMI-S CIMOMs, configured for a specified host, will be displayed.

Note that you will get the same output if you run the `omnidbsmis -ompasswd` command without the `-list` parameter.

`-ompasswd -check [-host hostname]`

Checks if the SMI-S CIMOMs were configured properly in the Data Protector cell. It performs a health check of your environment, which may help identify such potential problems as wrong user name or password provided, a broken network connection, a DNS resolution problem, and so on. The `-host` option is optional: if you enter a name of the host, the command will be run on the specified host, otherwise it will be run on the local host. Note that HP StorageWorks SMI-S Agent must be installed on the specified host.

`-dgrules -init`

Creates a template disk group pairs configuration file or overwrites an old one with the new template. Note that only configured disk group pair rules are overwritten.

`-dgrules -put filename`

Sets the EVA disk group pairs configuration file by reading the contents of the input file, checking its syntax, and uploading the file to the SMISDB. If the syntax of the file is inaccurate, the file is not uploaded.

`-dgrules -get filename`

Prepares the EVA disk group pairs configuration file for editing by reading the contents of the file from the SMISDB and saving it under *filename*.

`-dgrules -check EVA_WWN DG_name`

Provides the information on the disk group that is in pair with the disk group identified by the *EVA_WWN* and *DG_name*. The command returns the information on the 1st disk group name, 2nd disk group name, and EVA WWN. If there is no rule for the specified disk group, the first and the second disk groups are the same.

`-caconf -init`

Creates a template EVA home configuration file or overwrites an old one with the new template.

`-caconf -put filename`

Uploads the edited EVA home configuration file to the SMISDB. If the syntax of the file is inaccurate, the file is not uploaded.

`-caconf -get filename`

Prepares the EVA home configuration file for editing by reading the contents of the file from the SMISDB and saving it under *filename*.

`-caconf -list EVA_name`

Provides the information on the DR groups with the EVA identified by *EVA_Name* acting as home. The command returns the information on *EVA_Name* and the DR groups belonging to this EVA.

`-caconf -check DR_Group_Name`

Checks if a DR group, identified by *DRGroup_name*, is part of CA+BC configuration. The command returns the information on *DR_Group* and WWN of a home EVA.

`-show -session SessionID`

Lists expanded details of a session (identified by the backup session ID). The output of the command is the information on all target volumes created in the specified backup session. The following is displayed:

- Name, ID, and WWN of the target volume created in the backup session
- Name and ID of the EVA storage system on which the target volume was created
- Type of the target volume created
- ID of the source volume used in the backup session
- The backup session ID
- Time stamp of the target volume
- IR flag
- Name of the backup specification used in the backup session
- Names of the application and backup systems involved in the backup session

Note that you will get the same output if you run the `omnidbsmis -session SessionID` command without the `-show` parameter.

`-show -datalist DatalistName`

Lists all replicas that are part of the replica set, which is identified by the backup specification name. Replicas displayed are identified by their backup session IDs. Note that you will get the same output if you run the `omnidbsmis -datalist DatalistName` command without the `-show` parameter.

`-list -session [-ir]`

Lists all replicas that are part of a replica set, together with the backup session IDs and the backup specification names. Note that you will get the same output if you run the `omnidbsmis -session` command without the `-list` parameter. If used together with the `-ir` option, the command lists the sessions marked for instant recovery (ZDB-to-disk and ZDB-to-disk+tape sessions).

`-list -datalist`

Lists all backup specifications that are part of a replica set with existing members. Note that you will get the same output if you run the `omnidbsmis -datalist` command without the `-list` parameter.

`-list -purge`

Lists all virtual disks (source or target volumes) that are marked for purging in the SMISDB.

`-purge`

Runs SMI-S Agent to perform the SMISDB purge operation that attempts to remove the virtual disks (source or target volumes) that could not be deleted although they should be. These elements are marked for purging, and the information about them is stored in the SMISDB.

Used together with the `-force` option, the command forces removal of the elements marked for deletion even if they are presented to the hosts.

If the `-host hostname` option is specified, you can choose another location to start the SMISDB purge operation. Use this option if the systems, involved in a backup session, are no longer available, thus allowing redirection to another systems that have the SMI-S Agent installed.

`-delete -session SessionID`

Deletes a specific backup session (replica), identified by the session ID, on the disk array, and deletes information about the replica from the SMISDB.

`-delete -datalist DatalistName`

Deletes all backup sessions based on a specific backup specification (a replica set) on the disk array, and deletes information about the replica set from the SMISDB. Once excluded from use by Data Protector, sessions cannot be deleted.

`-delete -preview`

If used with the `-preview` option, the command does not delete anything, but lists replicas/replica sets that will be deleted if `-delete -session sessionID` or `-delete -datalist DatalistName` commands are run.

`-delete -force`

Forces deletion of the replicas even if they are presented to hosts.

`-delete -host hostname`

Sets another location to start the deletion. Use this option if the systems, involved in a backup session, are no longer available, thus allowing redirection to another systems that have the SMI-S Agent installed.

`-sync`

Synchronizes the persistent data in the SMISDB with the EVA storage system. If any target volume in a replica is missing on the EVA storage system, the whole backup session that created this replica is deleted from the database. Use this option if you deleted some replicas directly through the SMI-S EVA provider.

If run with the `-preview` option, the command does not delete anything, but lists the target volumes that would be deleted if `omnidbsmis -sync` is run.

Used together with the `-force` option, the command forces removal of the target volumes marked for deletion even if they are presented to hosts.

With the `-host hostname` option specified, you can choose another system to start the SMISDB synchronizing operation. Use this option if the systems, involved in a backup session, are no longer available, thus allowing redirection to another systems that have the SMI-S Agent installed.

EXAMPLES

1. To list all configured management systems together with the port numbers, on which SMI-S EVA providers listen to requests, run:

```
omnidbsmis -ompasswd -list
```

2. To remove a management system with the hostname "system1", together with its login and port number information, from the SMISDB, run:

```
omnidbsmis -ompasswd -remove system1
```

3. To store the login information for SMI-S EVA provider, installed and running on the management system with the hostname "system1", in the SMISDB, run:

```
omnidbsmis -ompasswd -add system1
```

You can also set optional parameters, such as the port number, namespace, and username. If you omit these parameters, the command will take the default values.

4. To perform a health check of you environment on the local host, run:

```
omnidbsmis -ompasswd -check
```

5. To create and set the disk group pairs configuration file or edit it, carry out the steps provided below on the application or backup system:

a) To create a template disk group pairs configuration file or overwrite an old one with the template, run:

```
omnidbsmis -dgrules -init
```

b) To get the file for editing and to save it as "c:\tmp\dgrules.txt", run:

```
omnidbsmis -dgrules -get c:\tmp\dgrules.txt
```

The command reads the disk group pairs configuration file from the SMISDB and saves it in the "c:\tmp" directory on a local system under "dgrules.txt".

c) Edit the "dgrules.txt" file residing in the "c:\tmp" directory and save it. Note that the order of defining disk group names is ignored. This means that if a source volume is found in "disk group 1", its snapclone will be created in "disk group 2", and vice versa. Note that a certain disk group can be a member of only one disk group pair.

d) To upload the "dgrules.txt" file to the server, run:

```
omnidbsmis -dgrules -put c:\tmp\dgrules.txt
```

The command reads the contents of the file, checks its syntax, and copies the file to its location on the Cell Manager.

6. To get the information on the disk group that is the pair of a disk group named `original_disk_group` configured on EVA storage system with WWN `50001FE15007CA90`, run:

```
omnidbsmis -dgrules -check EVA1 original_disk_group
```

The following is the output of the command:

```
Configured disk group pair: 1st disk group  
name:"original_disk_group" 2nd disk group  
name:"paired_disk_group_name" EVA name:"50001FE15007CA90"
```

If there is no rule for the specified disk group, the first and second disk groups are the same.

7. To create the EVA home configuration file or edit it, carry out the below steps on the application or backup system:

a) To create a template EVA home configuration file or overwrite an old one with the template, run:

```
omnidbsmis -caconf -init
```

b) To get the file for editing and to save it as "c:\tmp\cahome.txt", run:

```
omnidbsmis -caconf -get c:\tmp\cahome.txt
```

The command reads the EVA home configuration file from the SMISDB and saves it in the "c:\tmp" directory on a local system under "cahome.txt".

c) Edit the "cahome.txt" file residing in the "c:\tmp" directory and save it.

d) To copy the "cahome.txt" file to its original place, run:

```
omnidbsmis -caconf -put c:\tmp\cahome.txt
```

The command reads the contents of the file, checks its syntax, and copies the file back to the SMISDB.

8. To check if a DR group named `DR Group 1` is part of CA+BC configuration, run:

```
omnidbsmis -caconf -check DR Group 1
```

The following is the command output:

```
DR Group : "DR Group 1" Home EVA : "EVA_WWN"
```

9. To list all existing backup sessions, together with their session IDs and backup specification names, run:

```
omnidbsmis -session
```

- 10.** To find out the name, ID, WWW, type, and time stamp of the target volumes created in the backup session with the session ID "2008/05/13-3", run:
`omnidbsmis -session 2008/05/13-3`
- 11.** To delete a backup session with the session ID "2008/05/13-3" on the disk array and from the SMISDB, run:
`omnidbsmis -delete -session 2008/05/13-3`
- 12.** To run the SMISDB synchronizing operation and force removal of the target volumes marked for deletion, run:
`omnidbsmis -sync -force`

SEE ALSO

omnidb(1M), omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbupgrade(1M), omnidbutil(1M), omnidbva(1), omnidbvss(1), omnidbvp(1), upgrade_cm_from_evaa(1M)

omnidbva

queries the ZDB database (VADB) and administers the VA LUN exclude file, instant recovery and password information

(this command is available on systems with the Data Protector User Interface component installed)

omnidbva

SYNOPSIS

```
omnidbva -version | -help
omnidbva -exclude {-put filename | -get filename | -check VA_wwn
LUN | -init | -delete}
omnidbva -init [-force]
omnidbva -delete session_id [-force]
omnidbva {-session [session_id] | -lun [LUN]}
omnidbva -vapasswd VA_wwn password
omnidbva -samppasswd SAM_server_ID user password
omnidbva -dbcheck [-force]
```

DESCRIPTION

The `omnidbva` command can be used to manipulate the VADB, which is situated on the Data Protector Cell Manager. VADB contains configuration information required for LUN security, instant recovery sessions and security passwords that affect the operation of the HP StorageWorks Virtual Array integration.

LUN security information is contained in the VA LUN exclude file. The VA LUN exclude file is used to specify LUNs, within HP StorageWorks Virtual Arrays connected to a Data Protector cell, that are to be excluded from Data Protector operations. The file contains a list of such LUNs grouped according to the world-wide-name of the Virtual Arrays concerned. LUNs specified in the VA LUN exclude file in this way cannot be accessed by Data Protector for backup and restore purposes and can safely be reserved for other purposes.

The VA LUN exclude file is located on the Cell Manager as follows:

Data_Protector_program_data\db40\vadb\exclude (Windows Server 2008), *Data_Protector_home*\db40\vadb\exclude (other Windows systems), or /var/opt/omni/server/db40/vadb/exclude (UNIX systems).

Other LUN and session information is contained in the VADB, which is also within VADB.

Password information is held within a series of encrypted password files within VADB.

OPTIONS

`-version`

Displays the version of the `omnidbva` command.

`-help`

Displays the usage synopsis for the `omnidbva` command.

`-exclude -put filename`

Sets the list of excluded LUNs by reading the contents of the *filename*, checking its syntax and if the syntax is correct, copying the *filename* to its position on the Cell Manager. If the syntax is not correct, the file is not copied. This command must be used for updating the file. The VA LUN exclude file must not be edited directly.

`-exclude -get filename`

Prepares the VA LUN exclude file for editing by reading the contents of the VA LUN exclude file on the Cell Manager and saving it under *filename*. To update the exclusion list, *filename* must be edited and then used to perform the update using the `-exclude -put filename` command.

`-exclude -check VA_wwn LUN`

Checks whether the specified LUN, identified by its backup system virtual array world-wide-name (*VA_wwn*) and LUN number (*LUN*) is specified in the VA LUN exclude file on the Cell Manager and informs the user.

`-exclude -init`

Overwrites the current VA LUN exclude file on the Cell Manager with the template VA LUN exclude file.

`-exclude -delete`

Deletes the contents of the VA LUN exclude file on the Cell Manager.

`-init[-force]`

Reinitializes (deletes all entries) from the VADB (but will not delete any allocated LUNs). Unless the `-force` option is given, the user will be asked for a confirmation.

`-delete session_id [-force]`

Deletes a session from the VADB (both the disks and the database entries). If `-force` is specified, the command will try to delete the session without any consistency checks.

`-session[session_id]`

Displays available ZDB-to-disk and ZDB-to-disk+tape sessions (instant recovery enabled) within the database. If a *session_id* is specified, expanded details of the session will be displayed. If required, a range of session IDs can be specified.

`-lun[LUN]`

Displays LUN (disk) information about the available VADB objects. If a *LUN* is specified, detailed information for only that *LUN* is displayed.

`-vapasswd VA_wnn password`

Sets the access password for the Virtual Array node identified by its virtual array world-wide-name (*VA_wnn*). If Secure Manager is set ON for the Virtual Array node concerned, the password for the Virtual Array node must be specified using this command.

`-sampasswd SAM_server_ID user password`

Sets the HP Allocator access password. If a SAN network is being used, with HP Allocator installed, this password must be supplied using this command. Refer to the HP Allocator documentation for further information.

`-dbcheck [-force]`

Performs a consistency check of the VADB, and offers to fix invalid entries if necessary. If *-force* is specified, the VADB will be checked/fixed without any interactive prompts.

NOTES

The `omnidbva` command is available on HP-UX, Solaris, and Windows systems only.

The information within the VADB must be edited using the supplied tools. It must not be edited directly.

EXAMPLES

1. To set or change the VA LUN exclude file:

Use the following command on the application or backup system:

```
omnidbva -exclude -get c:/tmp/filename.txt
```

This command reads the VA LUN exclude file from the Cell Manager and saves it in the "c:\tmp\filename.txt" file.

Edit the `c:\tmp\filename.txt` file and save it when you are done editing.

Use the following command on the application or backup system:

```
omnidbva -exclude -put c:\tmp\filename.txt
```

This command reads the contents of the "c:\tmp\filename.txt", checks its syntax and if the syntax is correct copies the file to its position on the Cell Manager.

2. To check whether the LUN number "123" in the virtual array with world_wide-name "Abcde12345" is specified in the VA LUN exclude file, run:
`omnidbva -exclude -check Abcde12345 123`
3. To list all available ZDB-to-disk and ZDB-to-disk+tape sessions in the VADB, run:
`omnidbva -session`

SEE ALSO

`omnidb(1M)`, `omnidbcheck(1M)`, `omnidbinit(1M)`, `omnidbrestore(1M)`, `omnidbsmis(1)`, `omnidbupgrade(1M)`, `omnidbutil(1M)`, `omnidbvss(1)`, `omnidbxp(1)`

omnidbvss

queries the VSS database (VSSDB); browses, lists, saves, removes, and manages the items of the VSSDB

(this command is available on systems with the Data Protector User Interface component installed)

omnidbvss

SYNOPSIS

```
omnidbvss -version | -help
omnidbvss -init
omnidbvss -list session [-barlist BackupSpecName]
omnidbvss -list session_persistent [-barlist BackupSpecName]
[-older_than YYYY/MM/DD]
omnidbvss -get session {sessionID [SessionID ...] | -barlist
BackupSpecName | -all} [-detail] [-save_metadata Directory]
omnidbvss -get session_persistent {sessionID [SessionID ...] |
-barlist BackupSpecName [-older_than YYYY/MM/DD] | -all [
-older_than YYYY/MM/DD]} [-save_metadata Directory]
omnidbvss -remove session {sessionID [SessionID ...] | -barlist
BackupSpecName | -all} [-force] [-reference]
omnidbvss -remove session_persistent {sessionID [SessionID ...]
| -barlist BackupSpecName [-older_than YYYY/MM/DD] | -all
[-older_than YYYY/MM/DD]}
omnidbvss -disable session {sessionID [SessionID ...] | -barlist
BackupSpecName | -all} [-force [-backhost AlternativeBackupSystem]]
omnidbvss -enable session {sessionID [SessionID ...] | -barlist
BackupSpecName | -all} -backhost BackupSystem -mnttarget Mount-
Point [-no_session_id] [-readwrite] [-force]
omnidbvss -resolve {-apphost ApplicationSystem | -all}
```

DESCRIPTION

The `omnidbvss` command is used to query the VSSDB.

This command can be used to:

- list all available backup sessions (ZDB-to-disk, ZDB-to-disk+tape, and ZDB-to-tape)
- view information about a specific or all available backup sessions
- view details about a specific or all available ZDB-to-disk and ZDB-to-disk+tape sessions

- save backup components and writer metadata documents
- remove a specific or all available ZDB-to-disk and ZDB-to-disk+tape sessions, together with their replicas, from the VSSDB and from the disk array
- remove a reference to a specific or to all available backup sessions from the VSSDB
- disables the specified or all ZDB-to-disk or ZDB-to-disk+tape sessions
- enables the specified or all ZDB-to-disk, ZDB-to-disk+tape sessions
- initialize the VSSDB
- resolve the application systems in the Data Protector VSS integration cell.

OPTIONS

`-version`

Displays the version of the `omnidbvss` command.

`-help`

Displays the usage synopsis for the `omnidbvss` command.

`-init`

Initializes the VSSDB.

IMPORTANT: All data including sessions and created replicas is deleted from the VSSDB.

`-list session [-barlist barlist]`

Queries the VSSDB and lists all ZDB-to-disk and ZDB-to-disk+tape session IDs. If `-barlist` is specified, only the IDs of the ZDB-to-disk and ZDB-to-disk+tape sessions that were created using the backup specification are listed.

`-list session_persistent [-barlist barlist] [-older_than YYYY/MM/DD]`

Queries the VSSDB and lists all available backup session (ZDB to disk, ZDB to disk+tape, and ZDB to tape) IDs.

If `-barlist` is specified, only the IDs of the sessions that were created using the backup specification are listed.

If `-older_than` is specified, only the sessions IDs that were created before the specified date are listed.

`-get session {SessionID [SessionID...] -barlist BackupSpec-Name|-all}`

`[-detail] [-save_metadata Directory]`

Displays information about the ZDB-to-disk and ZDB-to-disk+tape sessions.

By specifying *SessionID*, the `-barlist`, or the `-all` option, information about the backup components and disks about the sessions that match the given criteria will be displayed.

`-detail` displays detailed information (components, disks) about the specified session.

`-save_metadata` saves the backup components document (Backup Components Document.xml) and writer metadata document (*writer_name.xml*) to the specified directory.

```
-get session_persistent {SessionID [SessionID...]|-barlist  
BackupSpecName
```

```
[-older_than YYYY/MM/DD]|-all [-older_than YYYY/MM/DD]}  
[-save_metadata Directory]
```

Displays information about any backup session created using VSS software or the hardware provider.

By specifying *SessionID*, the `-barlist`, or the `-all` option, information about the sessions that match the given criteria will be displayed.

`-older_than` displays information about the backup sessions, specified with the `-barlist` option, or all sessions that were created before the specified date.

`-save_metadata` saves the backup components document (Backup Components Document.xml) and writer metadata document (*writer_name.xml*) to the specified *directory*.

```
-remove session {SessionID [SessionID...]|-barlist  
BackupSpecName|-all}
```

```
[-force] [-reference]
```

Removes the specified ZDB-to-disk or ZDB-to-disk+tape sessions and their replicas from the VSSDB (non-persistent metadata) and disk array.

By specifying the *SessionID*, `-barlist`, or `-all` option, the information about the sessions that match the given criteria will be deleted from the VSSDB and the session's replicas will be deleted from the disk array.

If `-reference` is specified, only the reference information about the specified sessions and their replicas will be removed from the database. This option can be used to remove an entry that points to a replica that no longer exists.

The removing operation fails in the following cases, unless the `-force` option is used:

- If you have changed the disks' configuration manually after the backup (for example, the sessions target volumes were presented manually to some other system).

— If the target volumes cannot be unmounted because of a lock by some other process.

```
-remove session_persistent {SessionID [SessionID...]|-barlist  
BackupSpecName [-older_than YYYY/MM/DD]|-all [-older_than  
YYYY/MM/DD]}
```

Removes the reference information about the specified sessions from the VSSDB (persistent metadata). It does not remove the session's replicas from the disk array.

By specifying the *SessionID*, *-barlist*, or *-all* option, information about the sessions that match the given criteria will be removed.

-older_than removes the reference information about the backup sessions, specified by the *-barlist* option, or all sessions, that were created before the specified date.

```
-disable session {SessionID [SessionID...]|-barlist  
BackupSpecName|-all}
```

```
[-force [-backhost AlternativeBackupSystem]]
```

Disables the specified ZDB-disk or ZDB-to-disk+tape sessions (if *SessionID* is used), sessions created by the specified backup specification (if *-barlist* is used), or all sessions (if *-all* is used). Disabling means that the replicas (target volumes) created in the specified sessions or using the specified backup specification are unmounted and unrepresented from the backup system.

The disabling operation fails in the following cases, unless the *-force* option is used:

— If you have changed the disks' configuration manually after the backup (for example, the sessions target volumes were presented manually to some other system).

— If the target volumes cannot be unmounted because of a lock by some other process.

Use *-force -backhost AlternativeBackupSystem* if the backup system from which you want to disable a backup session is not available.

AlternativeBackupSystem specifies an alternative client system (any client in the Data Protector cell that has the VSS integration component installed), from which the session will be disabled by force.

```
-enable session {SessionID [SessionID...]|-barlist  
BackupSpecName|-all}
```

```
-backhost BackupSystem -mnttarget MountPoint  
[-no_session_id] [-readwrite] [-force]
```


Enables the specified ZDB-disk or ZDB-to-disk+tape sessions (if *SessionID* is used), or sessions created by the specified backup specification (if *-barlist* is used), or all sessions (if *-all* is used). Enabling means that the replicas (target volumes) created in the specified sessions or using the specified backup specification are presented and mounted to the specified backup system.

-backhost specifies the target client system where you want the target volumes to be presented.

-mnttarget specifies the directory on the *BackupSystem* where you want the target volumes to be mounted. By default, a new directory with the session ID is created in the specified directory and the disks are mounted there. If *-no_session_id* is used, the disks are mounted to the specified directory. Use *-no_session_id* only when mounting disks from only one backup session.

The enabling operation fails in the following cases, unless the *-force* option is used:

- When *-no_session_id* is used and another disk is already mounted in the specified directory.
- If the session to be enabled is already enabled on another backup system.
- If you have changed the disks' configuration manually after the backup.

If you use the *-force* option to enable disks on your specified system even if they are already specified on some other system, note that the disks will not be unmounted on the other system and you will need to clean the environment manually.

By default, the disks are mounted in read-only mode. If *-readwrite* is specified, the disks will be mounted in read/write mode.

-resolve {-apphost ApplicationSystem|-all}

Resolves the specified application system (if *-apphost* is used) or all application systems (if *-all* is used) in the Data Protector cell.

The command applies only to instant recovery-enabled backup sessions and must be run always after:

- installing or upgrading Data Protector
- your source volumes configuration on the application system has changed (for example, you have modified the existing source volumes or you have presented new source volumes)
- you have added a new storage object (for example, a Microsoft Exchange Server storage group)

For more information, see the *HP Data Protector zero downtime backup integration guide*.

EXAMPLES

1. To list the instant recovery-enabled sessions (ZDB to disk or ZDB to disk + tape) created using the backup specification "Backup1", run:

```
omnidbvss -list session -barlist Backup1
```

2. To get information about the backup components of all backup sessions created before February 1st, 2009, and to save information about the backup components and writer metadata to the directory "C:\metadata", run:

```
omnidbvss -get session_persistent -all older_than  
2009/02/01 -save_metadata C:\metadata
```

Note that the specified directory must exist before you run the command.

3. To remove the reference information about the sessions "2009/02/11-1" and "2009/02/11-2" from the VSSDB and to remove the associated replicas from the disk array, run:

```
omnidbvss -remove session 2009/02/11-1 2009/02/11-2
```

4. To mount the target volumes from the session "2009/02/15-1" in the directory "C:\mnt\", present them on the client system "backupsys", and to leave the volumes mounted in read/write mode, run:

```
omnidbvss -enable session 2009/02/15-1 -backhost backupsys  
-mnttarget C:\mnt -readwrite
```

Note that a new directory with the session ID is created and that the target volumes are mounted in the directory "C:\mnt\2009-02-15-1".

SEE ALSO

omnidb(1M), omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1), omnidbupgrade(1M), omnidbutil(1M), omnidbva(1), omnidbvp(1)

omnidbxbp

queries the ZDB database (XPDB), manipulates the XP LDEV exclude file, and configures the HP StorageWorks Disk Array XP command devices usage (this command is available on systems with the Data Protector User Interface component installed)

omnidbxbp

SYNOPSIS

```
omnidbxbp -version | -help
omnidbxbp -exclude {-put filename | -get filename | -check SEQ LDEV
| -init | -delete}
omnidbxbp [-ir] -session {-list | -show sessionID}
omnidbxbp [-ir] -ldev {-list | -show SEQ LDEV}
omnidbxbp -cm {-add serial {CU:LDEV | LDEV}hostname [instance] |
```

-update *serial* {*CU:LDEV* | *LDEV*}*hostname* [*instance*]}
omnidbxbp -cm -remove {all | *serial* [{*CU:LDEV* | *LDEV*] [*hostname*]}}
omnidbxbp -cm -list

DESCRIPTION

The following tasks can be performed using the omnidbxbp command:

QUERYING THE INFORMATION ON BACKUP OBJECTS AND MANIPULATING THE LDEV EXCLUDE FILE

The omnidbxbp command can be used to query the information stored in the ZDB database (XPDB), which stores the information about the LDEVs pairs and their mirror configurations during the Data Protector HP StorageWorks Disk Array XP backup and restore sessions. The XPDB is a set of ASCII files stored on the Cell Manager in the directory *Data_Protector_program_data\db40\xpdb* (Windows Server 2008), *Data_Protector_home\db40\xpdb* (other Windows systems), or */var/opt/omni/server/db40/xpdb* (UNIX systems). The XPDB contains data about the split P-VOL - S-VOL pairs used with the Data Protector HP StorageWorks Disk Array XP integration in a set of XPDB records. The XPDB is written to whenever a pair is split using the Data Protector HP StorageWorks Disk Array XP integration. A pair is deleted from the XPDB whenever such a pair is resynchronized using the Data Protector HP StorageWorks Disk Array XP integration.

The omnidbxbp command can also be used to manipulate the XP LDEV exclude file. The XP LDEV exclude file enables disabling of using certain LDEVs on the backup system (S-VOL LDEVs) by Data Protector. Thus, it is possible to reserve certain LDEVs

for other purposes than Data Protector backup and restore. The disabled LDEVs are, if used in a Data Protector session, ignored by Data Protector and such a session fails with critical error. The list of disabled LDEVs is kept in the XP LDEV exclude file on the Cell Manager:

Data_Protector_program_data\db40\exclude\XPexclude (Windows Server 2008), *Data_Protector_home\db40\exclude\XPexclude* (other Windows systems), or
/var/opt/omni/server/db40/xpdb/exclude/XPexclude (UNIX systems).

The `omnidbxp` options to be used for querying the XPDB and manipulating the XP LDEV exclude file are: `-exclude`, `-put`, `-get`, `-check`, `-init`, `-delete`, `-session`, `-list`, `-show`, `-ir`, `-ldev`, `-show`.

HP StorageWorks DISK ARRAY XP COMMAND DEVICE HANDLING

The HP StorageWorks Disk Array XP command devices are needed by any process that needs access to the HP StorageWorks Disk Array XP. The information about HP StorageWorks Disk Array XP command devices is kept in the XPDB for the purpose of eliminating duplicate instance usage and over-allocation. Data Protector provides the following mechanism to prevent duplicate instance usage and over allocation:

1. Whenever a session is started, Data Protector queries the XPDB for a list of command devices. If there is none in the XPDB (default behavior when the first session is started), Data Protector identifies command devices and generates a list of command devices in the XPDB as connected to every application and backup system in the cell.
2. Every command device is assigned an instance number (starting from 301) and the system (hostname) having access to it. If a command device can be accessed from more than one system, the hostname identifier enables Data Protector to be aware of the fact that the command device is already meant to be used by some other system; next available instance number is assigned to such a command device - hostname combination
3. When the list is created, every HP StorageWorks Disk Array XP attached to application and backup systems has a list of its command devices and systems having access to them (together with an instance number) assigned.
4. Whenever during a session an application or backup system needs access to an HP StorageWorks Disk Array XP, it uses the first assigned command device with the instance number from the list. If the command device fails, the next command device from the list assigned to a particular system is used. If all of them fail, the session fails. The successful command device is used by a particular system until the end of the session and the list of command devices is used for all consecutive sessions.

Using the `omnidbxp` command, it is possible to:

1. Specify a particular command device (identified by the HP StorageWorks Disk Array XP serial number and LDEV number) to be used by a particular system. Optionally, an instance number can be assigned too. If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number. The entire information is written in the XPDB.
2. List all command devices in the XPDB.
3. Remove a specific or all command devices from the XPDB or update the information about a specific command device in the XPDB.

The `omnidbxbp` options to be used for command device handling begin with the `-cm` option and are: `-add`, `-update`, `-remove` and `-list`.

OPTIONS

`-version`

Displays the version of the `omnidbxbp` command

`-help`

Displays the usage synopsis for the `omnidbxbp` command.

`-exclude -put filename`

Sets the list of excluded LDEVs by reading the contents of the *filename*, checking its syntax and if the syntax is correct, copying the file to its position on the Cell Manager. If the syntax is not correct, the file is not copied.

`-exclude -get filename`

Prepares the XP LDEV exclude file for editing by reading the contents of the XP LDEV exclude file on the Cell Manager and saving it under the *filename*.

`-exclude -check SEQ LDEV`

Checks whether the specified LDEV, identified by its backup system disk array serial/sequence number (*SEQ*) and LDEV number (*LDEV*) is specified in the XP LDEV exclude file on the Cell Manager. The LDEV number must be specified as the *CU#*:*LDEV* in decimal format. If the queried LDEV is specified in the XP LDEV exclude file, the command returns: YES! If the queried LDEV is not specified in the XP LDEV exclude file, the command returns: NO!

`-exclude -init`

Overwrites the current XP LDEV exclude file on the Cell Manager with the template XP LDEV exclude file.

`-exclude -delete`

Deletes the contents of the XP LDEV exclude file on the Cell Manager.

`-ir`

Specifies that the current `omnidbxp` command is executed only for the LDEVs pairs marked for the instant recovery in the XPDB. If this option is not specified, the current command is executed for all LDEVs pairs in the XPDB.

`-session -list`

Lists all available sessions in the XPDB.

`-session -show sessionID`

Lists all backup system S-VOL LDEVs that were involved in the session with the *sessionID*.

`-ldev -list`

Lists all S-VOL LDEVs in the XPDB together with their corresponding backup sessionID.

`-ldev -show SEQ LDEV`

Lists all available XPDB information about the specified S-VOL *LDEV*. The following information is listed: sessionID, CRC, IRflag, primary XP #, primary LDEV #, primary port #, mirror type, MU#, date and time, application system and backup system hostnames.

`-cm -add serial {CU:LDEV | LDEV} hostname [instance]`

Adds the command device identified by the serial number of the HP StorageWorks Disk Array XP (*serial*) and serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) to the XPDB, and assigns it the hostname of the system accessing it (*hostname*) and optionally the instance number (*instance*). If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number.

The instance number must be any number in the range between 301 and 399.

The command does not check whether the specified command device or system exist, it only checks if the optional instance number specified is within the correct range and if the command device together with the instance number is not already assigned to be used by some other system. If checks fail, the command fails with an appropriate error message.

`-cm -update serial {CU:LDEV | LDEV} hostname [instance]`

Updates the XPDB information about the command device identified by the serial number of the HP StorageWorks Disk Array XP (*serial*), serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) and the specified hostname of the system accessing it (*hostname*), by assigning the newly specified instance number (*instance*) to the HP StorageWorks Disk Array XP serial number, serial number of command device and hostname combination. If the instance number is not specified, Data Protector assigns the lowest not yet assigned instance number.

The instance number must be any number in the range between 301 and 399.

The command does not check whether the specified command device or system exist, it only checks if the optional instance number specified is within the correct range and if the command device together with the instance number is not already assigned to be used by some other system. If the checks fail, the command fails with an error message.

`-cm -remove all`

Removes the information about all command devices from the XPDB.

`-cm -remove serial [{CU:LDEV | LDEV} [hostname]]`

If only the *serial* argument is specified, the command removes the information about command devices within a specific HP StorageWorks Disk Array XP identified by the serial number of this HP StorageWorks Disk Array XP (*serial*) from the XPDB.

If the *CU:LDEV | LDEV* and optionally *hostname* arguments are specified as well, the command removes the information about the command device identified by the serial number of the HP StorageWorks Disk Array XP (*serial*), serial number of command device in the hexadecimal or decimal format (*CU:LDEV* or *LDEV*) and optionally by the hostname of the system (*hostname*).

When removing the information about the command device without specifying the system (*hostname*), the command deletes all entries for the specified command device, regardless of the system(s) assigned to it.

`-cm -list`

Lists all command devices in the XPDB.

NOTES

The `omnidbxp` command is available on HP-UX, Solaris, and Windows systems only.

EXAMPLES

1. To set or change the XP LDEV exclude file:
 - a.) Use the following command on the application or backup system:
`omnidbxp -exclude -get c:\tmp\filename.txt`
This command reads the XP LDEV exclude file from the Cell Manager and saves it in the "c:\tmp\filename.txt" file.
 - b.) Edit the `c:\tmp\filename.txt` file and save it when you are done editing.
 - c.) Use the following command on the application or backup system:

This command reads the contents of the "c:\tmp\filename.txt", checks its syntax and if the syntax is correct, copies the file to its position on the Cell Manager.

```
omnidbexp -exclude -put c:\tmp\filename.txt
```

2. To check whether the LDEV identified by the serial number "12345" and LDEV number "123" is specified in the XP LDEV exclude file, execute the following command:

```
omnidbexp -exclude -check 12345 2864
```

3. To list all backup system LDEVs, regardless of they being marked for instant recovery or not, that were involved in the session with the sessionID "2007/09/18-22", run:

```
omnidbexp -session -show 2007/09/18-22
```

4. To list all command devices in the XPDB, run:

```
omnidbexp -cm -list
```

5. To add the command device identified by the HP StorageWorks Disk Array XP serial number "00035371" and command device serial number "103" to the XPDB and assign it to be used on the "computer.company.com" system by the instance number "303", run:

```
omnidbexp -cm -add 00035371 103 computer.company.com 303
```

6. To remove the information about all command devices from the XPDB, run:

```
omnidbexp -cm -remove all
```

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1), omnidbupgrade(1M), omnidbutil(1M), omnidbva(1), omnidbvss(1)

omnidownload

downloads information about a backup device and a library from the Data Protector internal database (IDB)

(this command is available on systems with the Data Protector User Interface component installed)

omnidownload

SYNOPSIS

```
omnidownload -version | -help
omnidownload -list_devices [-detail]
omnidownload -dev_info
omnidownload -device BackupDevice [-file FileName]
omnidownload -list_libraries [-detail]
omnidownload -library Library [-file FileName]
```

DESCRIPTION

Allows the user to display information about backup devices or download the configuration of the specified backup device to an ASCII file. Used together with the `omniupload` utility, this command enables you to create and maintain backup devices using the Command-Line Interface.

OPTIONS

`-version`

Displays the version of the `omnidownload` command.

`-help`

Displays the usage synopsis for the `omnidownload` command.

`-device BackupDevice`

Specifies the name of the backup device you want to download to an ASCII file.

`-library Library`

Specifies the name of the library you want to download to an ASCII file.

`-file FileName`

Specifies the name of the target ASCII file for the backup device. By default, the file is created in the local directory. If this option is omitted, the data is sent to the standard output.

`-list_devices`

Displays information about the Data Protector backup devices. The report includes the following information for each device: device name, client, device type and pool.

`-dev_info`

Same as `-list_devices` option. Used only for compatibility with old Data Protector releases.

`-list_libraries`

Displays information about the Data Protector libraries. The report includes the following information for each device: library name, client and library type.

`-detail`

This option can be used in combination with the `-list_devices` and `-list_libraries` options to display more detailed information about the Data Protector backup devices or libraries.

EXAMPLES

This example downloads backup device "DAT1" into file "/tmp/DAT1":

```
omnidownload -device DAT1 -file /tmp/DAT1
```

SEE ALSO

`omniamo(1)`, `omnimcopy(1)`, `omniminit(1)`, `omnimlist(1)`, `omnimmm(1)`, `omnimnt(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`, `uma(1M)`

omniiso

primarily serves as a pre-exec script to prepare the ISO image file for One Button Disaster Recovery (OBDR); can also be used as a standalone command to automate your backup and disaster recovery process
(this command is available on systems with the Data Protector Automatic Disaster Recovery component installed)

omniiso

SYNOPSIS

```
omniiso -version | -help  
omniiso [-session SessionID] [-cd] [-iso Path] [-srd Path] [-rset  
plsPath DRImagePath] [-autoinject ] [-waik WaikPath] [-in-  
ject_drivers Path1 [Path2...]]
```

DESCRIPTION

The `omniiso` command can be used as a:

STANDALONE COMMAND

Although all functionality of the command is also available through the Disaster Recovery Wizard in the Data Protector GUI, it can also be used as a standalone command to automate your backup and disaster recovery process.

The command merges

- the DR image (the data required for temporary DR OS installation and configuration that is created during a full client backup),
- the SRD file (a file that contains all required backup and restore object information to perform the restore),
- and the P1S file (a file that contains information on how to format and partition all disks installed in the system)

with disaster recovery installation into a disaster recovery ISO image and saves the ISO image to a file on disk. By default, the ISO image file is created in the directory `Data_Protector_program_data\tmp` (Windows Vista and Windows Server 2008) or `Data_Protector_home\tmp` (other Windows systems). The ISO image can later be written to a tape or CD-ROM and used to perform disaster recovery.

Such ISO image can also be created using the OBDR Wizard in the Data Protector GUI instead of using this command (recommended).

PRE-EXEC SCRIPT

If the command is used as a pre-exec script in the OBDR Wizard in Data Protector GUI to prepare the disaster recovery ISO image, you do not have to specify any parameters, because they are obtained from the current environment.

OPTIONS

`-version`

Displays the version of the `omniiso` command.

`-help`

Displays the usage synopsis for the `omniiso` command.

`-session SessionID`

Specifies the ID of the session that serves as the basis for the object update. All objects, backed up in the specified session and included in the SRD file, will be included in the ISO image.

`-cd`

If this option is specified, `omniiso` creates an ISO file that can be written to a CD-ROM. If this option is not specified, the command creates disaster recovery ISO file to be written on a tape.

`-iso Path`

Specifies the location where the disaster recovery ISO image file is created. If this option is not specified, the ISO image file is created in the directory `Data_Protector_program_data\tmp` (Windows Vista and Windows Server 2008) or `Data_Protector_home\tmp` (other Windows systems).

`-srd Path`

Specifies the path to the SRD file. If the `-srd` option is not specified, the command creates a SRD file on the system, where `omniiso` is running and uses it to create the disaster recovery ISO image.

`-rset pls_Path DR_Image_Path`

Specifies the full path to the PIS file and the DR image. If this option is not specified, the command creates the PIS file and the DR image on the system, where `omniiso` is running and uses them to create the disaster recovery ISO image.

`-autoinject`

Automatically injects drivers into the DR OS image.

This option is available only for Windows Vista and Windows Server 2008.

`-waik WAIKPath`

Specifies the Windows Automated Installation Kit (WAIK) directory.

This option is available only for Windows Vista and Windows Server 2008.

`-inject_drivers Driver1Path [Driver2Path ...]`

Injects additional drivers into the DR OS image. You must specify a full path to the driver. A maximum of 50 paths can be specified.

This option is available only for Windows Vista and Windows Server 2008.

NOTE

The `omniiso` command is available on Windows systems only.

EXAMPLES

The following examples illustrate how the `omniiso` command works.

1. To create and save a disaster recovery ISO file for a CD-ROM in "C:\iso\dr\omnidr.iso", containing objects backed up in the session with the session ID "2008/08/16-23", using information stored in the SRD and PIS files stored in "C:\iso\dr\srd\machine101.company.com" and "C:\iso\dr\pls\machine101.company.com", using DR Image stored in "C:\iso\dr\img\machine101.company.com.img", run:

```
omniiso -session 2008/08/16-23 -cd  
-iso c:\iso\dr\omnidr.iso  
-srd C:\iso\dr\srd\machine101.company.com  
-rset C:\iso\dr\pls\machine101.company.com  
C:\iso\dr\img\machine101.company.com.img
```

2. To create and save a Windows Vista or Windows Server 2008 disaster recovery ISO file for a CD-ROM in "C:\iso\dr\omnidr.iso", containing objects backed up in the session with the session ID "2008/03/22-23", using information stored in the SRD and PIS files stored in "C:\iso\dr\srd\machine102.company.com" and "C:\iso\dr\pls\machine102.company.com", using DR Image stored in "C:\iso\dr\img\machine102.company.com.img" where the drivers are automatically injected, run:

```
omniiso -session 2008/03/22-23 -cd  
-iso C:\iso\dr\omnidr.iso  
-srd C:\iso\dr\srd\machine102.company.com  
-rset C:\iso\dr\pls\machine102.company.com  
C:\iso\dr\img\machine102.company.com.img -autoinject
```

SEE ALSO

`omnidr(1M)`, `omniofflr(1M)`, `omnisrupdate(1M)`

omnimcopy

makes a copy of a Data Protector medium using Data Protector backup devices as the source and destination

(this command is available on systems with the Data Protector User Interface component installed)

omnimcopy

SYNOPSIS

```
omnimcopy -version | -help
omnimcopy -copy BackupDevice [-slot Slot...] -from BackupDevice
[-src_slot Slot...] [BasicOptions] [LabelOptions]
omnimcopy -ams [-from VLS_SMART_COPY -src_slot SourceTapeBarcode]
[-copy VirtualTapeLibrary] [-slot TargetTapeBarcode] [-pool Pool-
Name BasicOptions] [LabelOptions]
```

BasicOptions

```
-pool PoolName
-location Location
-force
-size SpecSize
-encrypt
-eject
-permanent | -until Date
Date = [YY]YY/MM/DD (1969 < [YY]YY < 2038)
```

LabelOptions

```
-label UserLabel [-no_barcode_as_label] | -autolabel |
-[no_]barcode_as_label
```

DESCRIPTION

The `omnimcopy` copies a Data Protector medium. It reads data from the input medium and writes the data to the output medium. Note that the output medium is first initialized. During initialization, a medium is assigned a:

- Data Protector Medium Label: Depending on the selected options, the media labels can be user defined or generated automatically. By default, Data Protector automatically generates media labels from the media pool names, unless the `Use barcode as media label during initialization` option is selected in the library properties. This behavior can be changed during the initialization

of media using `-barcode_as_label`, `-no_barcode_as_label` and `MediumLabel` options.

- Medium ID (system-assigned)
- Location

The physical devices used for the input and output must be the same device type and have the same block size.

This copy functionality allows the user to use multiple tapes in order to implement vaulting with Data Protector. This copy function is a separate function within Data Protector and cannot be done automatically during backup. Main advantage of this implementation is that all devices can be used during backup (better performance).

The source and destination devices are backup devices which means they can be located everywhere in the Data Protector cell. During the copy the destination tape will be initialized before all data from the source tape is copied.

The writing destination tape will ignore the early end of tape mark and will write until the physical EOT is reached. If the space on the destination is not sufficient to keep the whole original tape the copy has to be restarted with a new tape.

After a copy operation both media are tracked in the media management database.

This enables also a listing of the copies for an original media as well as the listing of the original tape for a copy. If a mount request is issued during a restore session all tapes which contains the data will be listed (original and copies).

After the operation copy both tapes become nonappendable.

A copy of a copy is not possible.

If the original media get obsolete in the database, which means it is overwritten or it is exported from the cell, the first copy becomes automatically the original tape.

The `omnimcopy` command can also be used to perform VLS smart media copies. Data Protector adds its own media header to the copies on the target media thus allowing to distinguish between the source and the target medium.

OPTIONS

`-version`

Displays the version of the `omnimcopy` command

`-help`

Displays the usage synopsis for the `omnimcopy` command

`-copy BackupDevice [-slot Slot...]`

Specifies the output backup device - the device used to create a copy of the medium (target medium). You can specify only one slot. For VLS smart copies, the output backup device is the name of the VTL that will be used for automigration. The `-slot` parameter takes the barcode value of the target tape.

`-from BackupDevice [-src_slot Slot...]`

Specifies the input backup device — the device which is used as a source. You can specify only one slot. The `-src_slot` parameter takes the barcode value of the source tape.

`-ams`

Specifies that the VLS smart copy is to be created.

`-from VLS_SMART_COPY`

Specifies that VLS is the input backup device.

`-src_slot SourceTapeBarcode`

Specifies the barcode of the source tape.

`-copy VirtualTapeLibrary`

Specifies the name of the VTL used for automigration.

`-slot TargetTapeBarcode`

Specifies the barcode of the target tape.

`-pool PoolName`

Specify the poolname to which the copy of the medium is added. By default the medium is added to the source media poolname. This option is mandatory if the `-ams` option is specified, since no devices exist where a default pool can be derived from.

`-location Location`

Specifies the location of the media, when you keep them out of the library. Used for the vaulting purposes.

`-force`

Overwrites the data on the target medium even if this data is still protected by the Data Protector media management system. Note that this option must be used with an unprotected medium as well.

`-size SpecSize`

This option specifies the size of the target medium.

`-encrypt`

This option turns on hardware encryption on all destination drives.

`-eject`

Ejects the target medium from the drive after the medium is copied.

`-permanent`

This backup protection option provides permanent protection of backup media. This means that the data is permanently protected from being overwritten.

`-until Date`

This backup protection option provides protection until a date of your choice. This means that the data on the medium cannot be overwritten until the specified date. Protection for the data stops at noon on the selected day.

`-label UserLabel`

Manually specify the medium label for the copy of the medium. A description can have a maximum of 80 characters, including any keyboard character or space. If the `Use barcode as medium label on initialization` option is selected in the library properties, you have to specify also the `-no_barcode_as_label` option.

`-autolabel`

If this option is specified, the medium is labeled automatically by the Data Protector media management system.

`-barcode_as_label`

Data Protector uses barcode as a medium label during the initialization of the medium instead of generating media labels based on the media pools names. This option is supported only on library devices with enabled barcode support.

`-no_barcode_as_label`

Data Protector does not use barcodes as a medium label during the initialization of the medium, but generates media labels based on the media pools names. This option can be used to override the `Use barcode as medium label on initialization` option (if it is selected) in the library properties in the Data Protector GUI.

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omniminit(1)`, `omnimlist(1)`, `omnimm(1)`, `omnimnt(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`, `uma(1M)`

omniminit

initializes a Data Protector medium

(this command is available on systems with the Data Protector User Interface component installed)

omniminit

SYNOPSIS

```
omniminit -version | -help
omniminit -init BackupDevice [MediumLabel] [BasicOptions] [SlotOptions]
[-no_barcode_as_label]
omniminit -init BackupDevice [BasicOptions] [SlotOptions] [-barcode_as_label]
omniminit -init_magazine BackupDevice [MagazineDescription] [BasicOptions]
omniminit -init_mag_medium BackupDeviceMagazineDescription
[BasicOptions] [SlotOptions]
omniminit -preerase BackupDevice [SlotOptions] [-eject]
```

BasicOptions

```
-force
-pool PoolName
-size n
-location OffLineLoc
-wipe_on_init
-eject
```

SlotOptions

```
-slot SlotID [Side]
```

DESCRIPTION

The `omniminit` command initializes a backup medium. During initialization, a medium is assigned a:

- **Data Protector Medium Label:** Depending on the selected options, the media labels can be user defined or generated automatically. By default, Data Protector automatically generates media labels from the media pool names, unless the `Use barcode as media label during initialization` option is selected in the library properties. This behavior can be changed during the initialization

of media using `-barcode_as_label`, `-no_barcode_as_label` and `MediumLabel` options.

- Medium ID (system-assigned)
- Location

This information is added to the Data Protector internal database (IDB) and the medium is added to a Data Protector media pool. Medium ID is its unique identifier. The Medium Label does not necessarily have to be unique, but it is recommended. The medium location is optional, and can be used to define an offline location for the medium.

OPTIONS

`-version`

Displays the version of the `omniminit` command.

`-help`

Displays the usage synopsis for the `omniminit` command.

`-init BackupDevice [MediumLabel]`

Specifies two items: the name of the *BackupDevice* where the medium is mounted and the *MediumLabel* which is assigned to the medium by Data Protector after initialization. The *MediumLabel* can be up to 32 characters long. Any printable character, including spaces, can be used. The text must be enclosed in quotation marks.

`-init_magazine BackupDevice [MagazineDescription]`

Specifies two items: the name of the *BackupDevice* where the magazine is mounted and the *MagazineDescription* (optional) which is assigned to the magazine. Note that the *MagazineDescription* must be unique for each magazine. The description is also used for assigning *MediumLabel* to each medium.

`-init_mag_medium BackupDevice MagazineDescription`

Initializes single medium from magazine. *BackupDevice* specifies the device where the magazine is mounted. *MagazineDescription* must also be specified to identify the magazine. Note that single medium from the magazine can be initialized only if the magazine has been initialized before and therefore has a unique *MagazineDescription*.

`-preerase BackupDevice`

Pre-erases the optical disk. Pre-erasing a medium enables backups which are twice as fast. This is because the pre-erase step is removed from the backup

process. For best performance, optical disks should be pre-erased before each backup.

`-force`

Overrides the initialization safety checks. By default, a medium containing protected data or being in a non-Data Protector format cannot be initialized.

`-pool PoolName`

Specifies the name of the media pool to which this medium will be added. If no *PoolName* is specified, the medium is added to the default pool for the specified backup device.

`-slot SlotID [Side]`

Specifies the *SlotID* of the exchanger backup device where the medium is mounted. This option is only valid for this backup device type, but must be given for MO devices. To specify the side of the platter in this slot, use the additional *Side* parameter. Values of *Side* are A or B.

`-size n`

Specifies the medium capacity in MB. If not specified, Data Protector uses the standard capacity of the media class used with the backup device selected for initialization. The size is later used to calculate the free space remaining on the medium. (FreeSpace = Size - SpaceUsed)

`-location OffSiteLoc`

Specifies the location of the medium. This information is useful if media is stored off-site. The location can have maximum 32 characters. Any printable character, including spaces, can be used. The text must be enclosed in quotation marks.

`-wipe_on_init`

Wipes the data on medium after it has been initialized. This is done by overwriting the data on medium so it is impossible to restore the original data on medium after it has been wiped.

`-barcode_as_label`

Data Protector uses barcode as a medium label during the initialization of the medium instead of generating media labels based on the media pools names. This option is supported only on library devices with enabled barcode support.

`-no_barcode_as_label`

Data Protector does not use barcodes as a medium label during the initialization of the medium, but generates media labels based on the media pools names. This option can be used to override the `Use barcode as medium label` on `initializationoption` (if it is selected) in the library properties in the Data Protector GUI.

EXAMPLES

The following examples illustrate how the `omniminit` command works.

1. To init slot "4" of backup device "ADIC" with medium label "Label4", in location "Backup Room", run:

```
omniminit -init ADIC Label4 -slot 4 -location "Backup Room"
```

2. To preerase slot "8" side "A" of MO tape library unit "MO_Changer", run:

```
omniminit -preerase MO_Changer -slot 8 A
```

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omnimcopy(1)`, `omnimlist(1)`, `omnimmm(1)`, `omnimnt(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`, `uma(1M)`

omnimlist

lists the contents of a Data Protector medium
(this command is available on systems with the Data Protector User Interface component installed)

omnimlist

SYNOPSIS

```
omnir -version | -help
omnimlist -device BackupDevice [-slot SlotID [Side]] [-monitor]
[-detail]
omnimlist -device BackupDevice [-slot SlotID [Side]] [-header]
[-monitor]
omnimlist -device BackupDevice -session [-slot SlotID [Side]]
[-monitor] [-detail]
omnimlist -device BackupDevice -session SessionID [-slot SlotID
[Side]] [-monitor] [-detail]
omnimlist -device BackupDevice -catalog [-slot SlotID [Side]]
[-monitor]
omnimlist -device BackupDevice -catalog DiskAgentID [-slot SlotID
[Side]] [-monitor]
```

DESCRIPTION

The `omnimlist` command lists the contents of a Data Protector medium. The command scans the catalog (index) of the medium and shows all objects and sessions on the medium.

The command can also be used to display the Data Protector medium tape header. If used for such purpose, the command reads the first block of the tape and then displays the information.

OPTIONS

`-version`

Displays the version of the `omnimlist` command.

`-help`

Displays the usage synopsis for the `omnimlist` command.

`-device BackupDevice`

Specifies the *BackupDevice* where the medium is mounted. If no other option is specified the command lists all sessions and all their objects.

`-slot SlotID [Side]`

Specifies the *SlotID* of the library where the medium is mounted. This option is only valid for this backup device type, but must be given for MO devices. To specify the side of the platter in this slot, use the additional *Side* parameter. Values of *Side* are A or B.

`-session [SessionID]`

Displays information about the sessions on the medium. If no *SessionID* is specified, all sessions are shown. This reports shows for each session: the *SessionID*, Session Type, Session Status. For the user who initiated the session it shows: the UNIX Login, UNIX Group, and ClientName. If a *SessionID* is specified, the objects for that session are shown. The session report shows for each object: the Client, Mountpoint, Object Label, Disk Agent ID and Object Status.

`-catalog [DiskAgentID]`

Displays the detail catalog for single or multiple objects. The catalog shows file information for all the files included in the backup of the object in that session. The *DiskAgentID* is used to uniquely identify the backup object-session combination. If not specified all found objects are processed.

`-monitor`

Displays information about the Medium (Pool, Medium ID, Medium Label, Location, and Initialization date/time), the Session (Session ID, Owner, Datalist used, and Start date/time), Objects (Type, Start date/time, Backup Mode), and Session (Client, Mountpoint, Object Label, Disk Agent ID, and Object Status).

`-header`

The command first checks if the media header is in Data Protector format and if it is corrupted. If the media header is not in Data Protector format or if it is corrupted, an appropriate message is displayed. Otherwise the following information from the media header is displayed: medium ID, medium label, medium location, initialization date, last access date, last write date, last overwrite date, number of writes, number of overwrites, pool label, device information, device capacity, tape format version, medium ID from original tape (for replicated media only), medium data format type and medium data format subtype. For random access media, date and time information (last access date, last write date and last overwrite date) is updated every time the medium is accessed/written/overwritten. For all other media, header information is not updated except when initializing the medium.

`-detail`

Displays detailed information about the selected query.

NOTES

For the `-header` option, the following limitation applies: the command displays the header information stored on the medium, ignoring possible updates in the Data Protector internal database (IDB).

EXAMPLES

The following examples show how the `omnimlist` command works.

1. To list sessions and corresponding disk agents from device "DAT2", run:

```
omnimlist -device DAT2 -monitor
```
2. To list sessions on slot "43" side "B" of a tape library unit "MO_Changer", run:

```
omnimlist -device MO_Changer -slot 43 B -session
```
3. To list all disk agents for the session "2007/07/13-23" on the device "Exa8500", run:

```
omnimlist -device Exa8500 -session 2007/07/13-23
```
4. To list the catalog for the object-session combination with the DiskAgentID "774226832", from the medium located in slot "7" of device "Herstal2", run:

```
omnimlist -device Herstal2 -slot 7 -catalog 774226832
```
5. To display media header for the medium in the backup device named "dev_1", run:

```
omnimlist -device dev_1 -header
```

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omnimcopy(1)`, `omniminit(1)`, `omnimm(1)`, `omnimnt(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`, `uma(1M)`

omnimm

provides media management for Data Protector
(this command is available on systems with the Data Protector User Interface component installed)

omnimm

SYNOPSIS

```
omnimm -version | -help
omnimm -create_pool PoolName MediaType [Policy AgeLimit MaxOverWrites] [-[no_]alloc_uninit_first] [-[no_]free_pool [FreePoolName]] [-[no_]move_free_media]
omnimm -modify_pool PoolName NewPoolName [Policy AgeLimit MaxOverWrites] [-[no_]alloc_uninit_first] [-[no_]free_pool [FreePoolName]] [-[no_]move_free_media]
omnimm -create_free_pool PoolName MediaType [AgeLimit MaxOverWrites]
omnimm -modify_free_pool PoolName NewPoolName [AgeLimit MaxOverWrites]
omnimm -create_mag_pool PoolName MediaType [Policy AgeLimit MaxOverWrites]
omnimm -modify_mag_pool PoolName NewPoolName [Policy AgeLimit MaxOverWrites]
omnimm -remove_pool PoolName
omnimm -remove_mag_pool PoolName
omnimm -show_pools [PoolName]
omnimm -move_medium Medium ToPoolName
omnimm -move_magazine MagazineDescription NewPoolName
omnimm -modify_medium Medium NewMediumLabel NewLocation
omnimm -modify_magazine MagazineDescription NewLocation [NewMagazineDescription]
omnimm -reset_poor_medium Medium
omnimm -reset_wp_medium Medium
omnimm -list_pool [PoolName] [-detail]
omnimm -show_pool_alloc PoolName
omnimm -list_scratch_media PoolName [-detail]
omnimm -show_repository_alloc Library PoolName [-detail]
omnimm -list_media Medium [-detail | -encryptioninfo]
omnimm -list_appendable_media PoolName
omnimm -list_copy Medium
```

```

omnimm -media_info Medium [-detail | -encryptioninfo]
omnimm -list_magazines_of_pool PoolName [-detail]
omnimm -list_media_magazine MagazineDescription [-detail]
omnimm -catalog Medium
omnimm -check_protection Medium
omnimm -recycle Medium
omnimm -recycle_magazine MagazineDescription
omnimm -export Medium
omnimm -export_magazine MagazineDescription
omnimm -copy_to_mcf {Medium1 [Medium2...]} [-output_directory
Pathname]
omnimm -import LogicalDevice [-slot SlotID [Side]] [-no_log |
-log_dirs | -log_file] [-pool PoolName] [-import_as_original]
omnimm -import_catalog LogicalDevice [-slot SlotID [Side]] [-no_log
| -log_dirs | -log_file]
omnimm -import_magazine LogicalDevice [MagazineDescription] [-slot
SlotID [Side]] [-no_log | -log_dirs | -log_file] [-pool PoolName]
[-import_as_original]
omnimm -import_from_mcf {File1 [File2]...} [-pool_prefix PoolPrefix
| -no_pool_prefix] [-[no_]orig_pool] [-import_as_original]
omnimm -disable_lockname LockName
omnimm -enable_lockname LockName
omnimm -disable_device DeviceName [-ignore_lockname]
omnimm -enable_device DeviceName [-ignore_lockname]
omnimm -repository LibraryName
omnimm -repository_barcode_scan LibraryName
omnimm -repository_update DriveName [-slot SlotID [Side]]
omnimm -add_slots LibraryName {Slot... | FromSlot-ToSlot...}
omnimm -remove_slots LibraryName {Slot... | FromSlot-ToSlot...}
omnimm -silo_query LibraryName [-range FromSlot-ToSlot]
omnimm -silo_enter LibraryName -cap CapID
omnimm -silo_eject LibraryNme {Volser... | FromVolser-ToVolser...}
-cap CapID [-location Location]
omnimm -enter LibraryName {Slot | FromSlot-ToSlot...}
omnimm -eject LibraryName {Slot | FromSlot-ToSlot} [-location
Location]
omnimm -group PoolName MagazineDescription Medium... ..
omnimm -ungroup MagazineDescription
omnimm -reload_serial_number DeviceName
Policy =

```

```

Loose |
Strict |
App+Loose |
App+Strict |
AppIncr+Loose |
AppIncr+Strict

Medium =

Medium_Label|
Barcode|
Medium ID

Basic Options =

-force
-pool PoolName
-size n
-location OffLineLoc
-eject

```

DESCRIPTION

The main purpose of *media management* is to protect valuable user data.

To achieve this goal Data Protector provides the following functionality: protecting data from being overwritten, detecting and tracking bad or old media, utilizing and reporting space in auto changers, use of media within pools, drive cleaning, detecting standard tape and MO format. All this information is stored into the Data Protector internal database.

The `omnimmm` command manages media pools, checks the protection of a medium, maintains and updates the contents of the repository in the library.

Protecting data is more than just stopping Data Protector from overwriting the tape. The detection of an old and poor media informs the administrator before data loss so that he can react before he needs to restore the data and tape will never be used for backups again. This means protection of data which are on Data Protector tapes and protection for data which is still on the system and needs to be backed up.

For the list of supported media classes, refer to the *HP Data Protector product announcements, software notes, and references*.

Data Protector has the concept of *media pools* to manage large numbers of cartridges. Pools are logical collection of cartridges with same common media or

data properties. One pool can only contain media of one type. Data Protector support several media *pool policies* :

- *Loose* (loose, non-appendable); When Data Protector prompts for a medium and loose policy is selected, any medium in the defined pool will be accepted.
- *Strict* (strict, non-appendable); Data Protector decides which medium must be inserted for backup and only this medium will be accepted.
- *App+Loose* (loose, appendable);
- *App+Strict* (strict,appendable);
- *AppIncr+Loose* (loose, appendable for incrementals);
- *AppIncr+Strict* (strict, appendable for incrementals).

OPTIONS

`-version`

Displays the version of the `omnimmm` command

`-help`

Displays the usage synopsis for the `omnimmm` command

`-create_pool PoolName MediaType[Policy AgeLimit MaxOverWrites]`

Creates a new pool with *PoolName* for the medium of *MediaType* with the policy defined by *Policy*. For the list of supported media classes, refer to the *HP Data Protector product announcements, software notes, and references*. Supported policies are: *Loose*, *Strict*, *App+Loose*, *App+Strict*, *AppIncr+Loose* and *AppIncr+Strict*. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

`-[no_]alloc_uninit_first`

Option `-noalloc_uninit_first` sets/resets "Use uninitialized media first" pool policy. This option can be used with *Loose* policy only.

`-[no_]free_pool[FreePoolName]`

If `-free_pool` is set, the pool is linked to the free pool specified with *FreePoolName* in order to share free media. Condition factors are inherited from the free pool. If the `-no_free_pool` is set, the pool is not linked. The default setting is `-no_free_pool`.

`-[no_]move_free_media`

The `-move_free_pool` option can only be set if the `- free_pool` option was set. If `-move_free_media` is set, de-allocation of free media from a regular to a free pool is done automatically. If `-no_move_free_media` is set, there is

no automatic de-allocation of free media. The default setting is
`-no_move_free_media.`

`-modify_pool PoolName NewPoolName [Policy AgeLimit MaxOverWrites]`
 Renames the pool *PoolName* into *NewPoolName*. The *Policy*, *AgeLimit* and *MaxOverWrites* can also be changed. Supported policies are: Loose, Strict, App+Loose, App+Strict, Applncr+Loose and Applncr+Strict. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

`-create_free_pool PoolName MediaType [AgeLimit MaxOverWrites]`
 Creates a new free pool with *PoolName* for the medium of *MediaType*. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

`-modify_free_pool PoolName NewPoolName [AgeLimit MaxOverWrites]`
 Renames the free pool *PoolName* into *NewPoolName*. The *AgeLimit* and *MaxOverWrites* can also be changed. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

`-create_mag_pool PoolName MediaType [Policy AgeLimit MaxOverWrites]`
 Creates pool *PoolName* with magazine support.

`-modify_mag_pool PoolName NewPoolName [Policy AgeLimit MaxOverWrites]`
 Renames the magazine pool *PoolName* into *NewPoolName*. The *Policy*, *AgeLimit* and *MaxOverWrites* can also be changed. *AgeLimit* is set in months. The *MaxOverWrites* is the maximum number of times that the medium can be overwritten. The default is 250 overwrites.

`-remove_pool PoolName`
 Removes the pool specified by *PoolName*.

`-remove_mag_pool PoolName`
 Removes the magazine pool specified by *PoolName*.

`-show_pools [PoolName]`
 Shows media from the specified *PoolName* pool or from all pools if *PoolName* is omitted.

`-move_medium Medium ToPoolName`
 Moves medium from the current pool to the pool specified by *ToPoolName*.

`-move_magazine MagazineDescription NewPoolName`

Moves magazine *MagazineDescription* from the current pool to the pool specified by *NewPoolName*.

`-modify_medium Medium NewMediumLabel NewLocation`

Modifies medium with the specified *Medium*. Note that you should always enter the medium label *NewMediumLabel* and location *NewLocation* in that sequence.

`-modify_magazine MagDescription NewLocation [NewMagDescription]`

Changes the location of the magazine *MagDescription* to *NewLocation*. If *NewMagDescription* is specified, it is assigned to the magazine as a new *MagazineDescription*. Note that each magazine must have a unique *MagazineDescription*.

`-reset_poor_medium Medium`

Resets the media condition factors. Once the medium has expired (its maximum usage criteria), it is marked as *poor* and can no longer be used for backup. This option resets the medium quality status, thus enabling it to be used for backup. You have to be very cautious using this option, because a backup stored on an expired medium might not be recoverable.

`-reset_wp_medium Medium`

Removes the write-protected flag for the specified medium from the MMDB, thus making the medium available for writing.

`-list_pool [PoolName] [-detail]`

Displays all the media from pool *PoolName*. The report shows: medium label, status, location, appendability and protection. Appendability is shown under item FULL. If displayed status under FULL is "YES" then medium is unappendable, otherwise it is appendable. If *PoolName* is not specified, the command lists all the configured media pools. This report shows: pool name, status, media class, the number of media and free space in pool.

`-detail`

Displays information in a more detailed format.

`-show_pool_alloc PoolName`

Displays the sequence in which the media from the specified pool will be used for backup. The report shows: sequence, medium label and location.

`-list_scratch_media PoolName`

Displays media from the specified pool which are not protected and can be used for backup. The report shows sequence, medium label and location.

`-show_repository_alloc Library PoolName`

Displays the order in which the media in the repository of the specified *Library* will be used. The report shows: sequence, medium label, location and slot number.

`-list_media Medium`
 Displays all the objects, their type and their protection status for the medium you specified.

`-list_appendable_media PoolName`
 Displays all appendable media from the specified media pool.

`-list_copy Medium`
 List all copies of the given medium.

`-media_info Medium`
 Displays information on the given medium.

`-encryptioninfo`
 Displays detailed encryption information for objects on the specified medium.

`-list_magazines_of_pool PoolName`
 Lists magazines of the pool *PoolName*.

`-list_media_magazine MagazineDescription`
 Lists all the media in specified magazine.

`-catalog Medium`
 Lists catalog for all object versions located on the specified medium. Only files located on this medium are displayed.

`-recycle Medium`
 Resets the protection of data on medium. The present data can now be overwritten and medium can be used to store new data.

`-recycle_magazine MagazineDescription`
 Recycles all media of specified magazine.

`-export Medium`
 Purges from the database all data associated with the medium and the object versions it contains. This option is used when the medium will no longer be used for backup in this cell. A medium containing protected data cannot be exported.

`-export_magazine MagazineDescription`
 Exports all media of specified magazine.

`-copy_to_mcf Medium`
 Copies media-related catalog data into media container format (MCF) files, which you can transfer to another Cell Manager, thus enabling you to import all media-related information on another Cell Manager where it is then available for browsing. The media-related catalog data are not removed from the original Cell Manager. You can specify one or more media either by medium ID or medium label.

`-output_directory Pathname`
 Specifies the directory where MCF files are stored. You must specify a full path to the files. If not specified, the files are by default copied on the Cell Manager in the directory
Data_Protector_program_data\Config\Server\export\mcf
 (Windows Server 2008),
Data_Protector_home\Config\Server\export\mcf (other Windows systems), or in */var/opt/omni/server/export/mcf* (UNIX systems).

`-import LogicalDevice`
 Imports a medium from a different cell. The medium is put in the default pool of the specified backup device. Information about the new medium is added to the database. Slot side must be specified for MO devices.

`-no_log`
 Used with the `-import` option, this option omits the detail part of the catalog from the import.

`-log_dirs`
 Used with the `-import` option, this option imports only the detail part of the directories.

`-pool PoolName`
 Specifies the name of the pool.

`-import_catalog LogicalDevice`
 Rereads the detail catalog from the specified device into the database, in case this information has been deleted. If the detail catalog for the specified medium already exists in the database, import will fail.

`-import_magazine LogicalDevice [MagazineDescription]`
 Imports a magazine from a different cell. The magazine is put in the default pool of the specified backup device. Information about the new magazine and its media is added to the database.

`-import_from_mcf File`
 Imports one or more MCF files that contain copies of media-related catalog data from the original Cell Manager. You must specify a full path to the file on the current Cell Manager.

`-pool_prefix`
 Specifies an optional prefix for a media pool to which you want to import MCF files with media-related catalog data copies. If this option is not specified, the default prefix "IMPORTED" is used.
 If the `-no_pool_prefix` option is set, no prefix is generated for a pool.

`-[no_]orig_pool`

Specifies a media pool for import. By default, the `-orig_pool` option is set. It can be disabled with the `-[no_]orig_pool` option.

`-import_as_original`
Imports a medium copy or a medium-related catalog data copy as original if an original medium does not exist in a database.

`-disable_lockname LockName`
Disables devices with the *LockName* for any operation. The *LockName* must be defined using the Data Protector GUI or using the `omniupload` command.

`-enable_lockname LockName`
Enables devices with the *LockName*. The *LockName* must be defined using the Data Protector GUI or using the `omniupload` command.

`-disable_device DeviceName [-ignore_lockname]`
Disables the device with the *DeviceName* for any operation. The *DeviceName* must be defined using the Data Protector GUI or using the `omniupload` command. Unless the option `-ignore_lockname` is specified, if the device has a lockname defined, all devices with the same lockname are also disabled.

`-enable_device DeviceName [-ignore_lockname]`
Enables the device with the *DeviceName*. The *DeviceName* must be defined using the Data Protector GUI or using the `omniupload` command. Unless the option `-ignore_lockname` is specified, if the device has a lockname defined, all devices with the same lockname are also enabled.

`-repository LibraryName`
This option is used to specify the repository backup device that you want to check. This information is then used to update the database.

`-repository_barcode_scan LibraryName`
If this option is used then barcode reader is used to update the database. This option should be used only with devices that have enabled barcode reader.

`-repository_update DriveName`
Updates the database by reading all the slots (loads media in drive) in the device repository. If you additionally specify the slot number of the slot that is defined for a CL cartridge, then a cleaning operation is performed on the specified drive.

`-slot SlotID [Side]`
Specifies the *SlotID* of the library where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter in this slot, use the additional *Side* parameter. Slot *SlotID* must be specified for MO devices. Values of *Side* are A or B.

`-add_slots LibraryName {Slot... | FromSlot-ToSlot...}`

Adds slots to the selected library. With ADIC/GRAU DAS or StorageTek ACS libraries, this option adds volsers to the selected library. Make sure you use a format supported by your library. For example, when adding slots to a SCSI library, do not use letters or leading zeros.

`-remove_slots LibraryName {Slot... | FromSlot-ToSlot...}`

Removes slots from the selected library.

`-silo_query LibraryName`

Queries ACS/DAS server for the list of currently resident volsers and updates the Data Protector repository of specified library. This option is not recommended to be used with an ACS/DAS Server when querying logical libraries configured for the same physical library. In such a case, use the `-add_slots` option to add volsers manually.

With DAS Server, however, when logical libraries are not configured using Data Protector, but using the DAS utilities, the Data Protector query operation can safely be used on such libraries instead of adding volsers manually.

`-silo_enter LibraryName`

Moves ACS/DAS media from the CAP (ACS) or insert/eject area (DAS) to the repository.

`-cap CapID`

ID of Control Access Port of ACS or insert/eject area of DAS library.

`-silo_eject LibraryName {Volser... | FromVolser-ToVolser...}`

Moves media from the ACS/DAS repository into the CAP.

`-location Location`

Specifies the new location for the ejected media. Only media with barcode will be updated.

`-enter LibraryName {Slot... | FromSlot-ToSlot...}`

Moves media from the mail slots to the repository slots. This option is available only for SCSI libraries.

`-eject LibraryName {Slot... | FromSlot-ToSlot...}`

Moves media from the repository slots into the mail slots. This option is available only for SCSI libraries.

`-group PoolName MagazineDescription Medium...`

Creates a magazine *MagazineDescription* out of the specified non-magazine media. Note that all specified media must be resident in the same SCSI library at the time. The magazine is added to the pool *PoolName* which must be configured to support magazines.

`-ungroup MagazineDescription`

Splits the magazine *MagazineDescription* so that the magazine media become non-magazine media.

`-reload_serial_number DeviceName`

Reloads the device serial number and overwrites the serial number stored in the internal database. A physical device can therefore be replaced without changing the logical device properties.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omnimmm` command are:

- | | |
|---|--|
| 1 | Program failed, user error. |
| 2 | Program failed, environmental malfunction. |
| 3 | Program failed, internal malfunction. |
| 4 | Program failed, reason unknown. |

EXAMPLES

The following examples illustrate how the `omnimmm` command works.

1. To create pool "DDS_Pool" of the class "DDS", with policy "App+Loose". Media in the pool will be usable for 12 months or for 100 overwrites.

```
omnimmm -create_pool DDS_Pool "DDS" App+Loose 12 100
```

2. To modify the medium with label "Label23" changing the label to "LABEL23" and location to "Backup Room", run:

```
omnimmm -modify_medium Label23 LABEL23 "Backup Room"
```

3. To list detailed information for medium "dat1", run:

```
omnimmm -list_media dat1 -detail
```

4. To list encryption information for medium "MediaPool1_10", run:

```
omnimmm -list_media MediaPool1_10 -encryptioninfo
```

5. To import a medium in the backup device "Pool1" into pool "Default DDS", run:

```
omnimmm -import Pool1 -pool "Default DDS"
```

6. To copy media catalogs of media "DefaultFile_1" and "MyDLT_35" to the mcf directory on UNIX system, run:

```
omnimm -copy_to_mcf "DefaultFile_1" "MyDLT_35"  
-output_directory /tmp/mcf
```

7. To import media-related catalog data copies "2401110a_47d7f516_0aa0_0001.mcf" and "2401110a_47e26bc2_0a74_0002.mcf" from the default MCF directory on Windows Server 2003 into a new media pool with prefix "MCF_" located on another Cell Manager, run:

```
omnimm -import_from_mcf "C:\Program Files\OmniBack\Config\  
Server\import\mcf\2401110a_47d7f516_0aa0_0001.mcf"  
"C:\Program Files\OmniBack\Config\Server\import\mcf\  
2401110a_47e26bc2_0a74_0002.mcf" -pool_prefix "MCF_"  
-no_orig_pool
```

SEE ALSO

omniamo(1), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1),
omnimnt(1), omnimver(1), omniupload(1), sanconf(1M), uma(1M)

omnimnt

responds to a Data Protector mount requests for a medium
(this command is available on systems with the Data Protector User Interface component installed)

omnimnt

SYNOPSIS

```
omnimnt -version | -help  
omnimnt -device BackupDevice -session SessionID [-cancel]
```

DESCRIPTION

The `omnimnt` command satisfies or aborts a Data Protector mount request. A mount request is issued by a backup device once it has filled all the available media. A mount request is a prompt to mount a new medium. Once the requested medium is inserted in the device drive, the `omnimnt` command should be used to confirm that the correct medium is inserted. The mount request can also be canceled which is done by canceling device. If you cancel device, all data objects associated with the backup device that issued the mount request will not be processed any further. To view information on currently active sessions, use the `omnistat` command.

OPTIONS

- version
Displays the version of the `omnimnt` command
- help
Displays the usage synopsis for the `omnimnt` command
- cancel
Cancels the device. This will terminate processing of all objects that are associated with the backup device which issued the request.
- device *BackupDevice*
References the backup device *BackupDevice* which issued the mount request, in order to confirm mount request or cancel the device.
- session *SessionID*
Specifies the session using the backup device which issued the mount request.

EXAMPLES

The following examples illustrate how the `omnimnt` command works.

1. To satisfy a mount request issued by device "DAT1" in a session with SessionID "R-2008/05/05-275", run:

```
omnimnt -device DAT1 -session R-2008/05/05-275
```

2. To cancel device for the backup device "Juke" in the session with SessionID "R-2008/05/25-3", run:

```
omnimnt -device Juke -session R-2008/05/25-3 -cancel
```

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omnimcopy(1)`, `omniminit(1)`, `omnimlist(1)`,
`omnimmm(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`, `uma(1M)`

omnimver

verifies data on a medium
(this command is available on systems with the Data Protector User Interface component installed)

omnimver

SYNOPSIS

```
omnimver -version | -help  
omnimver -device BackupDevice [-slot SlotID [Side]] [-eject]
```

DESCRIPTION

The `omnimver` command is used to verify the contents of a Data Protector backup medium. It reads the data and verifies that data is written in Data Protector format. If the `-crc` option was used to backup the data it also checks the CRC for each block.

OPTIONS

`-version`
Displays the version of the `omnimver` command

`-help`
Displays an extended usage synopsis for the `omnimver` command

`-device BackupDevice`
Specifies the backup device where medium is located.

`-slot SlotID [Side]`
Specifies the *SlotID* of the Exchanger backup device where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter in this slot, use the additional *Side* parameter. Slot *Side* must be specified for MO devices.

`-eject`
Ejects the medium from the drive after the verification.

EXAMPLES

To verify slot 32 of backup device "Spectra60", run:

```
omnimver -device Spectra60 -slot 32
```

SEE ALSO

omniamo(1), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1),
omnimmm(1), omnimnt(1), omniupload(1), sanconf(1M), uma(1M)

omniobjconsolidate

consolidates Data Protector backup objects into synthetic full backups
(this command is available on systems with the Data Protector User Interface component installed)

omniobjconsolidate

SYNOPSIS

```
omniobjconsolidate -version | -help
omniobjconsolidate -consolidationlist ConsolidationSpecificationName -scheduled [GeneralOptions]
omniobjconsolidate -consolidationlist ConsolidationSpecificationName -postbackup -session SessionID [GeneralOptions]
omniobjconsolidate [GeneralOptions] [Device...]... Object [Object...]
```

GeneralOptions

```
[-dynamic min max]
[-protect {none | weeks n | days n | until Date | permanent}]
[-keepcatalog {weeks n | days n | until Date | same_as_data_protection}]
[-[no_]log | -log_dirs | -log_file]
[-recycle]
[-locationpriority MediumLocation [MediumLocation...]...]
[-no_monitor]
```

MediumLocation

```
= "MediumLocation" | "<MediumLocation"
```

Device

```
-targetdevice LogicalDevice [DeviceOptions]
```

DeviceOptions

```
[-concurrency ConcurrencyNumber]
[-crc]
[-encrypt]
[-pool PoolName]
[-prealloc MediumID [MediumID...]...]
```

Object

```
{-filesystem | -winfs} Client:MountPoint Label
-session SessionID
```

```

[-copy CopyID]
[-sourcedevice BackupDevice]
-consolidationdevice LogicalDevice
[-targetdevice LogicalDevice]
[-protect {none | weeks n | days n | until Date | permanent}]
[-keepcatalog {weeks n | days n | until Date | same_as_data_protec-
tion}]
[-[no_]log | -log_dirs | -log_file]
[-[no_]recycle]

OtherOptions

Date= [YY]YY/MM/DD (1969 < [YY]YY < 2038)

```

DESCRIPTION

The `omniobjconsolidate` command creates synthetic full backups from full and incremental backups. It can be used to:

- consolidate objects that you specify
- start a post-backup object consolidation specification
- start a scheduled object consolidation specification

To consolidate an object to a specific point in time, specify only the incremental version of that point in time. The restore chain is retrieved automatically.

To obtain the information about all backed up objects or sessions containing the objects you want to consolidate, use the `omnidb` command.

OPTIONS

```

-version
    Displays the version of the omniobjconsolidate command.

-help
    Displays the usage synopsis of the omniobjconsolidate command.

-consolidationlist ConsolidationSpecificationName
    Specifies the object consolidation specification identified by
    ConsolidationSpecificationName for object consolidation.

-scheduled
    Immediately starts a scheduled object consolidation specification.

-postbackup

```

Immediately starts a post-backup object consolidation specification specified by the `-session SessionID` option.

`-session SessionID`

If specified with the `-postbackup` option, provides the session ID for the post-backup object consolidation session.

If specified as part of the object definition, selects the point in time for object consolidation.

`-dynamic min max`

Specifies how many devices are locked prior to starting a session. Devices that are specified per object through the `-targetdevice` option are locked in any case. The *max* value is increased by Data Protector if the number of statically assigned devices is higher than the specified *max* value.

Min specifies the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be started) required for starting the session. If fewer devices are available than specified here, the session will queue. The default is 1.

Max specifies the maximum number of available devices that Data Protector will use in the session. The highest number you can specify is 32. The default is 5. Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. If this option is not specified, the default value for *max* is the number of specified devices.

`-protect{none | weeks n | days n | until Date | permanent}`

Sets a period of protection for the consolidated data on the backup medium to prevent the data from being overwritten. If this option is not specified, the data protection of the consolidated objects is the same as the protection of the full backup of the objects. If a relative period of protection was set for the full backup, such as *n* days or weeks, the same protection period is counted from the creation time of the synthetic full backup.

`-keepcatalog{weeks n | days n | until Date |
same_as_data_protection}`

Specifies file catalog retention time. If you do not want to save the file catalog, use the `-no_log` option. If this option is not specified, the catalog protection of the consolidated objects is the same as the catalog protection of the full backup of the objects. If a relative period of catalog protection was set for the full backup, such as *n* days or weeks, the same protection period is counted from the creation time of the synthetic full backup.

`-log`

Specifies the logging level of the object consolidation session. All detailed information about backed up files and directories (filenames, file versions, and

attributes) are logged to the IDB. You can browse directories and files before restoring and in addition look at file attributes. Data Protector can fast position on the tape when restoring a specific file or directory.

If the logging level is not specified, the logging level of the source object is used.

`-no_log`

Specifies the logging level of the object consolidation session. No information about backed up files and directories is logged to the IDB. You will not be able to search and browse files and directories before restoring.

`-log_dirs`

Specifies the logging level of the object consolidation session. All detailed information about backed up directories (names, versions, and attributes) is logged to the IDB. You can browse only directories before restoring.

`-log_file`

Specifies the logging level of the object consolidation session. All detailed information about backed up files and directories (filenames and file versions) is logged to the IDB. You can browse directories and files before restoring, and Data Protector can fast position on the tape when restoring a specific file or directory. The information does not occupy much space, since not all file details (file attributes) are logged to the database.

`-[no_]recycle`

The `-recycle` option removes data and catalog protection of the objects on the source media. When there are no more protected objects on the media, the media can be overwritten. The `-no_recycle` option is available as part of the object definition if the `-recycle` option is specified as part of *GENERAL_OPTIONS*.

IMPORTANT: If you recycle data protection of source objects, the recycled points in time will no longer be available. Unless copies of these points in time exist, you will be able to restore only to the latest (consolidated) point in time.

`-locationpriority MediumLocation [MediumLocation]`

The order in which media are selected for object consolidation in case copies of the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

The priority must be specified in the form "`=MediumLocation`" (equal to) or "`<MediumLocation`" (lower priority than).

If you specify `-locationpriority "=Loc1" "<Loc2" "=Loc3" "<Loc4"`, then `Loc1` has the highest priority, `Loc2` and `Loc3` have a lower priority, and `Loc4` has the lowest priority.

- no_monitor
If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.
- filesystem *Client:MountPoint Label*
Selects the filesystem identified with *Client:MountPoint Label* for object consolidation.
- winfs *Client:MountPoint Label*
Selects the Windows filesystem identified with *Client:MountPoint Label* for object consolidation.
- copy *CopyID*
Selects the copy identified with *CopyID*. If not specified, Data Protector automatically selects the most appropriate copy as the source for object consolidation.
- sourcedevice *LogicalDevice*
Specifies a logical device to be used for reading full object versions from the source media. If this option is not specified, Data Protector uses the logical device that was used for writing the objects.
- consolidationdevice *LogicalDevice*
Specifies a logical device that will read incremental object versions and perform object consolidation.
- targetdevice *LogicalDevice*
Specifies a logical device that will be used for writing consolidated object versions to the target media. If specified as a part of *GeneralOptions*, the device is used for all objects. In this case, you can also specify device options. If you specify several devices, the devices will be dynamically assigned to objects.
If specified as part of *Object*, the device is used only for this object.
You can combine static and dynamic assignment of devices by specifying some devices as part of *GeneralOptions*, and for some objects, specifying a device per object.
- concurrency *ConcurrencyNumber*
Specifies the number of Restore Media Agents that can send data to a device concurrently.
The maximum concurrency value is 32.
- crc
The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during object consolidation. The CRC checks enables you to verify the media after the operation.

Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and copying the media.

`-encrypt`

If this option is used, the Backup Media Agent enables hardware encryption on the device. Consolidated data is encrypted and written to media.

`-pool PoolName`

Selects a specific media pool for object consolidation. If not defined, a default media pool from the device definition will be used.

`-prealloc MediumID [MediumID] ...`

Defines the prealloc list. This is a subset of media used for object consolidation in the specified sequence.

When using the prealloc list and the strict media allocation policy with the backup device, Data Protector expects the sequence of the media in the device to correspond with that specified in the prealloc list. If the media are not available in this sequence, Data Protector issues a mount request. If no media are specified in this list, the Data Protector allocation procedure is used to allocate media.

NOTES

All options specified before the first *Object* are applied to all objects. Options specified as a part of an *Object* are applied only to that object and may override general options.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omniobjconsolidate` command are:

10

There was an error while consolidating some files. All agents completed successfully.

11

One or more agents failed, or there was a database error.

12

None of the agents completed the operation.

13

Session was aborted.

EXAMPLES

1. To start an objectconsolidation session that consolidates the WinFS object versions for "OBJECT1" on the host "system1.company.com" to the point in time defined with the session ID "2008/09/06-1", using the device "LTO3" as the source device and the file library "FILEDEV1" as the consolidation device, and writes the consolidated objects to the device "LTO4", use:

```
omniobjconsolidate -winfs system1.company.com:/C 'OBJECT1'  
-session 2008/09/06-1 -sourcedevice 'LTO3'  
-consolidationdevice 'FILEDEV1' -targetdevice 'LTO4'
```

2. To start an interactive object consolidation session for the filesystem object "system1.company.com:/ 'Label42'" from the session "2008/09/01-2", using the device "DEV1" to read the source object and the device "DEV2" to consolidate the object, and write the consolidated object to the device "DEV3", use:

```
omniobjconsolidate -filesystem system1.company.com:/  
'Label42' -session 2008/09/01-2 -sourcedevice 'DEV1'  
-consolidationdevice 'DEV2' -targetdevice 'DEV3'
```

3. To immediately start a post-backup object consolidation specification named "post_BU1" for the session "2009/08/03-1", run:

```
omniobjconsolidate -consolidationlist post_BU1 -postbackup  
-session 2009/08/03-1
```

4. To immediately start a scheduled object consolidation specification named "Consolidation_16_Spec", run:

```
omniobjconsolidate -consolidationlist Consolidation_16_Spec  
-scheduled
```

SEE ALSO

omnib(1), omnikeymigrate(1M), omnikeytool(1M), omniobjcopy(1), omniobjverify(1),
omnir(1)

omniobjcopy

creates additional copies of objects backed up with Data Protector on a different media set
(this command is available on systems with the Data Protector User Interface component installed)

omniobjcopy

SYNOPSIS

```
omniobjcopy -version | -help
omniobjcopy -copylist CopySpecificationName -scheduled [GeneralOptions]
omniobjcopy -copylist CopySpecificationName -postbackup -session SessionID [GeneralOptions]
omniobjcopy -restart SessionID
omniobjcopy [GeneralOptions] [Device] ... Object [Object] ...
```

GeneralOptions

```
[-dynamic min max]
[-targetprotect {none | weeks n | days n | until Date | permanent}]
[-keepcatalog {weeks n | days n | until Date | same_as_data_protection}]
[-[no_]log | -log_dirs | -log_file]
[-sourceprotect {none | weeks n | days n | until Date | permanent}]
[-locationpriority MediumLocation [MediumLocation...]]
[-no_monitor]
[-no_auto_device_selection]
```

MediumLocation

```
= "MediumLocation" | "<MediumLocation"
```

Device

```
== -targetdevice LogicalDevice [DeviceOptions]
```

DeviceOptions

```
[-concurrency ConcurrencyNumber]
[-crc]
[-encrypt]
[-pool PoolName]
[-prealloc MediumID [MediumID...]]
```

Object

```
{-filesystem | -winfs | -netware | -omnidb} Client:MountPoint Label  
-session SessionID  
[-copyid N[-fixedcopy...]]  
[-sourcedevice LogicalDevice]  
[-targetdevice LogicalDevice]  
[-targetprotect {none | weeks n | days n | until Date | permanent}]  
[-keepcatalog {weeks n | days n | until Date | same_as_data_protection}]  
[[-no_]log | -log_dirs | -log_file]  
[-sourceprotect {none | weeks n | days n | until Date | permanent | keep}]  
[-full]
```

Object

```
-rawdisk Client Label  
-session SessionID  
[-copyid N[-fixedcopy...]]  
[-sourcedevice LogicalDevice]  
[-targetdevice LogicalDevice]  
[-targetprotect {none | weeks n | days n | until Date | permanent}]  
[-sourceprotect {none | weeks n | days n | until Date | permanent | keep}]
```

Object

```
{-sap | -oracle8 | -informix | -msese | -mssql | -lotus | -mbx |  
-sapdb | -msvssw | -db2 | -sybase | -mssps | -vmware} Client:Set  
-session SessionID  
[-copyid N[-fixedcopy...]]  
[-sourcedevice LogicalDevice]  
[-targetdevice LogicalDevice]  
[-targetprotect {none | weeks n | days n | until Date | permanent}]  
[-sourceprotect {none | weeks n | days n | until Date | permanent | keep}]
```

OtherOptions

Date= [YY]YY/MM/DD (1969 < [YY]YY < 2038)

DESCRIPTION

The `omniobjcopy` command creates additional copies of objects backed up using Data Protector. You can use the `omniobjcopy` command to copy objects such as filesystems (UNIX or Windows), very big file systems, disk image sections, NetWare objects, and Data Protector internal database (IDB) to an additional media set. The command can be also used for copying the integration objects (SAP R/3, Oracle, Informix Server, VMware Virtual Infrastructure, Microsoft Exchange Server, Microsoft Exchange Server single mailboxes, Microsoft SQL Server, Lotus, Sybase, DB2, Microsoft Volume Shadow Copy Service, and SAP DB/MaxDB).

To obtain the information about all backed up objects or sessions containing the objects you want to copy, use the `omnidb` command.

This command starts an interactive or automated object copy session. Use this command to immediately start an automated (scheduled or post-backup) object copy specification.

OPTIONS

`-version`

Displays the version of the `omniobjcopy` command.

`-help`

Displays the usage synopsis for the `omniobjcopy` command.

`-copylist CopySpecificationName`

Specifies the name of the object copy specification identified by *CopySpecificationName* for object copying.

`-scheduled`

Immediately starts a scheduled object copy specification.

`-postbackup`

Immediately starts a post-backup object copy specification specified by the `-session SessionID` option.

`-session SessionID`

Selects the session ID for the `-postbackup` option or for the object definition.

`-restart SessionID`

Tries to restart a failed non-interactive object copy session, specified by its session ID.

`-dynamic min max`

Specifies how many devices are locked prior to starting a session. Devices that are specified per object through the `-targetdevice` option are locked in any case. The *max* value is increased by Data Protector if the number of statically assigned devices is higher than the specified *max* value.

Min specifies the minimum number of available devices (devices that are not being used by another Data Protector session and have the license to be started) required for starting the session. If fewer devices are available than specified here, the session will queue. The default is 1.

Max specifies the maximum number of available devices that Data Protector will use in the session. The highest number you can specify is 32. The default is 5. Data Protector will lock the number of devices that you specify using this parameter if so many devices are available. If this option is not specified, the default value for *max* is the number of specified devices.

`-targetprotect {none | weeks n | days n | until Date | permanent}`

Sets the level of protection for the copy object. The media containing this object copy session cannot be overwritten until the protection expires. By default (if this option is not specified), the protection is the same as the original protection for the source object.

The old `-recycle` option, which was the equivalent of `-targetprotect none`, is deprecated.

`-keepcatalog {weeks n | days n | until Date | same_as_data_protection}`

Specifies file catalog retention time. If you do not want to save the file catalog at all, use the `-no_log` option. By default (if this option is not specified), the protection is the same as for the source object.

`-log`

Specifies the logging level of the object copy session. All detailed information about backed up files and directories (filenames, file versions, and attributes) are logged to the Data Protector internal database (IDB). This allows you to browse directories and files before restore and in addition look at the file attributes. Data Protector can fast position on the tape when restoring a specific file.

If the logging level is not specified, it is set to the same logging level as for the source object.

`-no_log`

Specifies the logging level of the object copy session. Disables the logging of backed up files to the catalog database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log_dirs`

Specifies the logging level of the object copy session. If this option is specified, only the directories are logged into the database. By default, the filename and backup history of each backed up file is written to the catalog database.

`-log_file`

Specifies the logging level of the object copy session. All detailed information about backed up files and directories (filenames and file versions) is logged to the Data Protector internal database (IDB). This information allows you to search for backed up files and allows Data Protector to fast position the tape. It also does not take much space since some information on file details (file attributes) is not logged to the database.

`-sourceprotect {none | weeks n | days n | until Date | permanent | keep}`

Sets the level of protection for the source object after a successful copy. The media containing this source object cannot be overwritten until the protection expires. By default (if this option is not specified), the protection is not changed. The `none` option specifies that protection is removed from the source object immediately, allowing recycling.

The `keep` option can only be specified at the object level and specifies that the protection for that source object should not be changed. `-sourceprotect keep` is equivalent to the old `-no_recycle` option, which is deprecated.

`-locationpriority MediumLocation [MediumLocation]`

The order in which media are selected for the object copy in case that the same object version exist in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally matches the conditions of the media set selection algorithm.

The priority must be specified in the form "`=MediumLocation`" (equal to) or "`<MediumLocation`" (lower priority than).

If you specify `-locationpriority "=Loc1" "<Loc2" "=Loc3" "<Loc4"`, then `Loc1` has the highest priority, `Loc2` and `Loc3` have a lower priority, and `Loc4` has the lowest priority.

`-no_monitor`

If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.

`-no_auto_device_selection`

If this option is specified, Data Protector does not automatically replace unavailable devices with available devices of the same device tag.

`-concurrency ConcurrencyNumber`

Specifies the number of Restore Media Agents that can send data to a device concurrently.

The maximum concurrency value is 32.

`-crc`

The CRC check is an enhanced checksum function. When this option is selected, cyclic redundancy check sums (CRC) are written to the media during an object copy. The CRC checks enables you to verify the media after the operation. Data Protector re-calculates the CRC during a restore and compares it to the CRC on the medium. It is also used while verifying and the media.

`-encrypt`

If this option is used, the Backup Media Agent enables hardware encryption on the device. Data is encrypted and copied.

`-pool PoolName`

Selects a specific media pool for object copy. If not defined, a default media pool from the device definition will be used.

`-prealloc MediumID [MediumID] ...`

Defines the prealloc list. This is a subset of media used for object copy in the specified sequence.

When using the prealloc list and the strict media allocation policy with the backup device, Data Protector expects the sequence of the media in the device to correspond with that specified in the prealloc list. If the media are not available in this sequence, Data Protector issues a mount request. If no media are specified in this list, the Data Protector allocation procedure is used to allocate media.

`-filesystem Client:MountPoint Label`

Selects the filesystem identified with *Client:MountPoint Label* for object copying.

`-winfs Client:MountPoint Label`

Selects the Windows filesystem identified with *Client:MountPoint Label* for object copying.

`-netware Client:MountPoint Label`

Selects the Netware filesystem identified with *Client:MountPoint Label* for object copying.

`-omnidb Client:MountPoint Label`

Selects the IDB identified by *Client:MountPoint Label* for object copying.

`-copyid N [-fixedcopy]`

Selects the specified object copy as a source for object copying.

If `-fixedcopy` option is not specified, Data Protector selects the needed media set automatically. If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option is obligatory.

`-sourcedevice LogicalDevice`

Specifies a logical device different from the one used for the backup to be used for reading backed up objects from the source media. By default (if this option is not specified), the same backup device is used for backing up and reading backed up objects from the source media.

`-targetdevice LogicalDevice`

Specifies a backup device that will be used for writing object copies to the target media.

`-full`

Selects the whole restore chain of full and incremental backups for the object copy operation. This option is not supported for Data Protector application integrations.

`-sap Client:Set`

Selects the SAP R/3 object identified by `Client:Set` for object copying.

`-informix Client:Set`

Selects the Informix Server object identified by `Client:Set` for object copying.

`-msese Client:Set`

Selects the Microsoft Exchange Server object identified by `Client:Set` for object copying.

`-mssql Client:Set`

Selects the Microsoft SQL Server object identified by `Client:Set` for object copying.

`-lotus Client:Set`

Selects the Lotus Notes/Domino Server object identified by `Client:Set` for object copying.

`-mbx Client:Set`

Selects the Microsoft Exchange Server single mailbox object identified by `Client:Set` for object copying.

`-sapdb Client:Set`

Selects the SAP DB/MaxDB object identified by `Client:Set` for object copying.

`-msvssw Client:Set`

Selects the Microsoft Volume Shadow Copy Service object identified by `Client:Set` for object copying.

`-db2 Client:Set`

Selects the DB2 object identified by *Client:Set* for object copying.

`-sybase Client:Set`

Selects the Sybase object identified by *Client:Set* for object copying.

`-mssps Client:Set`

Selects the Microsoft SharePoint Portal Server object identified by *Client:Set* for object copying.

`-vmware Client:Set`

Selects the VMware Virtual Infrastructure object identified by *Client:Set* for object copying.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omniobjcopy` command are:

- | | |
|----|---|
| 10 | There was an error while copying some files. All agents completed successfully. |
| 11 | One or more agents failed, or there was a database error. |
| 12 | None of the agents completed the operation. |
| 13 | Session was aborted. |

EXAMPLES

1. To start an interactive object copy session for copying two WinFS objects "system.company.com:/C 'Object1'" and "system.company.com:/C 'Object1'" from two different sessions to the device "DEV1", so that the source object version for "Object1" is then recycled, run:

```
omniobjcopy -winfs system.company.com:/C 'Object1' -session
2008/09/01-3 -targetdevice 'DEV1' -recycle -winfs
systems.company.com:/C 'Object2' -session 2008/09/24-2
-targetdevice 'DEV1'
```

2. To start an interactive object copy session for copying the whole restore chain of full and incremental backups for the filesystem object "system1.company.com:/

'Label42'" from the session "2008/07/01-2", using the device "DEV1" to read the source objects and the device "DEV2" copy the objects, run:

```
omniobjcopy -filesystem system1.company.com:/ 'Label42'  
-session 2008/07/01-2 -sourcedevice 'DEV1' -targetdevice  
'DEV2' -full
```

3. To immediately start a post-backup object copy specification named "post_BU1" for the session "2008/08/03-1", use:

```
omniobjcopy -copylist post_BU1 -postbackup -session  
2008/08/03-1
```

4. To immediately start a scheduled object copy specification named "CopySpec", use:

```
omniobjcopy -copylist CopySpec -scheduled
```

5. To restart a failed post-backup object copy specification "2009/03/16-9", use:

```
omniobjcopy -restart "2009/03/16-9"
```

SEE ALSO

omnib(1), omnikeymigrate(1M), omnikeytool(1M), omniobjconsolidate(1),
omniobjverify(1), omnir(1)

omniobjverify

verifies Data Protector backup objects, either interactively or using pre-configured post-backup, or scheduled verification specifications
(this command is available on systems with the Data Protector User Interface component installed)

omniobjverify

SYNOPSIS

```
omniobjverify -version | -help
omniobjverify -verificationlist VerificationSpecificationName
-scheduled [GeneralOptions]
omniobjverify -verificationlist VerificationSpecificationName
-postbackup -session SessionID [GeneralOptions]
omniobjverify [GeneralOptions] Object [Object]...]
```

GeneralOptions

```
[{-verify_on_source | -verify_on_mahost | -verify_on_host host-name}]
[-locationpriority MediumLocation [MediumLocation]...]
[-no_monitor]
```

MediumLocation

```
= "MediumLocation" | "<MediumLocation"
```

Object

```
{-filesystem | -winfs | -netware | -omnidb | -rawdisk} Client:ObjectName Label
-session SessionID
[-copyid N [-fixedcopy...]]
[-sourcedevice LogicalDevice]
```

Object

```
{-sap | -oracle8 | -vmware | -informix | -msese | -mssql | -mssps |
-lotus | -mbx | -sapdb | -msvssw | -db2 | -sybase} Client:ObjectName
-session SessionID
[-copyid N [-fixedcopy...]]
[-sourcedevice LogicalDevice]
```

DESCRIPTION

The `omniobjverify` command verifies backup objects that have been created by Data Protector backup, object copy, or object consolidation sessions. You can use the `omniobjverify` command to verify objects such as filesystems (UNIX or Windows), very big file systems, disk image sections, NetWare objects, and the Data Protector Internal Database (IDB).

The command can be also used to verify integration objects (SAP R/3, Oracle, Informix Server, VMware Virtual Infrastructure, Microsoft Exchange Server, Microsoft Exchange Server single mailboxes, Microsoft SQL Server, Lotus, Sybase, DB2, Microsoft Volume Shadow Copy Service, and SAP DB/MaxDB). It verifies the data integrity of the objects and the ability of Data Protector to deliver them to the application integration, not the application integration's ability to restore them.

To obtain the information about all backed up objects or sessions containing the objects you want to verify, use the `omnidb` command.

This command can be used to start an interactive object verification session or immediately start an automated (scheduled or post-backup) object verification specification.

OPTIONS

`-version`

Displays the version of the `omniobjverify` command.

`-help`

Displays the usage synopsis for the `omniobjverify` command.

`-verificationlist VerificationSpecificationName`

Specifies the name of the verification specification, identified by *VerificationSpecificationName*, for object verification.

`-scheduled`

Immediately starts a scheduled verification specification.

`-postbackup`

Immediately starts a post-backup verification specification specified by the `-session SessionID` option.

`-session SessionID`

Selects the session ID for the `-postbackup` option or for the object definition.

`-verify_on_source`

Specifies the original backup object source host as the host on which the object verification process will be performed.

`-verify_on_mahost`

Specifies the media agent host as the host on which the object verification process will be performed.

`-verify_on_host hostname`

Specifies the host identified by *hostname* as the host on which the object verification process will be performed.

`-locationpriority MediumLocation [MediumLocation]`

The order in which media are selected for object verification if the same object version exists in more than one location. By default, Data Protector automatically selects the most appropriate media set. Media location priority is considered if more than one media set equally match the conditions of the media set selection algorithm.

The priority must be specified in the form "*=MediumLocation*" (equal to) or "*<MediumLocation*" (lower priority than).

If you specify `-locationpriority "=Loc1" "<Loc2" "=Loc3" "<Loc4"`, then *Loc1* has the highest priority, *Loc2* and *Loc3* have a lower priority, and *Loc4* has the lowest priority.

`-no_monitor`

If this option is used, the command displays only the session ID. By default, the command monitors the session and displays all messages.

`-filesystem Client:ObjectName Label`

Selects the filesystem identified by *Client:ObjectName Label* for object verification.

`-winfs Client:ObjectName Label`

Selects the Windows filesystem identified by *Client:ObjectName Label* for object verification.

`-netware Client:ObjectName Label`

Selects the Netware filesystem identified by *Client:ObjectName Label* for object verification.

`-omnidb Client:ObjectName Label`

Selects the IDB identified by *Client:ObjectName Label* for object verification.

`-rawdisk Client:ObjectName Label`

Selects the disk image identified by *Client: Label* for object verification. *ObjectName* is blank in this case

`-copyid N[-fixedcopy]`

Selects the specified copy of an object version as a source for object verification.

If `-fixedcopy` option is not specified, Data Protector selects the needed media set automatically. If several copies of the same object version exist in one session as a result of the object copy or object mirror operation, this option is obligatory.

`-sourcedevice LogicalDevice`

Specifies a logical device different from the one used for the backup to be used for reading backed up objects from the source media. By default (if this option is not specified), the original backup device is used for reading backed-up objects from the source media.

`-sap Client:ObjectName`

Selects the SAP R/3 object identified by *Client:ObjectName* for object verification.

`-informix Client:ObjectName`

Selects the Informix Server object identified by *Client:ObjectName* for object verification.

`-msese Client:ObjectName`

Selects the Microsoft Exchange Server object identified by *Client:ObjectName* for object verification.

`-mssql Client:ObjectName`

Selects the Microsoft SQL Server object identified by *Client:ObjectName* for object verification.

`-lotus Client:ObjectName`

Selects the Lotus Notes/Domino Server object identified by *Client:ObjectName* for object verification.

`-mbx Client:ObjectName`

Selects the Microsoft Exchange Server single mailbox object identified by *Client:ObjectName* for object verification.

`-sapdb Client:ObjectName`

Selects the SAP DB/MaxDB object identified by *Client:ObjectName* for object copying.

`-msvssw Client:ObjectName`

Selects the Microsoft Volume Shadow Copy Service object identified by *Client:ObjectName* for object verification.

`-db2 Client:ObjectName`

Selects the DB2 object identified by *Client:ObjectName* for object verification.

`-sybase Client:ObjectName`

Selects the Sybase object identified by *Client:ObjectName* for object verification.

`-mssps Client:ObjectName`

Selects the Microsoft SharePoint Portal Server object identified by *Client:ObjectName* for object verification.

`-vmware Client:ObjectName`

Selects the VMware Virtual Infrastructure object identified by *Client:ObjectName* for object verification.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omniobjverify` command are:

- | | |
|----|---|
| 10 | There was an error while verifying some files. All agents completed successfully. |
| 11 | One or more agents failed, or there was a database error. |
| 12 | None of the agents completed the operation. |
| 13 | Session was aborted. |

EXAMPLES

1. To start an interactive object verification session for verifying one WinFS object "system.company.com:/C 'Object1'" from session 2009/02/06-1, using the original host as the verification host, run:

```
omniobjverify -winfs system.company.com:/C 'Object1'
-session 2009/02/06-1
```

2. To start an interactive verification session for verifying two filesystem objects "system1.company.com:/ 'Label1'" and "system1.company.com:/ 'Label2'" from session 2009/03/01-2, on host "system2.company.com", run:

```
omniobjverify -verify_on_host system2.company.com
-filesystem system1.company.com:/ 'Label1' -session
2009/03/01-2 -filesystem system1.company.com:/ 'Label2'
-session 2009/03/01-2
```

3. To immediately start a post-backup verification specification named "post_bu_verify1" for the session "2009/01/03-1", run:

```
omniobjverify -verificationlist post_bu_verify1 -postbackup  
-session 2009/01/03-1
```
4. To immediately start a scheduled verification specification named "sched_verify1", run:

```
omniobjverify -verificationlist sched_verify1 -scheduled
```

SEE ALSO

omnib(1), omnidb(1), omnikeymigrate(1M), omnikeytool(1M), omniobjconsolidate(1), omniobjcopy(1), omnir(1)

omnir

restores filesystems, disk images, the Data Protector database (IDB), Microsoft Exchange Server single mailboxes and Public Folders, Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Portal Server (SPS), SAP R/3, SAP DB/MaxDB, Informix Server, VMware Virtual Infrastructure (VMware), Lotus, IBM DB2 UDB, NetWare objects, and NDMP objects backed up with Data Protector. The command is also used to start the instant recovery process. To restore a Sybase database, refer to the `syb_tool` man page.

(this command is available on systems with the Data Protector User Interface component installed)

omnir

SYNOPSIS

```
omnir -version | -help
omnir SESSION_OPTIONS [-noexpand] Object [Object]

SESSION_OPTIONS
-[no_]preview
-report {warning | minor | major | critical}

omnir -resume SessionID [-no_monitor]
```

FILESYSTEM RESTORE

Object

```
{-filesystem | -winfs | -netware} Client:MountPoint Label
-session SessionID [-copyid CopyID]
-tree TreeName...
[DATA_OPTIONS]
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
[SPLIT_MIRROR_OPTIONS]
```

Object

```
{-filesystem | -winfs | -netware} Client:MountPoint Label
-full [-session SessionID]
-tree TreeName...
[DATA_OPTIONS]
[FILESYSTEM_OPTIONS]
[SPLIT_MIRROR_OPTIONS]
[GENERAL_OPTIONS]
```

Object

```
{-filesystem | -winfs | -netware} Client:MountPoint Label
-omit_deleted_files [-session SessionID [-copyid CopyID] ]
-overwrite
-tree TreeName...
[DATA_OPTIONS]
[FILESYSTEM_OPTIONS]
[SPLIT_MIRROR_OPTIONS]
[GENERAL_OPTIONS]
```

Object

```
{-filesystem | -winfs | -netware} Client:MountPoint Label
-tree TreeName...
MEDIUM_OPTIONS
[DATA_OPTIONS]
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
```

Object

```
-host Clientname
-session SessionID
[-full | -omit_deleted_files -overwrite ]
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
```

INTERNAL DATABASE RESTORE

Object

```
-omnidb Client:MountPoint Label
-session SessionID [-copyid CopyID]
-tree TreeName...
-into Pathname
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
```

Object

```
-omnidb Client:MountPoint Label
-tree TreeName...
-into Pathname
MEDIUM_OPTIONS
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
```

RAW DISK RESTORE

Object

```
-rawdisk Host Label  
-session SessionID [-copyid CopyID]  
-section [ToSection=] Section  
[SPLIT_MIRROR_OPTIONS]  
[GENERAL_OPTIONS]
```

Object

```
-rawdisk Host Label  
-section [ToSection=] Section  
MEDIUM_OPTIONS  
[GENERAL_OPTIONS]
```

INSTANT RECOVERY

```
omnir -host ClientName  
-session SessionID  
-instant_restore  
[DISK_ARRAY_XP_OPTIONS | VIRTUAL_ARRAY_OPTIONS | ENTERPRISE_VIRTUAL_ARRAY_OPTIONS]  
[ORACLE_SPECIFIC_OPTIONS]  
[SAP_SPECIFIC_OPTIONS]  
  
DISK_ARRAY_XP_OPTIONS  
-keep_version  
-check_config  
  
VIRTUAL_ARRAY_OPTIONS  
-keep_version  
-check_config  
  
ENTERPRISE_VIRTUAL_ARRAY_OPTIONS  
-check_config  
-force_prp_replica  
  
SAP_SPECIFIC_OPTIONS  
-sap  
-user UserName -group GroupName  
-recover {now | time MM/DD/YY hh:mm:ss | logseq LogSeqNum thread ThreadNum | SCN Number} [-open [-resetlogs]]  
  
ORACLE_SPECIFIC_OPTIONS  
-oracle
```

```
-user UserName -group GroupName
-recover {now | time MM/DD/YY hh:mm:ss | logseq LogSeqNum thread
ThreadNum | SCN Number} [-open [-resetlogs]]
-appname ApplicationDatabaseName
-parallelism Number
```

NDMP RESTORE

Object

```
-filesystem Host:MountPoint Label
-full [-session SessionID]
-tree TreeName...
[NDMP_DATA_OPTIONS]
[NDMP_GENERAL_OPTIONS]
```

Object

```
-filesystem Host:MountPoint Label
-session sessionID [-full]
-tree TreeName...
[NDMP_DATA_OPTIONS]
[GENERAL_OPTIONS]
```

NDMP_DATA_OPTIONS

```
-into PathName
-ndmp_env FileName
-ndmp_user UserName
-ndmp_passwd Password
```

GENERAL_OPTIONS

```
-device BackupDevice
-server ServerName
-no_monitor
-variable VariableName VariableValue
```

SAP R/3 FILE RESTORE

Object

```
-sap Client:Set
-session SessionID [-copyid CopyID]
-tree FileName...
[DATA_OPTIONS]
[FILESYSTEM_OPTIONS]
[GENERAL_OPTIONS]
```

VMWARE VIRTUAL INFRASTRUCTURE RESTORE

RESTORE OF VIRTUAL MACHINES

```
omnir -vmware
-barhost OriginalVMwareManagementClient
-instance OriginalDatacenter
-method {Snapshot | Suspend | VCBimage}
[-session SessionID]
VirtualMachines [-disk Disk [-disk Disk ...]]
[VirtualMachines [-disk Disk [-disk Disk ]] ...]
[-destination RestoreClient]
[-newinstance TargetDatacenter]
[-consolidate]
[-memory]
[-register]
[-poweron]
[-overwrite [older]]
```

RESTORE OF FILESYSTEMS OF VIRTUAL MACHINES

```
omnir -vmware
-barhost OriginalVMwareManagementClient
-instance OriginalDatacenter
-method VCBfile
[-session SessionID]
VirtualMachines -target TargetClient [-file File [-file File ...] ]
[VirtualMachines -target TargetClient [-file File [-file File ...]]
...]
[-destination RestoreClient]
[-overwrite [older]]

VirtualMachines
{
-all [-exclude VMfolder [-exclude VMfolder ...]] |
-vmfolder VMfolder [-exclude VMfolder [-exclude VMfolder ...]] |
-vm VM
}
```

SAP DB/MAXDB RESTORE

```
omnir -sapdb
-barhost ClientName
-instance InstanceName
[-destination ClientName]
```

```
[-newinstance DestinationInstanceName]  
[-session SessionID]  
[-recover [-endlogs | -time: YYYY-MM-DD.hh.mm.ss] [-from_disk]]  
[-nochain]
```

INFORMIX SERVER RESTORE

```
omnir -informix  
-barhost ClientName  
-barcmd PathName  
-user User:Group  
-appname ApplicationDatabaseName  
-bararg OnBarRestoreArguments  
[SESSION_OPTIONS]  
[GENERAL_OPTIONS]  
  
SESSION_OPTIONS  
-report {warning | minor | major | critical}  
-load {low | medium | high}  
-no_monitor
```

MICROSOFT EXCHANGE SERVER RESTORE

```
omnir -msese  
-barhost ClientName  
[-destination ClientName]  
-appname full_application_name  
{-base DBName -session SessionID}...  
-logpath Path  
[-last [-mount] [-consistent]] [GENERAL_OPTIONS]
```

MICROSOFT EXCHANGE SINGLE MAILBOX RESTORE

```
omnir -mbx  
-barhost HostName  
[-destination HostName]  
-mailbox MailboxName -session SessionID [MAILBOX_OPTIONS]...  
-public -session SessionID [PUBLIC_FOLDERS_OPTIONS]  
[GENERAL_OPTIONS]  
  
MAILBOX_OPTIONS  
-folder FolderName  
-exclude FolderName  
-originalfolder {-keep_msg | -overwrite_msg}  
-destmailbox DestMailboxName  
-chain
```



```

PUBLIC_FOLDERS_OPTIONS
-folder FolderName
-exclude FolderName
-originalfolder {-keep_msg | -overwrite_msg}
-chain

```

MICROSOFT SQL SERVER RESTORE

```

omnir -mssql
-barhost ClientName
[-destination ClientName]
[-instance SourceInstanceName]
[-destinstance DestinationInstanceName]
{-base DBName [-session SessionID] [MSSQL_OPTIONS]... | -base DBName
-datafile GroupName/DataFileName -session SessionID [DATAFILE_OPTIONS]...}
[GENERAL_OPTIONS]

```

```

MSSQL_OPTIONS
-asbase NewDBName {-file LogicalFileName1 PhysicalFileName1 [-file
LogicalFileName2 PhysicalFileName2]...}
-replace
-nochain
-recovery {rec | norec}
-stopat yyyy/mm/dd.hh:mm:ss
-standby File

```

```

DATAFILE_OPTIONS
-replace
-nochain
-recovery {rec | norec}

```

MICROSOFT SHAREPOINT PORTAL SERVER RESTORE

```

omnir -mssps
-barhost ClientName MSSPS_OPTIONS

MSSPS_OPTIONS
[-changemaster]
[-portal VirtualServer {[-teamdb DBName MSSPS_SQL_Options...]}
[-index Index_Options] [-sitedbs SiteDBS_Options]} ...]
[-ssodb MSSPS_SQL_Options]
[-doclib -session SessionID]

MSSPS_SQL_Options
-session SessionID

```

```
[-tohost Client]  
[-instance Instance]  
[-as NewDBName]
```

```
Index_Options  
-session SessionID  
[-tohost Client]  
[-todir Directory]
```

```
SiteDBS_Options  
-session SessionID  
[-tohost Client]  
[-instance Instance]
```

LOTUS RESTORE

```
omnir -lotus  
-barhost ClientName  
[-user User:Group]  
[-destination ClientName]  
[-parallelism n]  
-domino_server srv_name  
-appname  
-db db1 [-db db2...]  
[-NSF] [-NTF] [-BOX] [-ALL]  
[-direx direx1 [-direx direx2]...]  
[-r_dest restore_dir]  
[-recover | recovery_time yyy/mm/dd.hh:mm:ss]  
[-session SessionID]
```

VSS RESTORE

```
omnir -vss  
-barhost ClientName  
-session SessionID1 -tree TreeName1 [-tree TreeName2...] [-session  
SessionID2 -tree TreeName3 [-tree TreeName4...]...]  
[[-into PathName] [-destination ClientName] | -instant_restore IN-  
STANT_RECOVERY_OPTIONS]  
[VSS_EXCHANGE_SPECIFIC_OPTIONS]  
[VSS_EXCHANGE_2007_SPECIFIC_OPTIONS]  
  
INSTANT_RECOVERY_OPTIONS  
[-conf_check {strict | non-strict | disabled}]  
[-no_recovery]
```

```
[-use_vds | VSS_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS | VSS_DISK_ARRAY_XP_OPTIONS]
```

```
VSS_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS
```

```
[-no_copy_back | -copy_back [-diskarray_wait Minutes [-delete_replica] | -no_diskarray_wait]]
```

```
[-no_retain_source]
```

```
VSS_DISK_ARRAY_XP_OPTIONS
```

```
-copy_back -no_retain_source [-no_diskarray_wait]
```

```
VSS_EXCHANGE_SPECIFIC_OPTIONS
```

```
[-exch_check [-exch_throttle Value]]
```

```
VSS_EXCHANGE_2007_SPECIFIC_OPTIONS
```

```
[-appsrv ClientName]
```

```
[[[-target_tree TargetStoreName | -exch_RSG LinkedStoreName]
```

```
-target_dir Directory]
```

DB2 RESTORE

```
omnir -db2
```

```
-barhost ClientName
```

```
-instance InstName
```

```
{[-dbname DBName [-session SessionID] [-newdbname NewDBName...]]
```

```
[-tsname DBName*TSName [-session SessionID] [-offline]...] [-logfile DBName*LogFileName [-session SessionID]...]}
```

```
[DB2_OPTIONS]
```

```
DB2_OPTIONS
```

```
-destination ClientName
```

```
-rollforward [-time YYYY-MM-DD.hh.mm.ss]
```

```
-frominstance InstName
```

DATA_OPTIONS

```
-exclude PathName ...
```

```
-skip MatchPattern ...
```

```
-only MatchPattern ...
```

```
-as Pathname
```

```
-into Pathname
```

MEDIUM_OPTIONS

```
-device BackupDevice
```

```
-medium MediumID
```

```
-id DiskAgentID
```

`[-slot SlotID [Side]]`

FILESYSTEM_OPTIONS

`-touch`
`-lock`
`-no_protection`
`-[no_]overwrite | -merge`
`-catalog`
`-sparse`
`-move_busy`
`-vsr_only`
`-trustee`
`-no_share[_info]`
`-omit_unrequired_object_versions`
`-[no_]resumable`

GENERAL_OPTIONS

`-device BackupDevice`
`-no_auto_device_selection`
`-server ServerName`
`-target Client`
`-profile`
`-load {low | medium | high}`
`-pre_exec PathName`
`-post_exec PathName`
`-variable VariableName VariableValue`
`-no_monitor`

SPLIT_MIRROR_OPTIONS

`-sse | -symmetrix`
`-remote Host Host | -local Host Host | -combined Host Host`
`-quiesce cmd`
`-restart cmd`
`-mirrors list`
`[-discovery]`
`[-re_establish_links_before_restore]`
`-disable_disks`
`-restore_links_after_restore`

DESCRIPTION

The `omnir` command restores objects backed up using Data Protector. You can use the `omnir` command to restore filesystems (UNIX, Windows), very big file systems, disk image sections, NetWare objects, NDMP objects and Data Protector internal database (IDB) to their original (or a new) location. The command can be also used for restoring Integration objects (SAP R/3, Microsoft Exchange Server, Microsoft Exchange Server single mailboxes, Microsoft SQL Server, Microsoft SharePoint Portal Server, Lotus, Informix Server, DB2 and SAP DB/MaxDB) or to start the instant recovery process. To restore a Sybase database, refer to the `syb_tool` man pages.

If several copies of the same object version exist, you can let Data Protector select which media set will be used for the restore. You can also specify the media set from which you want to restore the data, except when restoring integration objects. It is not possible to specify the media set created as a result of the media copy operation.

The `omnir` command also supports parallel restore. You can achieve this by specifying more than one object using the command line options. It is not possible to use the `-medium` option when performing a parallel restore. The number of objects for parallel restore is limited by the global option `MaxSessions`, which can be set on the Cell Manager in the file

`Data_Protector_program_data\Config\Server\options\global` (Windows Server 2008),

`Data_Protector_home\Config\Server\options\global` (other Windows systems), or `/etc/opt/omni/server/options/global` (UNIX systems).

NOTE: It is not allowed to specify the same object more than once within the same `omnir` command. To differentiate options for the same object (for example, the `-tree` option) specify these options for the same object as many times as needed.

Information about all backed up objects can be obtained from the IDB by using `omnidb` command or, in the case of the instant recovery, from the ZDB database by using the `omnidbxp`, `omnidbva`, `omnidbsmis`, or `omnidbvss` command. (See the related man pages for more information). For most restore actions you need to specify the `SessionID` of the session containing the object you want to restore, which can be obtained by the `omnidb` command.

NOTE: When restoring integration objects, provide the `SessionID` of the backup session. In case of object copies, do not use the object copy session ID, but the object's `BackupID`, which equals the object's backup session ID. If imported backup media are used for restoring an object, do not specify the new session ID which is assigned to the imported backup session, but the object's `BackupID` which is the original backup session ID for that object.

To restore objects from a medium that is not in IDB, use the `-medium MediumID` option, instead of the `SessionID`.

NOTE: The `-medium` option is not possible when performing a parallel restore.

To get the `MediumID` and `DiskAgentID` from the medium, use the `omnimlist` command to read the medium. See the `omnimlist` man page for more information on this command.

OPTIONS

`-version`

Displays the version of the `omnir` command.

`-help`

Displays the usage synopsis of the `omnir` command.

`-resume SessionID`

Starts a new session that continues with the restore from where the failed session `SessionID` left off, using the same options as used in the failed session. This functionality is supported for failed filesystem restore sessions, IDB restore sessions and for Data Protector Oracle Server integration restore sessions.

FILESYSTEM RESTORE

`-filesystem Client:MountPoint Label`

Selects the filesystem identified with `Client:MountPoint Label` for restore.

`-winfs Client:MountPoint Label`

Selects the Windows filesystem identified with `Client:MountPoint Label` for restore.

`-netware Client:MountPoint Label`

Selects the Netware filesystem identified with `Client:MountPoint Label` for restore.

`-session SessionID`

Specifies the session to be used for restore.

`-copyid CopyID`

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

`-tree TreeName`

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives). For example: `-tree /usr/temp` (UNIX system) and `-tree /temp/Filesystem/E` (Windows system).

`-full`

Specifies that the selected object will be restored from the last full backup and all incremental backups related to this full backup.

`-omit_deleted_files`

This option can be only used in combination with the `-overwrite` option.

If this option is specified, Data Protector attempts to recreate the state of the restored directory tree as it was when the last incremental backup was run, while preserving files that were created or modified after the last incremental backup. However, if the directory contains files that did not exist there at the time of the last incremental backup, but their modification time is older than the time of the incremental backup, Data Protector will delete these files as well.

When this option is used in combination with the `-as` or `-into` option, be careful when specifying the new location to prevent accidental deletion of existing files.

If this option is not specified, when restoring a directory from which files were deleted between a full and an incremental backup, these files are also restored.

The time on the Cell Manager and clients must be synchronized for this option to function properly.

`-host ClientName`

Restores all objects of the specified client that were backed up in the specified session. This option is only valid for the filesystem restore. If any other type of object (for example, the Data Protector internal database) was a part of the specified session, the restore will abort.

INTERNAL DATABASE RESTORE

`-omnidb Client:MountPoint Label`

Selects the IDB identified by `Client:MountPoint Label` for restore.

`-session SessionID`

Specifies the session to be used for restore.

`-copyid CopyID`

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is

not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

`-tree TreeName`

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives). For example: `-tree /usr/temp` (UNIX system) and `-tree /temp/Filesystem/E` (Windows system).

`-into Pathname`

Restores the selected fileset into the given directory.

RAW DISK RESTORE

`-rawdisk Client Label`

Selects the disk image identified by *Client* and *Label* for restore.

`-session SessionID`

Specifies the session to be used for restore.

`-copyid CopyID`

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

`-section [ToSection=]Section`

Specifies the disk image section to be restored. To restore the section to a new section, include both the source and destination section.

NDMP RESTORE

`-full`

Specifies that the selected object will be restored from the last full backup and all incremental backups related to this full backup.

`-filesystem Client:MountPoint Label`

Selects the filesystem identified with *Client:MountPoint Label* for restore.

`-session SessionID`

Specifies the session to be used for restore.

`-tree TreeName`

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives).

For example: `-tree /usr/temp` (UNIX system) and `-tree /temp/Filesytem/E` (Windows system).

`-into Pathname`

Restores the selected fileset into the given directory.

`-ndmp_user UserName`

Sets the username that is used by Data Protector to establish the connection to the NDMP server.

`-ndmp_passwd Password`

Sets the password for the username that is used by Data Protector to establish the connection to the NDMP server.

`-ndmp_env FileName`

Specifies the filename of file with NDMP environment variables for specific NDMP implementations.

SAP R/3 FILE RESTORE

`-sap Client:Set`

Selects the SAP R/3 object identified by *Client:Set* for restore.

`-session SessionID`

Specifies the session to be used for restore.

`-copyid CopyID`

If several copies of the same object exist in one session as a result of the object copy or object mirror operation, this option identifies the specific object copy (object mirror or object copy) to be used for restore. By default (if this option is not specified), Data Protector selects the media set to restore from automatically. When using this option, it is necessary to specify both the object and the session.

`-tree TreeName`

Specifies the file, component, or tree to restore. Note that when specifying trees on UNIX systems, complete trees must be specified including the mount points, whereas on Windows systems, trees must be specified without volumes (drives).

For example: `-tree /usr/temp` (UNIX system) and `-tree /temp/Filesytem/E` (Windows system).

INFORMIX SERVER RESTORE

`-informix`

Selects the Informix Server object for restore.

`-barhost ClientName`

Specifies the Informix Server client from which the data was backed up.

`-barcmd PathName`

The value of the `barcmd` option has to be set to `ob2onbar.pl`. The command should reside in `/opt/omni/bin` directory on HP-UX systems and in `Data_Protector_home\bin` directory on Windows systems.

`-user UserName:GroupName`

Specifies *Username* and *GroupName* that started the script specified by the `-barcmd` option.

`-appname ApplicationDatabaseName`

Specifies the database server name of Informix Server to be restored.

`-bararg OnBarRestoreArguments`

Specifies the onbar restore arguments. Each onbar restore argument has to be put in double quotes.

MICROSOFT EXCHANGE SERVER RESTORE

`-msese`

Selects the Microsoft Exchange Server object for restore.

`-barhost ClientName`

Specifies the Microsoft Exchange Server client from which the data was backed up.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-appname full_application_name`

Specifies a Microsoft Exchange Server Information Store, Site Replication Service or Key Management Service for the restore. The name of the Store/Service (*full_application_name*) must be provided in double quotes as follows:

- For the Information Store: Microsoft Exchange Server (Microsoft Information Store)
- For the Site Replication Service: Microsoft Exchange Server (Microsoft Site Replication Service)
- For the Key Management Service: Microsoft Exchange Server (Microsoft Key Management Service)

`-base DBName`

Specifies the Microsoft Exchange Server 2000/2003 store or logs for restore.

`-session SessionID`

Specifies the session to be used for restore.

When restoring objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

This option must be set for every `-base` option specified.

`-logpath path`

Specifying this option, you set the temporary directory for the Microsoft Exchange Server log files. Data Protector restores the log files to this directory. Using this directory, the Microsoft Exchange Server then recovers the database - this operation is referred to as hard recovery.

`-last`

Hard recovery is performed after the restore of the Microsoft Exchange Server object. Use this option if you are restoring the last set of files. If you do not set this option, you have to start the recovery manually by running the `eseutil /cc /t` utility from the directory for temporary log files. If this option is not specified, soft recovery is performed after the restore.

`-mount`

The restored Microsoft Exchange Server databases will be automatically mounted after the soft or hard recovery.

`-consistent`

Restores the database to its last consistent state. The latest log files, created after backup, are applied to the restored database during recovery.

MICROSOFT EXCHANGE SINGLE MAILBOX RESTORE

`-mbx`

Selects Microsoft Exchange Server single mailboxes and Public Folders for restore.

`-barhost ClientName`

Specifies the Microsoft Exchange Server client from which the data was backed up.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-mailbox MailboxName`

Specifies the Microsoft Exchange Server single mailboxes for restore.

`-session SessionID`

Specifies the session to be used for restore.

When restoring objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

`-public`

Specifies the Microsoft Exchange Server Public Folders for restore (as part of the Microsoft Exchange Server single mailbox restore).

`-folder FolderName`

Specifies folders to be restored. Note that the subfolders are also restored. If this option is not specified, all backed up folders are restored.

`-exclude FolderName`

Specifies the folders to be excluded from restore.

`-originalfolder{-keep_msg | -overwrite_msg}`

If this option is selected, Data Protector restores Exchange Server items to the same folders in which they were when the backup was performed.

If `-keep_msg` is selected, the messages in the mailbox or Public Folders are not restored, even if they are different from their backed up version.

If `-overwrite_msg` is selected, all messages are restored, replacing their current versions (if they exist). If different versions of the same message exist in the mailbox or Public Folders (for example, if you have a copy of the message), only one is replaced with the backed up version and all other versions remain intact.

The messages in the mailbox that were not backed up in the specified backup session (or the restore chain of backup sessions) always remain intact.

If `-originalfolder` is not specified, Data Protector creates a new folder in the root of the mailbox or in the root of All Public Folders and restores Exchange items into it. For a mailbox restore, the folder is named `Data Protector BackupDate BackupTime`, and for a Public Folders restore, it is named `Data Protector BackupDate BackupTime - public folder`. If you restore a mailbox or Public Folders from the same backup several times, a number is appended to the folder name. For example, in the second restore session of a mailbox, the folder `Data Protector BackupDate BackupTime (1)` is created.

`-destmailbox DestMailboxName`

Specifies the destination mailbox, into which data will be restored. The destination mailbox must exist on the target Microsoft Exchange Server. If this option is not specified, data is restored to the original mailbox.

`-chain`

If this option is specified, data is restored not only from the specified backup session, but also from the latest full, the latest incremental1 (if exists), and all incremental backups from the last incremental1 up to the specified version.

LOTUS RESTORE

`-lotus`

Selects the Lotus Notes/Domino Server object for restore.

`-barhost ClientName`

Specifies the Lotus Notes/Domino Server client from which the data was backed up.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-parallelism n`

Sets the number of restore streams, running in parallel. The default is 1.

`-domino_server srv_name`

Sets the name of the Lotus Notes/Domino Server which you want to restore.

`-appname`

Specifies the Lotus Notes/Domino Server instance source.

`-db db`

Sets the restore of an individual Lotus Notes/Domino Server database.

`-NSF`

Sets the restore of all NSF (Notes Storage Facility) databases.

`-NTF`

Sets the restore of all NTF (Notes Templates Facility) files.

`-BOX`

Sets the restore of all BOX files.

`-ALL`

Sets the restore of all objects, NSF databases, NTF files and BOX files.

`-dir dir`

Sets the Lotus Notes/Domino data directories that you want to include in the restore. Enter their relative pathnames to the Lotus Notes/Domino data directory.

`-direx direx`

Sets the Lotus Notes/Domino data directories that you want to exclude from the restore. Enter their relative pathname to the Lotus Notes/Domino data directory.

`-r_dest restore_dir`

Sets the relative pathname to the restored database directory.

`-recover`

Specify this option to perform the recovery of the restored database to the last possible consistent state.

`-recovery_time yyyy/mm/dd.hh:mm:ss`

Sets a point in time to which you want the database to be recovered.

`-session SessionID`

Specifies the session to be used for restore.

When restoring objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

DB2 RESTORE

`-db2`

Selects the IBM DB2 UDB object to restore.

`-barhost ClientName`

Specifies the IBM DB2 UDB client from which the data was backed up.

`-instance InstName`

Sets the name of the database instance that was backed up.

`-dbname DBName`

Sets the name of the DB2 database that you want to restore.

`-newdbname NewDBName`

Specify this option if you want to restore the whole DB2 database into a new database.

`-tsname DBName*TSName`

Sets the name of the DB2 table space that you want to restore. To specify the table space you would like to restore, write the name of the database, then the "*" character and finally the name of the table space (without spaces).

`-logfile DBName*LogFileName`

Sets the name of the DB2 Log file that you want to restore. It should not be used with the `-rollforward` option. To specify the Log file you would like to restore, write the name of the database, then the "*" character and finally the name of the Log file (without spaces).

`-offline`

Specify this option if you want to restore a table space offline.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-rollforward [time: YYYY-MM-DD.hh.mm.ss]`

Specify the point in time when you want a rollforward to be performed to. The rollforward point in time *must* be entered in local time (as it is set on the DB2 target server) and not in coordinated universal time (UTC). If you specify a `rollforward` option without `time` argument, a rollforward will be performed to the end of the logs.

`-frominstance InstName`

Sets the name of the DB2 instance from which you want to restore the data.

VSS RESTORE

`-vss`

Selects the VSS object for restore.

`-barhost ClientName`

Specifies the system where the VSS agent or application agent is run.

`-session SessionID`

Specifies the session to be used for restore.

When restoring integration objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

`-tree TreeName`

Specifies the file, component, or tree to restore. For example, to specify a component, you can use: `-tree "/Microsoft Exchange Writer(Exchange Information Store)/Microsoft Information Store/First Storage Group/StoreOne"`

When specifying trees, trees must be specified without drive letter.

`-into Pathname`

Restores the selected files, component, or tree into the given directory.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-instant_restore`

Selects instant recovery for ZDB and VSS integrations.

`-conf_check {strict | non-strict | disabled}`

Sets the configuration check mode. With this option, Data Protector checks whether the individual components can be selectively restored using the instant recovery functionality. A check detects, whether there are more than one component on the volume and whether there is any data besides component's data. If the check fails, the instant recovery session will fail. Select the *strict* mode to check each file or directory. Select the *non-strict* mode to check each folder. Disable configuration check only if instant recovery cannot be performed with an enabled configuration check and only if you are sure that this will not result in a loss of data during the instant recovery. In this case, you will lose the data that does not belong to a component, but resides on the same volume.

`-no_recovery`

Leaves the application database in the recovery mode after completion of the instant recovery session, enabling you to manually apply transaction logs to the database.

This option is available only for the SQL Server writer and Microsoft Exchange Server 2007 writer. It is not supported for Microsoft Exchange Server 2003 writer, where the transaction logs are always applied when the store is mounted.

`-use_vds`

Switches a replica from the specified backup session with the source volume. Once switched, the replica is not available for another instant recovery session and also information about this replica is deleted from the database (VSSDB). Does not use a ZDB array specific options or agents.

On HP StorageWorks Disk Array XP, this option must be used after the backup created with the XP provider in the VSS compliant mode.

VSS_ENTERPRISE_VIRTUAL_ARRAY_OPTIONS

`-no_copy_back`

If this option is specified, a replica from the specified backup session is switched with the source volume. Once used, the replica is not available for another instant recovery session.

`-copy_back`

If this option is specified, copy back is performed. This is also the default behavior when neither `-no_copy_back` nor `-copy_back` is specified.

`-diskarray_wait Minutes`

If this option is specified, there is a delay before the background processes can run. The duration of the delay (in minutes) is determined by *Minutes*. This is also the default behavior when neither `-diskarray_wait` nor `-no_diskarray_wait` are specified, in which case there is a 60-minute delay.

`-delete_replica`

If this option is specified, the replica from which data was restored is deleted from the disk array after restore.

`-no_diskarray_wait`

If this option is specified, the background processes, such as integrity check, will not stop during the copy creation. This may cause a slowdown of the copy process.

`-no_retain_source`

Deletes the source volume during restore. If this option is used with `-copy_back`, the disk is overwritten during restore. Failure during such restore will cause the source volume data to be lost. If used with `-no_copy_back`, the disk is deleted after successful restore.

VSS_DISK_ARRAY_XP_OPTIONS

-copy_back

Performs resynchronization of the disk pair, copying data from the target volume (backup disk) to the source volume. This option must be specified if the data was backed up with VSS provider in the resync mode.

-no_retain_source

Deletes the source volume during restore. This option must be specified if the data was backed up with VSS provider in the resync mode since there is no possibility to retain the source during re-synchronization of replica and source disk.

-no_diskarray_wait

If this option is specified, the source volume is immediately available while the synchronization or copy process is running in the background (quick restore). The SSE Agent does not wait for the synchronization or copy process to complete. If this option is not specified, there is a 60-minute delay before the background processes can run.

VSS_EXCHANGE_SPECIFIC_OPTIONS

-exch_check

Performs the consistency check of the Microsoft Exchange Server database replicated datafiles. The Microsoft Exchange Server database backup is considered as successful only if the consistency check succeeds. Use this option if consistency check was not performed during backup.

-exch_throttle Value

Throttles down the consistency check to lessen impact on restore performance. Set the number of input/output operations, after which the check is stopped for one second.

VSS_EXCHANGE_2007_SPECIFIC_OPTIONS

-appsrv ClientName

Specifies the system to which the components are restored. If not specified, the components are always restored to the server from where they were backed up. Note that all objects in one restore session must be restored to the same system.

-target_tree TargetStoreName

Specifies the target component to which the source component will be restored and enables you to restore a subcomponent to a different component than the one from which it was backed up. This option can be used only once for each *-tree* option and cannot be specified together with *-exch_RSG*.

TreeName and its *TargetStoreName* pair must always be fully expanded subcomponents representing an Exchange store or logs. See also the Exchange 2007 examples. To get a list of available targets on a specific host, run the command:

```
vssbar -appsrv:HostName -perfrom:browse -all
```

Potential targets can be identified by the string "RESTOREMODE = 1".

NOTE: You cannot restore only a store without logs to a different location. If you specify a target store for an original store, you must also specify logs with an additional `-tree TreeName -target_tree TargetStoreName` pair.

The option must be specified together with `-target_dir`.

`-exch_RSG LinkedStoreName`

Creates a new Recovery Storage Group (RSG) and links it to *LinkedStoreName*. This option can be used only once for each `-tree` option and cannot be specified together with `-target_tree`. Only one storage group per session can be restored with this option due to an Exchange limitation. *LinkedStoreName* and its *TreeName* pair must always be fully expanded subcomponents, representing an Exchange store or logs. See also the Exchange 2007 examples.

IMPORTANT: If the RSG already exists, it is removed and a new one is created. Any existing data in it will be lost. NOTE: You cannot restore only a store without logs to a different location. If you specify a target store for an original store, you must also specify logs with an additional `-tree TreeName -target_tree TargetStoreName` pair.

The option must be specified together with `-target_dir`.

`-target_dir Directory`

During an instant recovery session, the replica will be mounted to *Directory*. The target directory for one session must always be the same, for example, you cannot specify one target directory for the store(s) and another one for the logs.

SAP DB/MAXDB RESTORE

`-sapdb`

Selects the SAP DB/MaxDB object for restore.

`-barhost ClientName`

Specifies the SAP DB/MaxDB client from which the data was backed up.

`-instance InstName`

Sets the name of the database instance that was backed up.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-newinstance DestinationInstanceName`

Performs a restore to the SAP DB/MaxDB instance with the instance name *DestinationInstanceName*. This option is to be used only when a restore to an instance other than the one that was backed up is to be performed. Note that the specified instance must already exist and must be configured for use with Data Protector. This option does not create a new instance.

`-session SessionID`

Specifies the session to be used for restore.

When restoring objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

If this option is not specified, the last backup session is restored regardless of the `-endlogs` or the `-time` option selection.

`-recover [-endlogs | -time: YYYY-MM-DD.hh.mm.ss]`

Specify this option to recover the restored SAP DB/MaxDB database by applying the restored (if the `-from_disk` option is not specified) or client-resident logs (if the `-from_disk` option is specified) to the last available log (the default behavior, or if the `-endlogs` option is specified), or to the specified point in time (if the `-time:` option is specified).

Make sure that the backup session selected by the `-session` option will restore enough data for the integration to apply the redo logs until the last available log or until the specified point in time.

When this option is not specified, the following happens after the restore:

- If archive logs are not restored (if restore from a full backup session is performed), the database remains in the *Admin* mode after the restore.
- If archive logs are restored, the database is, if the restored archive logs allow it, switched to the *Online* mode. If the database, however, cannot be switched to the *Online* mode (because the restored archive logs do not allow it), it remains in the *Admin* mode.

`-endlogs`

Specify this option to recover the database until the last log. This is the default option.

`-time: YYYY-MM-DD.hh.mm.ss`

Specify the `-time:` option to recover the database until the point specified by the `YYYY-MM-DD.hh.mm.ss` argument.

Note that the specified time is the system time on the system running the Data Protector CLI. If the system to be recovered is not in the same time zone as the system running the Data Protector CLI, the point of recovery is adjusted to the local time setting on the system to be restored.

`-from_disk`

Specify this option to apply the existing archive logs on the SAP DB Server to SAP DB Server redo logs.

If this option is not specified, the backed up archive logs on backup media are applied to the redo logs (if trans backup session is restored), or the redo logs are left intact together with the existing archive logs on the SAP DB Server (if full or diff backup session is restored).

When a transactional backup session is selected for restore or when it is a part of the needed restore chain, and the this option is specified at the same time, the archive logs from Data Protector media are applied to the redo logs.

Thereafter, the archive logs on the SAP DB Server are applied to redo logs.

This option is ignored in case of SAP DB migration, thus allowing only for the restore of redo logs from the backed up archive logs on backup media (if trans backup session is restored).

`-nochain`

This option instructs the command to restore only the selected or last backup session; the integration does not restore the whole restore chain of full, differential, and transactional backups.

MICROSOFT SQL SERVER RESTORE

`-mssql`

Selects the Microsoft SQL Server object, identified with *DBName* for restore.

`-barhost ClientName`

Specifies the Microsoft SQL Server client from which the data was backed up.

`-destination ClientName`

Specifies the target client for restore. Use this option only when you restore to some other instance than the one that was backed up.

`-instance SourceInstanceName`

Sets the name of the Microsoft SQL Server instance to be restored. *Omnir* takes the (DEFAULT) instance by default.

`-destinstance DestinationInstanceName`

Specify this option to determine an Microsoft SQL Server instance into which the data will be restored. *Omnir* takes the (DEFAULT) instance by default.

`-base DBName`

Specifies the SQL Server database for restore. The database name is case-sensitive.

`-session SessionID`

Specifies the session to be used for restore.

When restoring objects that have copies, do not use the object copy session ID, but the object's *BackupID*, which equals the object's backup session ID.

`-datafile GroupName/DataFileName`

Specifies an SQL Server data file for restore. *GroupName* is the name of the group the data file belongs to.

`-asbase NewDBName {-file LogicalFileName1 PhysicalFileName1
[-file LogicalFileName2 PhysicalFileName2]...}`

This option can only be used for database restore.

Enables restore of the Microsoft SQL Server database under a new name and restore of files to a new location. If the `-asbase` option is used, all logical and physical filenames have to be specified with the `-file` option.

`-replace`

If the specified Microsoft SQL Server database already exists on the specified client, it is overwritten.

`-nochain`

Microsoft SQL Server only: Restores only the session identified by the `-session sessionID` option. If no *sessionID* is specified, only the latest session is restored.

`-recovery {rec | norec}`

Specifies the state (recovered, nonrecovered) of the Microsoft SQL Server database after the restore. The default value for this option is *rec*.

`-stopat yyyy/mm/dd.hh:mm:ss`

This option is only available for database objects.

Specifies the exact time when the rollforward of transactions will be stopped. Therefore, to enable database recovery to a particular point in time, the backup you restore from must be a transaction log backup.

You cannot use this option with *norecovery* or *standby*. If you specify a stop at time that is after the end of the restore log operation, the database is left in a non-recovered state (as if the restore log is run with *norecovery*).

`-standby File`

This option can only be used for database restore.

Specifies the standby state of the Microsoft SQL Server database after the restore.

VMWARE VIRTUAL INFRASTRUCTURE RESTORE

`-vmware`

Selects the VMware Virtual Infrastructure object for restore.

`-barhost OriginalVMwareManagementClient`

- Specifies the VMware management client that was used during backup.
- instance *OriginalDatacenter*
 - Specifies the datacenter from which the virtual machines were backed up.
- method *Method*
 - Specifies the method that was used for backup.
- session *SessionID*
 - Specifies the backup session to be used for restore.
- all
 - Restores all the virtual machines from the specified backup session.
- vmfolder *VMfolder*
 - Restores only the virtual machines from the specified folder.
- exclude *VMfolder*
 - Excludes from restore all the virtual machines located in *VMfolder*.
- vm *VM*
 - Restores the specified virtual machine.
- disk *Disk*
 - Restores only an individual virtual machine disk of each virtual machine.
- target *TargetClient*
 - Specifies the client to which to restore filesystems of virtual machines.
- file *File*
 - Restores only an individual file or folder of each virtual machine.
 - Provide the complete pathname of a file or folder, using slashes instead of backslashes to separate folders. Also, omit the colon that follows the disk partition letter. For example, to restore the file C:\Test\hello.txt, specify -file C/Test/hello.txt.
- destination *RestoreClient*
 - Specifies the client that the restore session is started on. If this option is not specified, the session is started on the same client on which the backup was started.
 - Use this option in the case of a disaster recovery when you restore from a Suspend, Snapshot, or VCBimage backup and the new VMware management client does not have the same name as the original one. Ensure that the new client is configured for use with the Data Protector VMware Virtual Infrastructure integration and has access to all the required datastores.
 - You can also use this option to restore the virtual machines outside of a datacenter, in which case you must specify the client to restore to.

`-newinstance TargetDatacenter`

Specifies the datacenter that the virtual machines are restored to. By default, the virtual machines are restored to the original datacenter. Use this option in the case of a disaster recovery when the new datacenter does not have the same name as the original one.

You can also use this option to restore the virtual machines outside of a datacenter, in which case you must specify `-newinstance "None"`.

This option is not applicable if you restore from a `VCBfile` backup.

`-consolidate`

Removes all existing virtual machine snapshots (including non-Data Protector ones) after the restore completes. It means that all the changes made on the active snapshot branch are committed to the virtual machine base.

`-memory`

Restores also the virtual machine memory file if it was backed up.

`-register`

Enables you to restore virtual machines to datacenters in which virtual machines with such names are not registered. If this option is not specified, unregistered virtual machines are not restored.

`-poweron`

Puts the newly restored virtual machines online when the session completes.

`-overwrite [older]`

This option has different meanings, depending on whether you restore from a Snapshot, Suspend, `VCBimage`, or `VCBfile` backup:

Snapshot, Suspend, `VCBimage`: If the virtual machines to be restored already exist in the destination, Data Protector unregisters such virtual machines, deletes their files, and then restores them from the backup. If this option is not specified or if you specify `-overwrite older`, the existing virtual machines remain intact. They are not restored from the backup.

Note that if you restore from a Snapshot, Suspend, or `VCBimage` backup, and at the same time you specify `-newinstance "None"`, the same description applies as if you restored from a `VCBfile` backup.

`VCBfile`: If the files to be restored already exist in the destination, Data Protector overwrites them with the files from the backup. If you add `older`, the files are overwritten only if they are older than the files from the backup. Otherwise, they remain intact: they are not restored from the backup. If this option is not specified, the existing files remain intact: they are not restored from the backup.

MICROSOFT SHAREPOINT PORTAL SERVER RESTORE

`-mssps`

Selects the Microsoft SharePoint Portal Server object for restore.

`-barhost ClientName`

Specifies the front-end Web server system that was used during backup.

`-changemaster`

Applicable only if the Microsoft SharePoint Portal Server farm is centralized (having the master and child portals). If you are restoring the master portal and you specify this option, the current master portal becomes a child of the restored master portal. By default, the old master portal is restored as a child on the current master portal.

`-portal VirtualServer { [-teamdb DBName MSSPS_SQL_OPTIONS]`

`...`

`[-index INDEX_OPTIONS] [-sitedbs SITEDBS_OPTIONS] }`

Specifies portal objects for restore. You need to specify at least one SPS object: either a team database, index server, or site databases.

`-session SessionID`

Specifies the session to be used for restore.

`-ssodb`

Specifies the Microsoft SharePoint Portal Server single sign-on database for restore.

`-doclib`

Specifies the Microsoft SharePoint Portal Server document library for restore.

`-tohost Client`

Specifies the client to restore to. When you restore Microsoft SQL Server databases, the client must be an SQL Server system.

`-instance Instance`

Specifies the Microsoft SQL Server instance to restore to.

`-as NewDBName`

Enables you to restore the Microsoft SQL Server database under a different name. By default, Microsoft SQL Server databases are restored with the same names.

`-todir Directory`

Specifies a directory to restore to. By default, index servers are restored to their original directories.

INSTANT RECOVERY

`-instant_restore`

Restores data on a disk array using instant recovery.

`-host ClientName`

Restores all objects of the specified client that were backed up in the specified session.

`-session SessionID`

Specifies the session to be used for restore.

ENTERPRISE_VIRTUAL_ARRAY_OPTIONS

`-check_config`

If this option is set, the current volume group configuration of the volume groups involved in the instant recovery session is compared with the volume group configuration during the ZDB-to-disk or ZDB-to-disk+tape session kept in the ZDB database (EVADB or SMISDB). If the volume group configuration has changed since the ZDB-to-disk or ZDB-to-disk+tape session, the restore is aborted.

When instant recovery is performed in an MC/ServiceGuard cluster to some other node than the one that was backed up, the current volume group configuration on the node to which instant recovery is to be performed is different from the volume group configuration kept in the ZDB database. In such a case the ZDB database volume group configuration data is replaced by the current volume group configuration data on the node to which instant recovery is to be performed and the session is not aborted.

When performing instant recovery in an MC/ServiceGuard cluster to some other node than the one that was backed up, select this option.

`-force_prp_replica`

If this option is selected and if any target volume to be restored is presented to any system, the SMI-S Agent removes these presentations. If the option is not selected and a presentation exists, the instant recovery session is aborted.

VIRTUAL_ARRAY_OPTIONS

`-keep_version`

If this option is set, the replica from which the data was restored is left on the disk array after the restore is finished.

`-check_config`

If this option is set, the current volume group configuration of the volume groups involved in the instant recovery session is compared with the volume group configuration during the ZDB-to-disk or ZDB-to-disk+tape session kept in the ZDB database (VADB or SMISDB). If the volume group configuration has changed since the ZDB-to-disk or ZDB-to-disk+tape session, the restore is aborted.

When instant recovery is performed in an MC/ServiceGuard cluster to some other node than the one that was backed up, the current volume group configuration on the node to which instant recovery is to be performed is different

from the volume group configuration kept in the VADB. In such a case the VADB volume group configuration data is replaced by the current volume group configuration data on the node to which instant recovery is to be performed and the session is not aborted.

When performing instant recovery in an MC/ServiceGuard cluster to some other node than the one that was backed up, select this option.

The CRC check information for the data on the original volumes in the VADB is compared to the CRC check information for the data in the selected replica. If the items compared do not match, the session is aborted.

DISK_ARRAY_XP_OPTIONS

-keep_version

If this option is set, the LDEV pairs involved in the current instant recovery session are split after the restore is finished.

-check_config

If this option is set, the current volume group configuration of the volume groups involved in the instant recovery session is compared with the volume group configuration during the split mirror backup session kept in the XPDB.

If the volume group configuration has changed since the split mirror backup session, the session is aborted.

When instant recovery is performed in an MC/ServiceGuard cluster to some other node than the one that was backed up, the current volume group configuration on the node to which instant recovery is to be performed is different from the volume group configuration kept in the XPDB. In such a case the XPDB volume group configuration data is replaced by the current volume group configuration data on the node to which instant recovery is to be performed and the session is not aborted.

When performing instant recovery in an MC/ServiceGuard cluster to some other node than the one that was backed up, select this option.

The CRC check information for the selected LDEV stored in the XPDB database is compared to the current CRC check information. If the items compared do not match, the session is aborted.

A RAID Manager Library flag, which is set whenever the selected mirror LDEV is accessed/changed by any (including non-Data Protector) process is checked. If the flag is set, the session fails with an appropriate warning.

ORACLE/SAP_SPECIFIC_OPTIONS

-oracle

Selects the Oracle options for instant recovery.

-sap

Selects the SAP R/3 options for instant recovery.

`-recover {now | time Time | logseq LogSeqNum
thread ThreadNum | SCN Number}`

Selects the point in time to which the database is recovered. The following options are available:

`now`

All existing archive logs are applied.

`time MM/DD/YY hh:mm:ss`

Specifies an incomplete recovery. Archive logs are applied only to a specific point in time.

`logseq LogSeqNum thread ThreadNum`

Specifies an incomplete recovery. Archive logs are applied only to the specified redo log sequence and thread number.

`SCN Number`

Specifies an incomplete recovery. The archive logs are applied only to the specified SCN number.

`-open`

Opens the database after recovery.

`-resetlogs`

Resets the logs after the database is opened. Available only if the `-open` option is specified. This option is not available if the `-recovery` option is set to `now`.

The following are recommendations on when to reset the logs.

Always reset the logs:

- After an incomplete recovery, that is if not all archive redo logs will be applied.
- If a backup of a control file is used in recovery.

Do not reset the logs:

- After a complete recovery where a backup of a control file is not used in recovery.
- If the archive logs are used for a standby database. If you must reset the archive logs, then you have to recreate the standby database.

`-user UserName -group GroupName`

Specifies the username and group name of the account under which Data Protector starts instant recovery. Required only for UNIX clients.

`-apname ApplicationDatabaseName`

Name of the backed up database.

`-parallelism Number`

Selects the parallelism for the restore of archive logs and restore from incremental backups.

DATA_OPTIONS

`-exclude TreeName`

Excludes the specified tree from the restore. This option is not supported with the Data Protector NDMP server integration.

`-skip MatchPattern`

Excludes files matching *MatchPattern* from restore. This option is not supported with Data Protector NDMP server integration.

`-only MatchPattern`

Restores only files that match the given *MatchPattern*. This option is not supported with Data Protector NDMP server integration.

`-as Pathname`

Restores the selected fileset as the specified tree.

`-into Pathname`

Restores the selected fileset into the given directory.

SESSION_OPTIONS

`-preview`

Checks the restore parameters without performing the actual restore.

`-report{warning | minor | major | critical}`

Sets the level of error notification for the session. Errors are classified (in ascending order) as: warning, minor, major and critical. When you select a level, errors of this level and higher are displayed in the Monitor window. For example, if major is selected, only major and critical errors are reported. By default, all errors are reported.

MEDIUM_OPTIONS

`-device BackupDevice`

Specifies the backup device where the backup medium is mounted.

`-medium MediumID`

Specifies the medium from which data will be restored.

This option is not possible when performing a parallel restore.

`-slot SlotID [Side]`

Specifies the *SlotID* of the tape library unit where the medium is mounted. This option is only valid for this backup device type. To specify the side of the platter

in this slot, use the additional *Side* parameter. Slot *Side* must be specified for MO devices. Values for side are A or B.

`-id DiskAgentID`

Specifies the ID of the disk agent which should be used for restore.

FILESYSTEM_OPTIONS

`-touch`

Updates the access date/time of the file during the restore. By default the access date/time of the backup version is used.

This option is not supported on Novell NetWare.

`-lock`

When performing a restore of a file, the disk agent tries to lock the file. By default the file is not locked.

`-no_protection`

Do not restore protection of the backed up files, instead use the default protection settings.

`-overwrite`

Overwrites files with the same name in the specified fileset on the disk.

`-no_overwrite`

Does not overwrite existing files with the same name.

`-merge`

This option merges files from the backup medium to the target directory and replaces older versions that exist in the directory with newer (if they exist on the medium) files. Existing files are overwritten if the version on the medium is newer than version on disk. No existing directory is deleted.

If a directory or file doesn't exist on disk (but is on the backup medium) it is restored (created).

`-catalog`

Displays the restored files and directories.

`-sparse`

Restores sparse files in their original form.

`-move_busy`

This option is useful only in case the option `-overwrite` is specified. A problem can occur if, for example, a file to be overwritten cannot be deleted because it is currently in use. Setting this option causes busy files to be moved to a filename starting with #. The original file can thus be deleted as the lock is transferred to

the corresponding file starting with # sign. For example,
/tmp/DIR1/DIR2/FILE would be moved to /tmp/DIR1/DIR2/#FILE.

-vsr_only

A Novell NetWare specific option, allowing a restore of volume space restrictions on NetWare or NSS volume without restoring any other data. This option works only if volume object is selected for restore. If volume object is not selected for restore, the `-vsr_only` option does not affect the restore process.

-trustee

A Novell Network specific option, allowing a restore of inheritance filters and ownership information of the selected objects only. If enabled, Conflict Handling options are also enabled.

-no_share[_info]

If this option is specified, share information for directories on Windows is not restored. If a directory was shared on the network when a backup was run with the `Backup share information for directories` option set (by default), it will be automatically shared after restore, unless this option is selected for restore.

-omit_unrequired_object_versions

This option applies if you select directories for restore and the backup was performed with the logging level `-log` or `-log_files`. If specified, Data Protector checks in the IDB for each backup in the restore chain if there are any files to restore. Backups with no object versions to restore are skipped. Note that this check may take some time. If not specified, each backup in the restore chain is read, even if there was no change since the previous backup. To restore empty directories, do not specify this option.

-[no_]resumable

By default, Data Protector creates checkpoint files during the restore session. The checkpoint files are needed if the restore session fails and you want to restart the failed session, using the Data Protector resume session functionality. If you specify the option `-no_resumable`, the checkpoint files are not created.

If you have changed the default using the global option `ResumableRestoreDefault`, specify the option `-resumable` if you want checkpoint files to be created.

SPLIT_MIRROR_OPTIONS

-sse

Selects the HP StorageWorks Disk Array XP split mirror restore.

-symmetrix

Selects the EMC Symmetrix split mirror restore.

`-remote ApplicationClient BackupClient`

If the `-symmetrix` option was specified, this option selects the EMC Symmetrix Remote Data Facility (SRDF) split mirror configuration. If the `-sse` option was specified, this option selects the HP StorageWorks Continuous Access (CA) split mirror configuration.

`-local ApplicationClient BackupClient`

If the `-symmetrix` option was specified, this option selects the EMC Symmetrix Time Finder split mirror configuration. If the `-sse` option was specified, this option selects the HP StorageWorks Business Copy (BC) split mirror configuration.

`-combined ApplicationClient BackupClient`

If the `-symmetrix` option was specified, this option selects the EMC Symmetrix combined (SRDF & Time Finder) split mirror configuration. If the `-sse` option was specified, this option selects the HP StorageWorks combined (CA+BC) split mirror configuration.

`-mirrors list`

Specify a specific first level mirror to be used in the restore session, or a range or a sequence of first level mirrors to define a replica set from which the integration, according to the replica set rotation, selects one mirror to be used in the restore session. If this option is not specified, the MU# 0 is set.

`-quiesce cmd`

Sets the command/script to be run before links are split. You must create the command/script in the `/opt/omni/sbin` (HP-UX or Solaris systems) or in the `Data_Protector_home\bin` (Windows systems) directory of the application system. The command/script is used for stopping the application and unmounting file systems that are not to be restored in the active session and to prepare volume groups for deactivation.

`-restart cmd`

Sets the optional restart application command/script. Create this command/script in the `/opt/omni/sbin` (HP-UX or Solaris) or in the `Data_Protector_home\bin` (Windows) directory of the application system. The restart application command/script is executed on the application system immediately after the links are resynchronized. It can be used, for example, to restart the application or to mount a filesystem.

`-discovery`

This option is possible only for the EMC Symmetrix split mirror restore. The option builds or re-builds the Data Protector Symmetrix database on both the application and backup systems. Its functionality is the same as that of the Data Protector `Syma -init` command. (Refer to the *HP Data Protector zero downtime backup administrator's guide*).

`-re-establish_links_before_restore`

This option is used to synchronize split disks, that is, to move data to backup disks. This is necessary to prepare the disks for restore and to enable accurate restores. If the mirrored disks were split before the restore, and only some files need to be restored, then this option can be used to update the backup system. This will ensure that the correct data is resynchronized to the application system. This option is not set by default.

`-disable_disks`

Disks on the application system are disabled, that is, the filesystems are dismounted and volume groups are deactivated. This is performed before the split. The disks are enabled after the links are restored. Note that only filesystems selected for restore are dismounted. If other filesystems exist in the volume or disk group, the stop/quiesce application command/script and restart application command/script must be created to dismount these filesystems. You must always select this option for restore when you want to move data from the backup to the application system, that is, to incrementally restore links. The application system disks have to be disabled to provide data integrity after the links are restored, that is, data is moved.

`-restore_links_after_restore`

With this option enabled, the HP StorageWorks Disk Array XP agent incrementally restores links for LDEVs that were successfully restored by Data Protector to the backup system. The HP StorageWorks Disk Array XP agent also incrementally re-establishes links for LDEVs that were not successfully restored by Data Protector to the backup system.

GENERAL_OPTIONS

`-device BackupDevice`

Specifies the backup device where the backup medium is mounted.

`-no_auto_device_selection`

If this option is specified, Data Protector does not automatically replace unavailable devices with available devices of the same device tag.

`-server ServerName`

Selects the Cell Manager with the client name *ServerName* as the Cell Manager. Use this option to perform a restore to a client that is not in the current Data Protector cell.

`-target Client`

Restores the selected fileset to the specified client.

`-profile`

Displays restore statistics.

`-load{low | medium | high}`

Specifies the level of network traffic generated by a session during a time period. `High` level generates as much traffic as allowed by the network, resulting in a faster restore. A `low` level has less impact on network performance, but results in a slower restore. By default, this option is set to `high`.

`-pre_exec PathName`

Instructs the Disk Agent to execute this command before restoring the data object. The complete pathname of the command should be specified.

`-post_exec PathName`

Instructs the Disk Agent to execute this command after restoring the data object. The complete pathname of the command should be specified.

`-variable VariableName VariableValue`

This option lets you specify a variable name and its value for proper operation of some platforms and integrations, for example, for backing up and restoring data on MPE/iX System. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

`-no_monitor`

By default the command monitors the session and displays all messages. If this option is used, the command displays only the sessionID.

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omnior` command are:

- | | |
|----|---|
| 10 | There was an error while restoring some files. All agents completed successfully. |
| 11 | One or more agents failed, or there was a database error. |
| 12 | None of the agents completed the operation. |
| 13 | Session was aborted. |

EXAMPLES

The following examples illustrate how the `omnir` command works.

1. To restore trees `"/tree1"` and `"/tree2"` of the root filesystem on `"fs"`, with the label `"lb1"`, from the session `"2007/07/12-33"`, as the trees `"/tmp/tree1"` and `"/tmp/tree2"`, skipping `".xyz"` files, run:

```
omnir -filesystem fs:/ lb1 -session 2007/07/12-33 -tree  
/tree1 -as /tmp/tree1 -tree /tree2 -as /tmp/tree2 -skip  
*.xyz
```

2. To perform a full restore of tree `"/ac"` on filesystem `"bb:/"`, with no label, from the session `"2007/07/12-2"`, run:

```
omnir -filesystem bb:/ -full -session 2007/07/12-2 -tree  
/ac
```

3. To perform restore of the section `"/dev/rdisk/c201d6s0"` of the disk image labeled `"RawRoot"` on the client `"machine"` from the session `"2007/07/23-12"`, run:

```
omnir -rawdisk machine "RawRoot" -section  
/dev/rdisk/c201d6s0 -session 2007/07/23-12
```

4. To restore an IDB on the client `"server"` and pathname `"/usr/omni/config"` from the session `"2007/07/24-2"`, run:

```
omnir -omnidb server:/ -session 2007/07/24-2 -tree / -into  
/tmp/omnidb
```

5. To use parallel restore for restoring two objects, run:

```
omnir -filesystem client1:/ -session 2007/04/17-2 -tree  
/users -into /tmp -filesystem client2:/opt -session  
2007/04/17-3 -tree /opt -into /tmp
```

6. To perform an instant recovery to the system named `"machine"` from the backup session `"2007/08/08-1"`, keeping the replica on the backup system disk, run:

```
omnir -host machine -session 2007/08/08-1 -instant_restore  
-keep_version
```

7. To perform an instant recovery of filesystem backup data on HP StorageWorks Disk Array XP or HP StorageWorks Virtual Array to the system named `"computer"` from the backup session `"2008/01/02-1"`, keeping the replica on the backup system disk, run:

```
omnir -host computer -session 2008/01/02-1 -instant_restore  
-keep_version
```

8. To perform an instant recovery on HP StorageWorks Enterprise Virtual Array to the system named "computer" from the backup session "2008/01/08-1" and to perform volume group configuration check, run:

```
omnir -host computer -session 2008/01/08-1 -instant_restore  
-check_config
```

9. To perform a point in time recovery of the database "dbase.nsf" and all Lotus Notes/Domino Server NTF files of the Lotus Notes/Domino Server "BLUE" from the system "computer", to the original location with parallelism 4, run:

```
omnir -lotus -barhost computer -domino_server BLUE  
-parallelism 4 -db dbase.nsf -NTF -recovery_time  
2007/09/15.15:00:00
```

10. To perform an Informix Server restore of the database server "ol_computer" on the UNIX system "computer" with the bar argument "-r rootdbs", run:

```
omnir -informix -barhost computer -barcmd ob2onbar.pl  
-user informix:informix -bararg "-r rootdbs" -appname  
ol_computer
```

11. The Microsoft Information Store with the "/First Storage Group/STORE/Public Folder Store" store and "/First Storage Group/LOGS/Logs" logs is to be restored to the system called "computer.company.com" (where it was backed up), using the Data Protector session with the session ID "2007/07/07-13". The Microsoft Exchange Server log files are to be restored to "c:\temp" directory, the hard recovery is to be performed after the restore has finished. The database is to be mounted after the hard recovery. Run:

```
omnir -msese -barhost computer.company.com -appname  
"Microsoft Exchange Server(Microsoft Information Store)"  
-base "/First Storage Group/LOGS/Logs" -session  
"2007/07/07-13" -base "/First Storage Group/STORE/Public  
Folder Store" -session "2007/07/07-13" -logpath c:\temp  
-last -mount
```

12. VMware Virtual Infrastructure restore: Suppose you want to restore the complete virtual machine "/vm/MachineA" and only individual disks ("scsi0:0" and "scsi0:1") of the virtual machine "/vm/MachineB". At the time of backup, the virtual machines were running on the ESX Server systems that belonged to the datacenter "/MyDatacenter" managed by the VirtualCenter system "Virtualcenter.company.com". The virtual machines were backed up with the "Suspend" backup method and you want to restore to the original location, using the backup session "2008/07/14-1". If, in this session, virtual machine memory files were also backed up, you want to restore them as well. You also

want to ensure that the newly restored virtual machines are put online when the session completes. Run:

```
omnir -vmware -barhost Virtualcenter.company.com -instance  
/MyDatacenter -method Suspend -session 2006/2/7-31 -vm  
/vm/MachineA -vm /vm/MachineB -disk scsi0:0 -disk scsi0:1  
-memory -poweron
```

- 13.** VMware Virtual Infrastructure restore: Suppose the virtual machines "/MyVirtualMachines/machineA" and "/MyVirtualMachines/machineB" were backed up in the session "2009/8/14-5" from the datacenter "/MyDatacenter" that is managed by the VirtualCenter Server system "VirtualCenter.company.com", using the "VCBImage" backup method. To restore the virtual machines outside of a datacenter, to the directory "C:\tmp" on the VCB proxy system "proxy.company.com", set the VCB proxy system omnirc OB2_VMWARE_PATH variable to "C:\tmp" and run:

```
omnir -vmware -barhost VirtualCenter.company.com -instance  
/MyDatacenter -method VCBImage -session 2009/8/14-5 -vm  
/MyVirtualMachines/machineA -vm /MyVirtualMachines/machineB  
-destination proxy.company.com -newinstance "None"
```

- 14.** VMware Virtual Infrastructure restore: Suppose you want to restore all filesystems of all the virtual machines contained in the Virtual Infrastructure inventory folder "/MyVirtualMachines", except the filesystems of the virtual machine "/MyVirtualMachines/MachineA". The restore destination is the Windows client "computer1.company.com". In addition, you want to restore the "C:\Documents and Settings" folder and the file "C:\Test\Schedule.txt" of the virtual machine "/MyVirtualMachines2/MachineB" back to the same virtual machine "MachineB.company.com". The virtual machines were backed up from the datacenter "/MyDatacenter" that was managed by the VirtualCenter system "VirtualCenter.company.com". You want to restore from the last backup session. Run:

```
omnir -vmware -barhost Virtualcenter.company.com -instance  
/MyDatacenter -method VCBfile -vmfolder /MyVirtualMachines  
-exclude /MyVirtualMachines/MachineA -target  
computer1.company.com -vm /MyVirtualMachines2/MachineB  
-target MachineB.company.com -file "C/Documents and  
Settings" -file C/Test/Schedule.txt
```

- 15.** To perform a VSS restore of the "Registry Writer" and "System Writer" trees from the backup session "2007/10/20-3" and the "Event Log Writer" tree from the backup session "2007/10/27-1" to the client "daneel" into the "c:\tmp" directory, run:

```
omnir -vss -barhost daneel -session 2007/10/20-3 -tree
/"Registry Writer" -tree /"System Writer" -session
2007/10/27-1 -tree /"Event Log Writer" -into c:\tmp
```

- 16.** To start an online restore of a DB2 database called "TEMP" from instance "DB2Inst" on the client "splendid" and roll it forward till the 10th January 2007, 9:15 a.m., run:

```
omnir -db2 -barhost splendid -instance DB2Inst -dbname
TEMP -rollforward -time 2007-01-10.09.15.00
```

- 17.** To restore the contents of a mailbox called "FIRST" residing on an Microsoft Exchange Server system called "infinity.ipr.hermes", with the backup session ID 2007/01/10-1, into the new mailbox called "TEMP", run:

```
omnir -mbx -barhost infinity.ipr.hermes -mailbox FIRST
-session 2007/01/10-1 -destmailbox TEMP
```

- 18.** To restore all messages from the "Inbox" folder (and all subfolders) from the "User 1" mailbox residing on the Microsoft Exchange Server system called "exchange.hp.com", into the original location, using the backup made in the session "2007/03/10-18", without overwriting the messages, run:

```
omnir -mbx -barhost exchange.hp.com -mailbox "User 1"
-session 2007/03/10-18 -folder Inbox -originalfolder
-keep_msg
```

- 19.** To restore all messages from the "User 2" mailbox residing on the Microsoft Exchange Server system called "exchange.hp.com", except for the messages in the folder "Deleted Items", into a new location, using the backup made in the session "2007/03/10-19" (for example, performed at 13:47:00), run:

```
omnir -mbx -barhost exchange.hp.com -mailbox "User 2"
-session 2007/03/10-19 -exclude "Deleted Items"
```

The messages will be restored in the "Data Protector 03/10/03 13:47:00" mailbox on the "exchange.hp.com" Microsoft Exchange Server.

- 20.** To start an online restore of a SAP DB/MaxDB database called "TEMP" on the client "splendid" and roll it forward till the 10th January 2007, 9:15 a.m. from the archive logs already residing on the client, run:

```
omnir -sapdb -barhost splendid -instance TEMP -recover
-time: 2007-01-10.09.15.00 -from_disk
```

- 21.** On Disk Array XP, to recover an Oracle database "DB1" on the Windows client "san32", from the session "2008/02/05-18", until the most recent time, and to open the database after the recovery, and to keep the replica on the disk array, and to set parallelism to 1, run:

```
omnir -host san32 -session 2008/02/05-18 -keep_version  
-recover disk now -appname DB1 -parallelism 1 -open
```

- 22.** To perform restore of the section `"/dev/rdisk/c201d6s0"` of the disk image labeled `"Raw"` on the client `"system1"` from the session `"2007/07/23-12"` using the media set containing the object copy with ID `"132123"`, run:

```
omnir -rawdisk system "Raw" -section /dev/rdisk/c201d6s0  
-session 2007/07/23-12 -copyid 132123
```

- 23.** To start instant recovery of data on the HP StorageWorks Enterprise Virtual Array on the system named `"system1"` from the VSS backup session `"2007/08/08-14"` which copies the data from the replica to the source disk group overwriting the source volume, execute the following command:

```
omnir -vss -barhost system1 -session 2007/08/08-14  
-copy_back -no_retain_source
```

- 24.** To restore the `SqlServerWriter` from the VSS backup session `"2007/08/07-9"` on the system named `"system1"` using the Microsoft Virtual Disk Service with the possibility to later apply transaction logs on the SQL Server, execute the following command:

```
omnir -vss -instant_restore -use_vds -barhost system1  
-session 2007/08/07-9 -tree "/SqlServerWriter(SQL Server  
2005:SQLWriter)" -no_recovery
```

- 25.** Exchange 2007 VSS restore to a different storage group:

To restore the Exchange 2007 Writer logs on the system `"exch2007.company.com"` from the storage group copy `"Replicated Storage Group"` created by LCR, from the session `"2007/04/08-12"`, to storage group `"Original Storage Group"`, and with the files restored in the `"C:\Omni"` directory, execute the following command:

```
omnir -vss -use_vds -barhost exch2007.company.com -session  
2007/04/08-12 -tree "/Microsoft Exchange Writer(Exchange  
Replication Service)/Microsoft Information Store/Replicated  
Storage Group/Logs" -target_tree "/Microsoft Exchange  
Writer(Exchange Information Store)/Microsoft Information  
Store/Original Storage Group/Logs" -target_dir "C:\Omni"
```

- 26.** Exchange 2007 VSS instant recovery to a non-Exchange location:

To perform instant recovery of the Exchange 2007 Writer store `"StoreOne"` from the storage group `"First Storage Group"` from the backup session `"2007/04/08-9"` on the system `"exch2007.company.com"`, to the system `"server2"`, and with the replicas mounted to `"C:\Omni_Mnt"`, run:

```
omnir -vss -instant_restore -use_vds -barhost
exch2007.company.com -appsrv server2 -session 2007/04/08-9
-tree "/Microsoft Exchange Writer(Exchange Information
Store)/Microsoft Information Store/First Storage
Group/StoreOne" -target_dir "c:\mnt" -tree "/Microsoft
Exchange Writer(Exchange Information Store)/Microsoft
Information Store/First Storage Group/Logs" -target_dir
"C:\Omni_Mnt"
```

27. Exchange 2007 VSS restore to a non-Exchange location and creating RSG:

To restore the Exchange 2007 Writer store "Store One" from the storage group named "First Storage Group" from the backup session "2007/04/10-9" on the system "exch2007.company.com" , and to create the Recovery Storage Group "DP RSG" that links restored store to "Store Two" in storage group "Second Storage Group", and with the files restored in the "C:\Omni" directory, run:

```
omnir -vss -use_vds -barhost exch2007.company.com -session
2007/04/10-9 -tree "/Microsoft Exchange Writer(Exchange
Information Store)/Microsoft Information Store/First
Storage Group/Store One" -exch_RSG "/Microsoft Exchange
Writer(Exchange Information Store)/Microsoft Information
Store/Second Storage Group/Store Two/" -target_dir
"c:\mount" -tree "/Microsoft Exchange Writer(Exchange
Information Store)/Microsoft Information Store/First
Storage Group/Logs" -exch_RSG "/Microsoft Exchange
Writer(Exchange Information Store)/Microsoft Information
Store/Second Storage Group/Logs" -target_dir "C:\Omni"
```

SEE ALSO

omnib(1), omnikeymigrate(1M), omnikeytool(1M), omniobjconsolidate(1),
omniobjcopy(1), omniobjverify(1)

omnirpt

generates various reports about the Data Protector environment, for example, about backup, object copy, object consolidation, and object verification sessions in a specific time frame, session specifications, media, Data Protector configuration, and single sessions

(this command is available on systems with the Data Protector User Interface component installed)

omnirpt

SYNOPSIS

```
omnirpt -version | -help
```

```
omnirpt -report ReportName ReportOptions [MethodOptions] [FormatOptions] [-header] [-multicell] [-[no]_multiple]
```

```
omnirpt -rptgroup ReportGroup
```

FORMATOPTIONS

```
-ascii |
```

```
-html |
```

```
-tab |
```

```
-short
```

METHODOPTIONS

```
-email EmailAddress ... |
```

```
-smtp EmailAddress ... |
```

```
-snmp Hostname ... |
```

```
-broadcast Hostname ... |
```

```
-log Filename ... |
```

```
-external CommandName ...
```

REPORTNAME

```
list_sessions |
```

```
session_flow |
```

```
device_flow |
```

```
used_media |
```

```
used_media_extended |
```

```
host_statistics |
```

```
session_statistics |
```

```
session_errors |
```

```
dl_trees |
```

```
obj_nobackup |
```

obj_copies |
obj_lastbackup |
obj_avesize |
fs_not_conf |
dl_info |
dl_sched |
db_size |
db_purge |
db_purge_preview |
db_system |
cell_info |
hosts_unused |
dev_unused |
lookup_sch |
hosts_not_conf |
licensing |
host |
media_list |
media_list_extended |
media_statistics |
pool_list |
single_session |
session_objects |
session_hosts |
session_devices |
session_media |
session_objcopies

REPORTOPTIONS

SessionOption

-session *SessionID*

PoolOption

-pool *Poolname ...*

LabelOption

-label *Label*

LocationOption

-location *Location ...*

LibraryOption

```

-[no_]library Library ...
ProtectionOption
-[no_]protection NoOfDays
MediaClassOption
-class MediaClass
MediaStatusOption
-status MediaStatus
SpecificationOptions
-datalist BackupSpecificationName ...
-copylist_sch ScheduledCopySpecificationName ...
-copylist_post PostbackupCopySpecificationName ...
-verificationlist_sch ScheduledVerificationSpecificationName
...
-verificationlist_post PostbackupVerificationSpecificationName
...
-conslist_sch ScheduledConsolidationSpecificationName ...
-conslist_post PostbackupConsolidationSpecificationName ...
-no_datalist
-no_copylist
-no_verificationlist
-no_conslist
BackupSpecificationGroupOption
-group BackupSpecificationGroup
LookupSchedulesOption
-schedule NoOfdays
NetworkOption
-network Network_IP_Adress ...
HostsOption
-hosts Hostname ...
HostOption
-host Hostname
LevelOption

```

```

-level Level
ObjectCopiesOption
-num_copies {less | equal | more} NumberOfCopies
TimeframeOption
-timeframe {Start Duration | Day Hour Day Hour}
LatestObjectOption
-days NoOfdays
Level: {warning | minor | major | critical}
Day: [YY]YY/MM/DD
Hour:: HH:MM

```

DESCRIPTION

The `omnirpt` command generates various reports about Data Protector environment: reports about backup, object copy, object consolidation, and object verification sessions in a specific time frame, about backup, object copy, object consolidation, and object verification specifications, media, Data Protector configuration and single sessions. Each report is defined by its name `-report ReportName` and a set of options that specify report parameters (described below). The reports are provided in four different formats: ASCII, HTML, tabulator separated format and short ASCII format. Each report is described in two parts: input (what user has to/may specify to configure a report) and output (what is the content of the report). Input items that are enclosed in square brackets (`[]`) are optional, while all others are required. The following *report categories* are available:

Sessions in Timeframe

"Sessions in Timeframe" reports provide reports about backup, object copy, object consolidation, and object verification activities in a certain past time period. This time period can either be defined in relative terms (such as last 24 hours) or absolute (15/03/07 00:00 - 16/03/07 00:00). Two other common report options for all "Sessions in Timeframe" reports are backup specification and backup specification group. These two limit the report to selected backup specifications. "Session in Timeframe" reports are:

- List of Sessions (`list_sessions`)
- Session Flow Report (`session_flow`)
- Device Flow Report (`device_flow`)
- Report on Used Media (`used_media`)

- Extended Report on Used Media (`used_media_extended`)
- Client Statistics (`host_statistics`)
- Session Statistics (`session_statistics`)
- Session Errors (`session_errors`)
- Object Copies Report (`obj_copies`)

Session Specifications

"Session Specifications" reports provide different configuration reports which are based on backup, object copy, object consolidation, and object verification specifications. By default, all backup, object copy, object consolidation, and object verification specifications are used, but you may choose to limit a report to a certain session specification. Selection of a backup specification group is available only for backup specifications. "Session Specifications" reports are:

- Trees in Backup Specification (`dl_trees`)
- Objects Without Backup (`obj_nobackup`)
- Object's Latest Backup (`obj_lastbackup`)
- Average Backup Object Sizes (`obj_avesize`)
- Filesystems Not Configured for Backup (`fs_not_conf`)
- Session Specification Information (`dl_info`)
- Session Specification Schedule (`dl_sched`)

Internal Database

"Internal Database" reports provide information about Data Protector internal database (IDB) and about Data Protector client systems dynamics. "Internal Database" reports are:

- Internal Database Size Report (`db_size`)
- Internal Database Purge Report (`db_purge`)
- Internal Database Purge Preview Report (`db_purge_preview`)
- Report on System Dynamics (`db_system`)

Configuration

"Configuration" reports provide various reports about Data Protector environment. "Configuration" reports are:

- Cell Information (`cell_info`)
- Configured Clients not Used by Data Protector (`hosts_unused`)
- Configured Devices not Used by Data Protector (`dev_unused`)
- Look up Schedule (`lookup_sch`)

- Clients not Configured for Data Protector (`hosts_not_conf`)
- Licensing report (`licensing`)
- Client Backup Report (`host`)

Pools and Media

"Pools and Media" reports provide four reports that search through Data Protector pools for media that match the search criteria. The default is to list all media or pools and each report option can then limit the search to a certain set of media. "Pools and Media" reports are:

- List of Pools (`media_list`)
- Extended List of Media (`media_list_extended`)
- Media Statistics (`media_statistics`)
- List of Media (`pool_list`)

Single Session

"Single session" reports provide various information about single Data Protector backup, object copy, object consolidation, or object verification sessions. These reports are mostly used as End of Session notification. In this case, Data Protector will use the session ID of the current session (the one that generated the End of Session event) to create the appropriate report. "Single session" reports are:

- Single Session Report (`single_session`)
- Session Objects Report (`session_objects`)
- Session per Client Report (`session_hosts`)
- Session Devices Report (`session_devices`)
- Session Media Report (`session_media`)
- Session Object Copies Report (`session_objcopies`)

OPTIONS

`-version`

Displays the version of the `omnirpt` command.

`-help`

Displays the usage synopsis for the `omnirpt` command.

`-header`

This option is not used for the reports that have no required or optional report options. If this option is set, the output of the report will display report options too. If it is not set, only the output of the report is displayed.

`-multicell`

This option is only used with Manager-of-Managers. If this option is specified, the report will be generated for all Cell Managers configured in the MoM environment (multi-cell report).

`-[no_]multiple`

This option is only used for enterprise reports (multi-cell) and for Session per Client reports. If this option is specified, the report will be divided into sections. For enterprise reports the report will be divided by Cell Manager and for Session per Client reports it will be divided by client.

Report Names

`list_sessions`

Lists all sessions in the specified time frame. The report is defined by set of options that specify report parameters. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

`-timeframe {Start Duration | Day Hour Day Hour}`

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`[-copylist_sch ScheduledCopySpecificationName ...]`

`[-copylist_post PostbackupCopySpecificationName ...]`

`[-verificationlist_sch
ScheduledVerificationSpecificationName ...]`

`[-verificationlist_post
PostbackupVerificationSpecificationName ...]`

`[-conslist_sch ScheduledConsolidationSpecificationName ...]`

`[-conslist_post PostbackupConsolidationSpecificationName ...]`

Report filtering options are:

`[-no_datalist]`

`[-no_copylist]`

`[-no_verificationlist]`

`[-no_conslist]`

`session_flow`

Graphically presents duration of each session specified in certain time frame. Flow chart of the backup, object copy, object consolidation and object verification

sessions matching search criteria is shown. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}
[-datalist BackupSpecificationName ...]
[-group BackupSpecificationGroup]
[-copylist_sch ScheduledCopySpecificationName ...]
[-copylist_post PostbackupCopySpecificationName ...]
[-verificationlist_sch
ScheduledVerificationSpecificationName ...]
[-verificationlist_post
PostbackupVerificationSpecificationName ...]
[-conslist_sch ScheduledConsolidationSpecificationName ...]
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]
[-no_copylist ]
[-no_verificationlist ]
[-no_conslist ]
```

device_flow

Graphically presents usage of each device. Flow chart of the backup, object copy, and object consolidation sessions matching search criteria is shown. If you set the *RptShowPhysicalDeviceInDeviceFlowReport* global variable to 1, the same physical devices (presented by their lock names or serial numbers) are grouped together. If there is no lock name or serial number specified, the logical name is displayed. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}
[-datalist BackupSpecificationName ...]
[-group BackupSpecificationGroup]
[-copylist_sch ScheduledCopySpecificationName ...]
[-copylist_post PostbackupCopySpecificationName ...]
```



```
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]  
[-no_copylist ]  
[-no_conslist ]
```

`used_media`

Lists destination media that have been used by backup, object copy, and object consolidation sessions in the specific time frame together with their statistics. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-copylist_sch ScheduledCopySpecificationName ...]  
[-copylist_post PostbackupCopySpecificationName ...]  
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]  
[-no_copylist ]  
[-no_conslist ]
```

`used_media_extended`

Provides extended information on destination media that have been used by backup, object copy, and object consolidation sessions in the specific time frame, as well as the session type and subtype. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-copylist_sch ScheduledCopySpecificationName ...]
```

```
[-copylist_post PostbackupCopySpecificationName ...]  
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]  
[-no_copylist ]  
[-no_conslist ]
```

host_statistics

Lists of clients and their backup status - only clients that were used by the backup sessions matching the search criteria are displayed.

Additionally, clients can be limited also with hosts report option.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-hosts]
```

session_statistics

Shows statistics about backup, object copy and object consolidation status in the selected time frame, limited to sessions matching the search criteria. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-copylist_sch ScheduledCopySpecificationName ...]  
[-copylist_post PostbackupCopySpecificationName ...]  
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]  
[-no_copylist ]  
[-no_conslist ]
```

session_errors

Shows list of messages that occur during backup, object copy, and object consolidation sessions in the specified time frame for selected session specifications. The messages are grouped by clients (for all selected clients). By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-copylist_sch ScheduledCopySpecificationName ...]  
[-copylist_post PostbackupCopySpecificationName ...]  
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]  
[-hosts Hostname ...]  
[-level Level]
```

Report filtering options are:

```
[-no_datalist ]  
[-no_copylist ]  
[-no_conslist ]
```

obj_copies

Lists object versions that are created in the specified time frame with the number of their valid copies. The number of copies includes the original object version. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
-timeframe {Start Duration | Day Hour Day Hour}  
-num_copies {less | equal | more} NumberOfCopies  
[-datalist BackupSpecificationName ...]  
[-group BackupSpecificationGroup]  
[-copylist_sch ScheduledCopySpecificationName ...]  
[-copylist_post PostbackupCopySpecificationName ...]  
[-conslist_sch ScheduledConsolidationSpecificationName ...]  
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

`[-no_datalist]`

`[-no_copylist]`

`[-no_conslist]`

`dl_trees`

Lists all trees in the specified backup specification. It also shows names of drives and the name of a tree.

Report options are:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`obj_nobackup`

Lists all objects, specified for backup in selected backup specifications, which do not have a valid backup. A valid backup means that the backup completed successfully and its protection has not expired. For each object that does not have a valid protected full backup, the following items are shown: backup specification, an object type, an object name and a description. Only objects from the selected backup specification are used for the report. If HOST object is used: Host object is expanded (get disks) and report checks that expanded objects are in database. UNIX, NetWare, and Windows filesystems are supported. This option is not available for backup specifications for integrations.

Report options are:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`[-days NoOfDays]`

`obj_lastbackup`

Lists all objects in the IDB. For each object, it displays the last full and the last incremental backup time, the last full and the last incremental object copy time, and the last object consolidation time.

Objects of the Client System type (host backup) are expanded; it means that the information is listed for each volume separately. As for objects of the Filesystem type (filesystem objects), only the UNIX, NetWare, and Windows filesystems are supported.

You can narrow the scope of objects listed using the following report options:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`[-days NoOfDays]`

However, note the following:

- Filesystem objects that do not match the condition in the object creation time filter are listed anyway. However, in this case, the object creation time fields remain empty.

- If you clear certain filesystem objects from a backup specification, these filesystem objects will not be included in the report even if the objects exist in the IDB.

The above note is not applicable for objects of the Bar type (integration objects).

`obj_avesize`

Lists all objects, specified for backup in selected backup specifications, which have a valid backup. A valid backup means that the backup completed successfully and its protection has not expired. For each object average full and average incremental backup size is displayed. If HOST object is used: Host object is expanded (get disks) and report checks that expanded objects are in database. UNIX, NetWare, and Windows filesystems are supported.

Report options are:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`[-days NoOfDays]`

`fs_not_conf`

Displays a list of mounted filesystems which are not in selected backup specifications. Output is a list of filesystems. If HOST object is used, the report will not report any disk from client as not configured (assuming that HOST backup will backup all disks). If HOST object is used, the report will not report any disk from client as not configured (assuming that HOST backup will backup all disks).

Report options are:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`dl_info`

Shows information about all selected backup, object copy, object consolidation, and object verification specifications (type, session type, session specification name, group, owner, and pre & post exec commands). HOST does not influence report. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

`[-datalist BackupSpecificationName ...]`

`[-group BackupSpecificationGroup]`

`[-copylist_sch ScheduledCopySpecificationName ...]`

```

[-copylist_post PostbackupCopySpecificationName ...]
[-verificationlist_sch
ScheduledVerificationSpecificationName ...]
[-verificationlist_post
PostbackupVerificationSpecificationName ...]
[-conslist_sch ScheduledConsolidationSpecificationName ...]
[-conslist_post PostbackupConsolidationSpecificationName ...]

```

Report filtering options are:

```

[-no_datalist ]
[-no_copylist ]
[-no_verificationlist ]
[-no_conslist ]

```

dl_sched

Shows information about all selected backup, object copy, object consolidation, and object verification specifications and their next scheduled time up to one year in advance (type, session type, session specification name, group, next execution, and backup operation time). HOST does not influence report. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, object consolidation, or object verification specification.

Report options are:

```

[-datalist BackupSpecificationName ...]
[-group BackupSpecificationGroup]
[-copylist_sch ScheduledCopySpecificationName ...]
[-copylist_post PostbackupCopySpecificationName ...]
[-verificationlist_sch
ScheduledVerificationSpecificationName ...]
[-verificationlist_post
PostbackupVerificationSpecificationName ...]
[-conslist_sch ScheduledConsolidationSpecificationName ...]
[-conslist_post PostbackupConsolidationSpecificationName ...]

```

Report filtering options are:

```

[-no_datalist ]
[-no_copylist ]
[-no_verificationlist ]
[-no_conslist ]

```

`db_size`

Lists a table that contains information about the MMDB, CDB, IDB extension files, statistics for DCBF, SMBF and SIBF, and low IDB disk space. The `Used` columns in this report show the percentage of used records. This figure is calculated as current amount of used records divided by the amount of records allocated in the IDB in percents. Thus, this figure may substantially vary, since Data Protector automatically allocates new records whenever this figure reaches 100 percent (whenever all currently allocated records are used). To find out whether certain parts of the IDB are running out of space, you can additionally configure the IDB Space Low or IDB Tablespace Space Low notification, or check the last part of this report - it lists the low disk space information when allocated records for any of the involved disks are running out of space. There are no report options for this report.

`db_purge`

Lists all purged sessions (from `purge.log` file) with the following information: start time, end time, duration, inactivity time and number of file names, file versions and sessions purged. There are no report options for this report.

`db_purge_preview`

Lists the following information: overall number of filenames in database (in thousands), estimated number of obsolete filenames in database (in thousands) and estimated duration of database purge (in seconds). There are no report options for this report.

`db_system`

Lists the following information about each Data Protector client in the cell: the number of filenames (in thousands) in the Data Protector internal database (IDB), the number of active filenames (in thousands) in the IDB, the IDB filenames growing ratio (new filenames per day), the number of deleted filenames in the IDB per day, active growth per year, and dynamics indicator (medium/high/low/critical). The filenames that are not active are filenames of the backed up files in the IDB that have no associated file versions in the IDB. The active growth per year is calculated in two ways: If there is no IDB purge session recorded in the IDB, the active growth per year is calculated on the basis of data in last 11 days and then extrapolated to one year. If there is an IDB purge session recorded in the IDB, the active growth per year is calculated on the basis data in the time span since the last IDB purge session and then extrapolated to one year. There are no report options for this report.

`cell_info`

Data Protector cell related information (number of clients, Backup specifications, Media Management server, Licensing server).

`hosts_unused`

List of configured clients that are not used for backup and do not have any device configured.

`dev_unused`

List of configured destination devices that are not used for backup, object copy, or object consolidation at all.

`lookup_sch`

List of backup, object copy, and object consolidation specifications that are scheduled to start in the next *n* number of days up to one year in advance (where *n* is the number of days specified by user).

Report option is:

`[-schedule NoOfDays]`

`hosts_not_conf`

List of clients in selected domain(s) that are not configured for Data Protector. Note that Data Protector will display also routers and other machines that have IP address in selected domain.

Report option is:

`-network Network_IP_Address...`

`licensing`

List all licenses with their total and available amount.

`host`

Report output is all end-user backup related information about specific client: list of filesystems not configured for selected clients, list of all objects configured in backup specifications for the selected client, list of all objects with a valid backup for specified client with times and average sizes.

Report option is:

`-host HostName`

`media_list`

List of all media matching the search criteria. The following information is provided for each medium: ID, label, location, status, protection, used and total MB, the time when media was last used, the media pool, and media class.

Report options are:

`[-label Label]`

`[-location Location ...]`

`[-pool PoolName ...]`

`[-class MediaClass]`

`[-status MediaStatus]`


```
[-[no_]protection NoOfDays]
[-timeframe {Start Duration | Day Hour Day Hour}]
[-[no_]library Library ...]
```

media_list_extended

List of all media matching the search criteria. The following information is provided for each medium: ID, label, location, status, protection, used and total MB, the time when media was last used, the media pool and media type, session specifications that have used this medium for backup, object copy, or object consolidation, as well as the session type and subtype. By default, the report is generated for all session specifications. Use the report filtering options to generate a report only for a specific backup, object copy, or object consolidation specification.

Report options are:

```
[-label Label]
[-location Location ...]
[-pool Pool Name ...]
[-class MediaClass]
[-status MediaStatus]
[-[no_]protection NoOfDays]
[-timeframe {Start Duration | Day Hour Day Hour}]
[-[no_]library Library ...]
[-datalist BackupSpecificationName...]
[-group BackupSpecificationGroup]
[-copylist_sch ScheduledCopySpecificationName ...]
[-copylist_post PostbackupCopySpecificationName ...]
[-conslist_sch ScheduledConsolidationSpecificationName ...]
[-conslist_post PostbackupConsolidationSpecificationName ...]
```

Report filtering options are:

```
[-no_datalist ]
[-no_copylist ]
[-no_conslist ]
```

media_statistics

Reports the statistics on the media matching the search criteria. The following information is provided: number of media; number of scratch media; number of protected, good, fair and poor media; number of appendable media; and total, used, and free space on media.

Report options are:

```
[-label Label]  
[-location Location ...]  
[-pool PoolName ...]  
[-class MediaClass]  
[-status MediaStatus]  
[-[no_]protection NoOfDays]  
[-timeframe {Start Duration | Day Hour Day Hour}]  
[-[no_]library Library ...]
```

pool_list

Lists all pools matching a specified search criteria. For each pool the following information is provided: pool name, description, media type, total number of media, number of full and appendable media containing protected data, number of free media containing no protected data, number of poor, fair and good media.

Report options are:

```
[-pool PoolName ...]  
[-location Location ...]  
[-class MediaClass]  
[-[no_]library Library ...]  
[-timeframe {Start Duration | Day Hour Day Hour}]
```

single_session

Report displays all relevant information about single Data Protector backup, object copy, object consolidation, and object verification sessions.

Report option is:

```
-session SessionID  
[-level Level]
```

session_objects

Returns all information about all backup, object copy, or object consolidation objects that took part in a selected session.

Report option is:

```
-session SessionID
```

session_hosts

Provides information for each client that took part in the selected backup session: statistics about backup status for the client, list of objects and their related information for the client, error messages for the client.

All information is grouped for each client separately. Using the `-multiple` option, this report can be split into smaller reports, one for each client (see section Notifications for details).

Report option is:

`-session SessionID`

`[-level Level]`

`session_devices`

Provides information about all devices that took part in a selected session.

Report option is:

`-session SessionID`

`session_media`

Provides information about all destination media that took part in a selected session.

Report option is:

`-session SessionID`

`session_objcopies`

Lists object versions that are created in the selected backup, object copy, and object consolidation session with the number of their valid copies.

Report option is:

`-session SessionID`

Method options

`-email EmailAddress`

Sends the report to the specified *EmailAddress*.

On Windows, you need a configured MAPI profile. You can either use an existing mail profile or create a new one, named `Omniback`. To use an existing profile, edit the `omnirc` variable `OB2_MAPIPROFILE`.

On UNIX, `/usr/bin/mail` is used for sending the e-mails.

`-smtp EmailAddress`

The recommended option for sending reports by e-mail. Sends the report to the specified *EmailAddress* using the SMTP protocol.

By default, the SMTP server address is set to the Cell Manager address. To change the SMTP server, edit the variable `SMTPServer` in the global options file. The

server must be accessible from the Cell Manager system, but does not need to be part of the Data Protector cell.

`-snmp Hostname`

Report is send as an SNMP (Simple Network Mailing Protocol) trap.

`-broadcast Hostname`

Report is broadcasted to the selected machine. Note: Only Windows machines can be specified as broadcast destination.

`-log Filename`

Report is saved in to the log file specified with *Filename*.

`-external CommandName`

Specifies a script which receives the report. Optionally the script can than parse the report and forward it to user configured recipient. Usually, TAB report format is used in combination with `-external` option.

Report options

`-rptgroup ReportGroup`

This option executes the specified *ReportGroup*.

`-session SessionID`

This option is used to specify the Session ID report option.

`-pool Poolname ...`

This option is used to specify the media pool name report option.

`-label Label`

This option is used to specify the medium label report option.

`-location Location ...`

This option is used to specify the medium location report option.

`-[no_]library Library ...`

This option is used to specify the library report option. If it is set to `-no_library`, all libraries in the cell are selected for the report.

`-[no_]protection NoOfDays`

This option is used to specify the protection report option. The number of days in which the protection will expire can be specified. If it is set to `no_protection`, all media in the cell will be selected for the report.

`-class MediaClass`

This option is used to specify the media class report option.

`-status MediaStatus`

This option is used to specify the media status report option. It can have one of the following values: *poor*, *fair*, or *good*.

`-datalist BackupSpecificationName ...`

This option is used to specify the backup specifications for the report. Note that you can specify more than one backup specification. In such a case, separate the specification names with spaces.

`-copylist_sch ScheduledCopySpecificationName ...`

This option is used to specify the scheduled object copy specifications for the report. Note that you can specify more than one scheduled object copy specification. In such a case, separate the names with spaces.

`-copylist_post PostbackupCopySpecificationName ...`

This option is used to specify the post-backup object copy specification report option. Note that you can specify more than one post-backup object copy specification. In such a case, separate the specification names with spaces.

`-verificationlist_sch ScheduledVerificationSpecificationName ...`

This option is used to specify the scheduled object verification specifications for the report. Note that you can specify more than one scheduled object verification specification. In such a case, separate the names with spaces.

`-verificationlist_post PostbackupVerificationSpecificationName ...`

This option is used to specify the post-backup object verification specification report option. Note that you can specify more than one post-backup object verification specification. In such a case, separate the specification names with spaces.

`-constlist_sch ScheduledConsolidationSpecificationName ...`

This option is used to specify the scheduled object consolidation specifications for the report. Note that you can specify more than one scheduled object consolidation specification. In such a case, separate specification names with spaces.

`-constlist_post PostbackupConsolidationSpecificationName ...`

This option is used to specify the post-backup object consolidation specifications for the report. Note that you can specify more than one post-backup object consolidation specification. In such a case, separate the specification names with spaces.

`-group BackupSpecificationGroup`

This option is used to specify backup specification group for the report.

`-schedule NoOfDays`

This option is used to specify report option, which defines the number of days for which to display the schedule information.

`-network Network_IP_Address ...`

This option specifies one or more network IP addresses. Network IP address is represented by the first three numbers in the IP address, for example 123.44.5. You can specify more than one network IP address using spaces in between.

`-hosts Hostname ...`

Select the client systems for which you want to create the report.

`-host Hostname`

Select the client system for which you want to create the report.

`-level Level`

Select the level of warnings that should be included in the report. The levels are warning, minor, major, and critical.

`-num_copies {less | equal | more} NumberOfCopies`

This option is used to specify the number of valid object versions copies. Note that you can specify more than, equal to, or less than the selected number of copies.

`-timeframe Start Duration`

This option is used to specify a relative time frame report option. It is useful for recurrent reports, for example you can use `-timeframe 24 24` each day to set the time frame to last 24 hours.

`-timeframe Day Hour Day Hour`

This option is used to specify an absolute time frame report option.

`-days NoOfDays`

The report will filter objects that have been backed up recently. Specify the number of days.

Report filtering options

`-no_datalist`

This option is used to exclude all backup specifications from the report.

`-no_copylist`

This option is used to exclude all object copy specifications from the report.

`-no_verificationlist`

This option is used to exclude all object verification specifications from the report.

`-no_conslist`

This option is used to exclude all object consolidation specifications from the report.

Report Formats

<code>-ascii</code>	Specifies report format: ASCII
<code>-html</code>	Specifies report format: HTML
<code>-tab</code>	Specifies report format: TAB
<code>-short</code>	Specifies report format: SHORT

EXAMPLES

1. To list all backup sessions that have started in the last 24 hours and display the report in the default ASCII format, run:

```
omnirpt -report list_sessions -timeframe 24 24 -no_copylist  
-no_conslist -no_verificationlist
```
2. To list all objects from session "2009/03/16-1" in tabulator separated format, which is useful for additional parsing or can be used with other tools for analysis, run:

```
omnirpt -report session_objects -session 2009/03/16-1 -tab
```
3. To list all media of class DLT with location string "COMPANY", for which protection will expire in the next 5 days, run:

```
omnirpt -report media_list -protection 5 -class DLT  
-location COMPANY
```

This report can be used as a base for the vaulting process, as it can list you media that need to be taken to the vault.
4. To send "Internal Database Size Report" in HTML format to the user "name@domain.com" using the SMTP protocol, run:

```
omnirpt -report db_size -html -smtp name@domain.com
```
5. To execute the report group named "MyReportGroup", run:

```
omnirpt -rptgroup MyReportGroup
```
6. To graphically present the usage of devices that were used for backup and object consolidation (but not object copy) sessions in the last 48 hours in HTML format that will be sent as the file "session1.html" to the directory "C:\Temp", run:

```
omnirpt -report device_flow -timeframe 48 48 -no_copylist  
-html >C:\Temp\session1.html
```

7. To list all the media used only for object copy and object consolidation sessions, run:
`omnirpt -report media_list_extended -no_datalist`
8. To list all object versions created in the last 72 hours that have less than 5 valid copies, run:
`omnirpt -report obj_copies -timeframe 72 72 -num_copies less 5`
9. To list all destination media that were used only for scheduled object copy specification named "Alpha" in the last 2 days, run:
`omnirpt -report used_media -timeframe 48 48 -copylist_sch Alpha -no_datalist -no_conslist`
10. To show statistics about backup status (but not object copy, object consolidation, and object verification) in the last 24 hours, run:
`omnirpt -report session_statistics -timeframe 24 24 -no_copylist -no_conslist -no_verificationlist`
11. To graphically present duration of all object consolidation sessions in the last 24 hours in HTML format that will be sent as the file "session_flow1.html" to the directory "C:\Temp", run:
`omnirpt -report session_flow -timeframe 24 24 -no_datalist -no_copylist -no_verificationlist -html`
`>C:\Temp\session_flow1.html`

SEE ALSO

omnihealthcheck(1M), omnitrig(1M)

omnistat

displays the status of active Data Protector backup and restore sessions
(this command is available on systems with the Data Protector User Interface component installed)

omnistat

SYNOPSIS

```
omnistat -version | -help
omnistat -session SessionID [-status_only | -monitor | -detail]
omnistat [-user Username] [-mount] [-error] [-detail]
omnistat -previous [-user Username] [{-since Date | -until Date} |
-last Number] [-failed]

Date
[YY]YY/MM/DD
```

DESCRIPTION

The `omnistat` command displays information on active sessions. You can view all active sessions (default) or only details of a specific session. An active session is referenced by its *SessionID*.

OPTIONS

`-version`
Displays the version of the `omnistat` command.

`-help`
Displays the usage synopsis for the `omnistat` command.

`-session SessionID`
Displays detailed information on the single active session identified by this *SessionID*.

`-monitor`
`omnistat` connects to the specified active session and starts monitoring the progress of the session.

`-status_only`
Displays only the overall status of the active session.

`-detail`

- Displays detailed information about all current sessions.
- user *Username*
Displays information on active sessions belonging to the specified user.
- failed
Displays information on sessions containing data objects that failed due to errors.
- error
Displays information on active sessions with the status "In Progress (errors)"
- mount
Displays all active sessions with mount requests pending.
- previous
Lists all sessions from the Data Protector internal database (IDB).
- since *Date*
Lists all sessions since the specified *Date*.
- until *Date*
Lists all sessions until the specified *Date*.
- last *n*
Lists all sessions within the last *n* days.

EXAMPLES

The following examples illustrate how some options of the `omnistat` command work.

1. To view sessions that are currently active and have mount requests pending, run:
`omnistat -mount`
2. To see detailed information for the session with the SessionID "2008/04/24-32". The SessionID can be specified in two different ways:
`omnistat -detail -session 2008/04/24-32`
`omnistat -detail -sess 32`
3. To see an overview of the sessions that occurred in last 3 days and were run by user `root`, run:
`omnistat -previous -user root -last 3`
4. To see information regarding the sessions that occurred within the last 3 days and had objects that have failed, run:
`omnistat -previous -last 3 -failed`

5. To see only the status of session with this SessionID, run:
`omnistat -status_only -session 2`
6. To monitor the session with the SessionID "R-2008/05/13-8", run:
`omnistat -session R-8 -monitor`

SEE ALSO

`omniabort(1)`

omniupload

uploads information about a backup device from an ASCII file to the Data Protector internal database (IDB)

(this command is available on systems with the Data Protector User Interface component installed)

omniupload

SYNOPSIS

```
omniupload -version | -help
omniupload -create_device FileName
omniupload -modify_device BackupDevice [-file FileName]
omniupload -remove_device BackupDevice
omniupload -create_library FileName
omniupload -modify_library Library [-file FileName]
omniupload -remove_library Library
```

DESCRIPTION

Uploads a backup device file to the Data Protector internal database (IDB).

Information on Data Protector backup devices is stored in the IDB. To configure a backup device, information on this device must be downloaded into a file. This is done using the `omnidownload` command. The file is then modified and uploaded back to the IDB.

OPTIONS

`-version`

Displays the version of the `omniupload` command.

`-help`

Displays the usage synopsis for the `omniupload` command.

`-create_device FileName`

Specifies the ASCII file containing the information about the backup device. This option is used to create a new backup device. If `-` is specified as *FileName* then data is read from stdin.

`-modify_device BackupDevice`

Uses the information in the uploaded file to modify an existing backup device in the IDB. If no filename is specified using the `-file` option the command searches

the current directory for a file with the same name as the *BackupDevice*. Note that the media class may not be changed.

`-file FileName`

Specifies the ASCII file that will be parsed for information about the backup device (library). This option is used to modify an existing backup device (library). If `-` is specified as *FileName* then data is read from stdin.

`-remove_device BackupDevice`

Removes information about the *BackupDevice* from the IDB.

`-create_library FileName`

Specifies the ASCII file containing the information about the library. This option is used to create a new library. If `-` is specified as *FileName* then data is read from stdin.

`-modify_library Library`

Uses the information in the uploaded file to modify an existing library in the IDB. If no filename is specified using, the `-file` option the command searches the current directory for a file with the same name as the *Library*. Note that the media class may not be changed.

`-remove_library Library`

Removes information about the *Library* from the IDB.

EXAMPLES

The following examples illustrate how the `omniupload` command works.

1. To create a backup device using the information in the file `"/tmp/Device"`, run:
`omniupload -create_device /tmp/Device`
2. To modify Library "Exabyte1" using the information in the file `"/tmp/EXA"`, run:
`omniupload -modify_library Exabyte1 -file /tmp/EXA`
3. To remove backup device "Stacker", run:
`omniupload -remove_device Stacker`

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omnimcopy(1)`, `omniminit(1)`, `omnimlist(1)`, `omnimmm(1)`, `omnimnt(1)`, `omnimver(1)`, `sanconf(1M)`, `uma(1M)`

omniusers

adds or removes Data Protector users to or from an existing Data Protector user group, or lists the configured Data Protector users. It enables you to use all GUI functionality on a Cell Manager platform on which the GUI is not supported, using a GUI installed on another system.

(this command is available on systems with the Data Protector User Interface component installed)

omniusers

SYNOPSIS

```
omniusers -version | -help
omniusers -add -type {U | W} -usergroup DPUserGroup -name UserName
-group GroupOrDomainName -client ClientName [-desc Description]
omniusers -remove -name UserName -group GroupOrDomainName -client
ClientName
omniusers -list
```

DESCRIPTION

The command adds, removes or lists the configured Data Protector users on the Cell Manager where it is run. It does not create or remove user groups.

Use the command to create a remote Data Protector user on those Cell Manager platforms on which Data Protector GUI is *not* supported. You can then use the created user account to start the Data Protector GUI on another system with the Data Protector GUI installed, and connect to the Cell Manager.

OPTIONS

-version

Displays the version of the `omniusers` command.

-help

Displays the usage synopsis for the `omniusers` command.

-add

Adds a user to the specified Data Protector user group.

-remove

Removes a user from its Data Protector user group.

-name *UserName*

Specifies username of the user to be added/removed. By specifying asterisk (*) as the username, all users from the specified group (on UNIX systems) or domain (on Windows systems) will be granted/revoked access from the specified clients to the Cell Manager. * corresponds to <Any> in the Data Protector GUI. Note that in some shells, backslash and asterisk (*) must be used instead of *.

Note that UNIX usernames and usernames of the configured Data Protector users are case sensitive.

Note that usernames and domain names of Windows GUI clients that are used with an HP-UX Cell Manager must be in capital letters.

`-type {U|W}`

Specifies the user type: a UNIX user (U) or a Windows user (W).

`-group GroupOrDomainName`

A group (on UNIX systems) or a domain (on Windows systems) the specified user belongs to. By specifying asterisk (*) as the group or domain name, the specified user will be granted/revoked access from any group (on UNIX systems) or domain (on Windows systems) from the specified clients. * corresponds to <Any> in the Data Protector GUI. Note that in some shells, backslash and asterisk (*) must be used instead of *.

Note that domain names of Windows GUI clients that are used with an HP-UX Cell Manager must be in capital letters.

`-client ClientName`

Specifies the name of the client system from where the specified user will have access to the Cell Manager. By specifying asterisk (*) as the client name, the specified user will be granted/revoked access to the Cell Manager from any Data Protector client system. * corresponds to <Any> in the Data Protector GUI. Note that in some shells, backslash and asterisk (*) must be used instead of *.

If this option is used with the `-remove` option, *ClientName* must contain the fully qualified domain name (FQDN) of the client system.

`-usergroup DPUserGroup`

Specifies the Data Protector user group the user(s) will be added to.

`-desc Description`

Specifies the description for the added user(s).

`-list`

Lists users in all configured Data Protector user groups in the cell. For each configured Data Protector user the username, UNIX group or Windows domain, fully qualified domain name (FQDN) of the client system from which the user has

granted access, and the user description are displayed. Asterisk (*) corresponds to the <Any> string in the Data Protector GUI.

RETURN VALUES

The return values of the `omniusers` command are:

- | | |
|---|---|
| 0 | The command operation completed successfully. |
| 1 | A generic error occurred. |
| 2 | The operation for adding or removing a user failed. |
| 4 | Error parsing options. |

NOTE

The `omniusers` command is designed to be used in Data Protector cells where the Cell Manager is running on a platform on which the Data Protector GUI is not supported. For details on supported operating systems, see the *HP Data Protector product announcements, software notes, and references*.

EXAMPLES

The following examples illustrate how the `omniusers` command works.

1. To add the Windows user "win_user" from the domain "domain1" to the Data Protector "admin" user group and allow access only from the client system "client.company.com", run the following command:

```
omniusers -add -type W -name win_user -usergroup admin  
-group domain1 -client client.company.com
```
2. To add the UNIX user "root" from the "sys" group to the Data Protector "admin" user group and allow access only from the client system "client.company.com", run:

```
omniusers -add -type U -name root -usergroup admin -group  
sys -client client.company.com
```
3. To add the UNIX user "root" to the Data Protector "admin" user group and allow access from any UNIX group but only from the system "client.company.com", run:

```
omniusers -add -type U -name root -usergroup admin -group  
\* -client client.company.com
```

4. To display the Data Protector users in all configured Data Protector user groups, run:

```
omniusers -list
```

SEE ALSO

ob2install(1M), omnigui(5), omniintro(9), omnimigrate.pl(1M), omnisetup.sh(1M),
upgrade_cm_from_evaa(1M), winomnimigrate.pl(1M)

syb_tool

a utility used to get ISQL command needed to restore a Sybase database that was backed up by Data Protector
(this command is available on systems with the Data Protector Sybase Integration component installed)

syb_tool

SYNOPSIS

```
syb_tool dbname servername  
-date YYYY/MM/DD.hh:mm:ss  
[-new_db dbname]  
[-new_server servername]  
[-file filename]  
[-media]
```

DESCRIPTION

The `syb_tool` is used to get the data needed for restore of Sybase databases.

OPTIONS

dbname

The name of Sybase database.

servername

The name of Sybase database server on which the backup was performed.

`-date YYYY/MM/DD.hh:mm:ss`

The date until which your database will be restored. `syb_tool` will find the first backup done after this date.

`-new_db dbname`

The name of the database that you want to restore to.

`-new_server servername`

The name of the server that you want to restore to.

`-file filename`

The name of the file where the ISQL statement needed for restore of desired database will be written to. The ISQL command can be started with the option `-i`, followed by the name of the file.

See also the section "Notes".

-media

This option returns the list of all media needed for restore.

NOTES

If the names of backed up objects contain characters that cannot be displayed using the current language group (on Windows) or code page (on UNIX):

1. Set the encoding used on the terminal to UTF-8.
2. **Windows only:** Set the environment variable `OB2_CLI_UTF8` to 1.
3. Redirect the output of the `syb_tool` command to a text file using the `-i` option.
If you need to edit the file containing the load command, use a UTF-8 aware editor that does not set the first byte ("BOM"), since such a file is not supported by `isql`. Note that the Windows Notepad editor cannot be used.
4. When restoring the objects, add the `-i file_name -J utf8` options to the `isql` command, where `file_name` is the file with the load command.

For details, see *HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*.

EXAMPLES

1. To get the ISQL statement needed for the restore of the last backup of the database named "database1" on the Sybase Adaptive Server named "server", run:

```
syb_tool database1 server -date
```
2. To get the ISQL statement needed for the restore of the database named "database1" on the Sybase Adaptive Server named "server", using the first backup performed after midday of July 07. 2007, run:

```
syb_tool database1 server -date 2007/07/07.12:00:00
```
3. To get the ISQL statement needed for the restore of the database named "database1" on the Sybase Adaptive Server named "server", using the first backup performed after midday of July 07. 2007 and restoring it as "database_one" on the Sybase server called "server_one", run:

```
syb_tool database1 server -date 2007/07/07.12:00:00 -new_db  
database_one -new_server server_one
```
4. To get the ISQL statement needed for the restore of the last backup performed for database named "database1" on the Sybase Adaptive Server named

"server", saving the ISQL statement to file "/tmp/stat.isql", and getting the list of media IDs needed for restore, run:

```
syb_tool database1 server -date -file /tmp/stat.isql -media
```

To start the restore, start the ISQL command, specifying the input file "/tmp/stat.isql" in the following way:

```
isql -Usa -P -Sserver -i /tmp/stat.isql
```

Section 1M: Administrative Commands

cjutil

starts, stops, and queries the Change Journal
(this command is available on systems with the Data Protector Disk Agent
component installed)

cjutil

SYNOPSIS

```
cjutil -volume vol {-start [-maxsize max -delta del] | -stop [-wait]  
| -query}
```

DESCRIPTION

The `cjutil` command is used to control and administer the Change Journal. It is located in the `Data_Protector_home\bin` directory on a Windows client.

OPTIONS

`-volume vol`

Defines the volume name in the form `/C` or `/C:\mounted_folder`.

`-start [-maxsize max -delta del]`

Starts the Change Journal on the specified volume.

The `-maxsize max` option sets the maximum size of the Change Journal in bytes. The highest possible value is 4 GB (4294967296 bytes). Any specified value greater than 4 GB will be rounded down to 4 GB. Note that a reasonable size for a 100 GB drive is an 85 MB Change Journal.

The `-delta del` option specifies the size in bytes to be purged from the Change Journal when it reaches its maximum size. We recommend the value be approximately one-eighth to one-quarter the value of the maximum size but not greater than one quarter the size of the maximum size. This value may be automatically adjusted to better correspond to the volume cluster size.

`-stop [-wait]`

Stops the Change Journal asynchronously.

The `-wait` specifies that the Change Journal will be stopped synchronously. The call returns only after the Change Journal has been deleted.

`-query`

Queries the status of the Change Journal.

NOTES

If the `-start` option is specified and the Change Journal is already active, the Change Journal is adjusted to the value of the maximum size and delta. Note that these values can only be adjusted to increase.

When starting the Change Journal, if you not specify `-maxsize` and `-delta`, or specify 0 for these parameters, the system chooses a default value based on the volume size.

As an alternative to the Data Protector `cjutil` command, you can also use the Windows `fsutil` command for administering the Change Journal.

EXAMPLES

To start the Change Journal with the maximum size of 8 MB (in bytes) and specify the size of 1 MB (in bytes) to be purged from the Change Journal when it reaches the specified maximum size, run:

```
cjutil -start -maxsize 8388608 -delta 1048576
```

SEE ALSO

`omnicjutil(1M)`

NNMpost.ovpl

a script with no arguments that resumes the eight processes paused by NNMpre.ovpl (this command is available on systems with the Data Protector HP Network Node Manager Integration component installed)

NNMpost.ovpl

SYNOPSIS

NNMpost.ovpl

DESCRIPTION

A script with no arguments that resumes the eight processes paused by NNMpre.ovpl.

SEE ALSO

NNMpre.ovpl(1M), NNMScript.exe(1M)

NNMpre.ovpl

starts NNM embedded database backup
(this command is available on systems with the Data Protector HP Network Node
Manager Integration component installed)

NNMpre.ovpl

SYNOPSIS

NNMpre.ovpl

DESCRIPTION

The NNMpre.ovpl script starts the NNM embedded database backup. The embedded database makes a direct copy of itself to a location specified in the solid.ini file. The script also pauses eight NNM processes.

SEE ALSO

NNMpost.ovpl(1M), NNMScript.exe(1M)

NNMScript.exe

finds the location of the NNM Perl compiler and the NNMpre.ovpl and NNMpost.ovpl scripts and starts the two scripts
(this command is available on systems with the Data Protector HP Network Node Manager Integration component installed)

NNMScript.exe

SYNOPSIS

```
NNMScript.exe -pre | -post
```

DESCRIPTION

The NNMScript.exe finds the location of the NNM Perl compiler and the NNMpre.ovpl and NNMpost.ovpl scripts (because the NNM Perl compiler is used to run the scripts and its path must be supplied to Windows on the command line). The directory location is found via the registry and the location of the compiler and scripts are relative to this location. NNMScript.exe also starts the scripts. An argument specifies the script to run.

OPTIONS

-version

Displays the version of the NNMScript.exe command.

-help

Displays the usage synopsis for the NNMScript.exe command.

-pre

Starts the NNMpre.ovpl script.

-post

Starts the NNMpost.ovpl script.

NOTES

The NNMScript.exe command is available on Windows systems only.

SEE ALSO

NNMpost.ovpl(1M), NNMpre.ovpl(1M)

ob2install

runs remote client installation, uninstallation, upgrade, or check of a client from the selected Installation Server

(this command is available on the Data Protector Installation Server)

ob2install

SYNOPSIS

ob2install -version | -help

ob2install -server *installation_server* -input *filename*

DESCRIPTION

The `ob2install` command is used for running remote client installation from the Cell Manager. You have to select an Installation Server from which you want to run remote client installation.

OPTIONS

-version

Displays the version of the `ob2install` command.

-help

Displays the usage synopsis for the `ob2install` command.

-server *installation_server*

Specifies the Installation Server used for the installation session. The Installation Server must belong to local cell.

-input *filename*

Specifies the input file (a text file) containing the data for the client installation. Each client is described in the input file with a newline-separated ASCII string, using the format described below.

INPUT FILE FORMAT SYNOPSIS

-host *Hostname* -component *version* -push_inst
Push_Installation_Parameters

INPUT FILE OPTIONS

-host *Hostname*

Specifies the system on which the remote installation will be performed. The *Hostname* must be enclosed in double quotes.

-component version

Selects the components for the installation. The *version* argument specifies the version of the product. For the A.06.11 release, for example: `-smisa A.06.11`. Select only the components that are supported on target Data Protector system. The available components are:

`cc` installs the User Interface software component

`javagui` installs the Java GUI Client software component

`da` installs the Disk Agent software component

`ndmp` installs the NDMP Media Agent software component

`ma` installs the General Media Agent software component

`sap` installs the SAP R/3 Integration software component

`sapdb` installs the SAP DB Integration software component

`emc` installs the EMC Symmetrix Agent software component

`oracle` installs the Oracle Integration software component

`sybase` installs the Sybase Integration software component

`ssea` installs the HP StorageWorks XP Agent software component

`snapa` installs the HP StorageWorks VA Agent software component

`informix` installs the Informix Integration software component

`ov` installs the HP Network Node Manager Integration software component

`lotus` installs the Lotus Integration software component

`db2` installs the DB2 Integration software component

`smisa` installs the HP StorageWorks EVA SMI-S Agent software component

`vls_am` installs the VLS Automigration software component

`vmware` installs the VMware Integration software component

`docs` installs the English Documentation & Help software component

`jpn_ls` installs the Japanese Documentation & Help software component

`fra_ls` installs the French Documentation & Help software component

-push_inst Push_Installation_Parameters

This option specifies all parameters that are crucial for a successful remote client installation. The option must be used with all its parameters. All parameters except *GeneralInstallationType* and *InstallationType* must be specified in double quotation marks.

Push_Installation_Parameters

InstallPath

Specifies the path for installation — the Data Protector home directory. The parameter must be enclosed in double quotes. For UNIX remote client installation this path is ignored and a placeholder ("–") can be used.

UserName

Specifies the user name that is used during the remote client installation. If not specified, the default value "root" is used. The user name must be enclosed in double quotes. If you perform remote installation using secure shell, use a placeholder ("–").

Password

Specifies the password that is used while the Installation Server connects to the client. If you do not provide a password (in such a case, you must use "–"), you will have to provide it later during installation. The password must be enclosed in double quotes. If you perform remote installation using secure shell, leave this parameter empty.

CellManagerName

Specifies the name of the client's Cell Manager. It must be enclosed in double quotes.

GeneralInstallationType

General installation type can have two values: 1 or 2. 2 specifies a client installation. 1 is reserved for future extensions. For Data Protector A.06.11 release only the client installation is supported.

InstallationType

Specifies installation type:

- 1 new installation
- 2 update
- 3 delete
- 4 check installation

NOTES

The `ob2install` command is available on UNIX systems only.

EXAMPLES

The following example illustrates how the `ob2install` command works.

To start a remote client installation from the Installation Server "computer1.company.com" to the client "computer2.company.com" belonging to the Cell Manager "computer3.company.com", where the input file is named "infile.txt" and the selected components are Disk Agent, General Media Agent and Cell Console, run the following command on the Cell Manager:

```
ob2install -server computer1.company.com -input infile.txt
```

The input file "infile.txt" must contain the following line:

```
-host "computer2.company.com" -cc A.06.11 -da A.06.11 -ma  
A.06.11 -push_inst "-" "-" "-" "computer3.company.com" 2 1
```

The installation path, user name, and password are not specified.

SEE ALSO

omnigui(5), omniintro(9), omnimigrate.pl(1M), omnisetup.sh(1M), omniusers(1), upgrade_cm_from_evaa(1M), winomnimigrate.pl(1M)

omnicheck

performs a DNS connections check within a Data Protector cell and lists Data Protector patches installed on Data Protector clients
(this command is available on systems with any Data Protector component installed)

omnicheck

SYNOPSIS

```
omnicheck -version | -help  
omnicheck -dns [-host Client | -full] [-verbose]  
omnicheck -patches -host Client
```

DESCRIPTION

The following tasks can be performed using the `omnicheck` command:

CHECKING DNS CONNECTIONS WITHIN A DATA PROTECTOR CELL

To check DNS connections within a Data Protector cell, use the `-dns` option with the `omnicheck` command.

The `omnicheck` command does not verify DNS connections in general. It verifies that DNS information matches over all communications relevant for Data Protector among Data Protector cell members. The command reports only failed checks and the total number of failed checks unless the `-verbose` option is specified.

It is possible to verify the following DNS connections in the Data Protector cell, using the `omnicheck` command:

- To check that the Cell Manager and every Media Agent resolve DNS connections to every Data Protector client in the same cell properly and vice versa, use the `-dns` option.
- To check that a particular Data Protector client resolves DNS connections to every Data Protector client in the same cell properly and vice versa, use the `-host` option.
- To check all possible DNS connections in the cell, when every client resolves DNS connections to all other clients in the same cell, use the `-full` option.

LISTING PATCHES INSTALLED ON DATA PROTECTOR CLIENTS

The `omnicheck` command can be used to list Data Protector patches installed on a particular client. The `omnicheck` option used to list Data Protector patches installed on a particular client is `-patches`.

OPTIONS

`-version`

Displays the version of the `omnicheck` command

`-help`

Displays the usage synopsis for the `omnicheck` command.

`-dns`

Checks that the Cell Manager and every Media Agent resolve DNS connections to every Data Protector client in the same cell properly and vice versa. This option performs the same as running the `omnicheck -dns -host cell_manager` and `omnicheck -dns -host media_agent_1 ... omnicheck -dns -host media_agent_n` commands.

`-dns -host Client`

Checks that a Data Protector client specified by the `-host` option resolves DNS connections to every Data Protector client in the same cell properly and vice versa.

`-dns -full`

Checks all possible DNS connections in the cell. Every client in the cell tries to resolve all other clients in the same cell.

`-verbose`

Returns all the messages when using the `-dns` option. If this option is not set (default), only the messages that are the result of failed checks are returned.

`-patches -host Client`

Returns Data Protector patches (patch level, patch description and number of all patches installed) installed on a Data Protector client specified by the `-host` option. To use this option, you need the `Client` configuration user right (by default only users in the `admin` user group).

RETURN VALUES

See the man page `omniintro` for return values.

Additional return values of the `omnicheck` command used to check the DNS connections are:

`client_1 cannot connect to client_2`

`client_1 connects to client_2, but connected system presents itself as client_3`

```
client_1 failed to connect to client_2
checking connection between client_1 and client_2
all checks completed successfully.
number_of_failed_checks checks failed.
client is not a member of the cell.
client contacted, but is apparently an older version. Hostname
is not checked.
```

Additional return values of the `omnicheck` command used to list the Data Protector patches are:

```
List of patches found on host client
Patch level Patch description
Number of patches found: number_of_patches
List of patches on host client is not available.
Host client is not a member of this cell.
Host client is unreachable.
```

NOTES

The `omnicheck` command can be used only within one Data Protector cell.

EXAMPLES

1. To check DNS connections needed for normal Data Protector operating (the Cell Manager and every Media Agent in the cell resolves DNS connections to every Data Protector client in the cell properly and vice versa), run:
`omnicheck -dns`
2. To check if the client with the hostname `backup.system.com` resolves DNS connections to every Data Protector client in the same cell properly and vice versa and to get all relevant messages, run:
`omnicheck -dns -host backup.system.com -verbose`
3. To list the patches installed on client with the hostname `backup.system.com`, run:
`omnicheck -patches -host backup.system.com`

SEE ALSO

`omnicc(1)`, `omnicellinfo(1)`, `omnidlc(1M)`, `omniinstlic(1M)`, `omnisv(1M)`

omnicjutil

starts, stops, and queries the Change Journal on Windows clients
(this command is available on the Data Protector Cell Manager)

omnicjutil

SYNOPSIS

```
omnicjutil -help
omnicjutil -version
omnicjutil -file filename
omnicjutil -host hostname -volume vol {-start [-maxsize max -delta del] | -stop [-wait] | -query}
```

DESCRIPTION

The `omnicjutil` command is used to remotely control and administer the Change Journal on Windows clients. It is located in the `Data_Protector_home\bin` directory on Windows Cell Managers or in the `/opt/omni/sbin` directory on UNIX Cell Managers.

OPTIONS

`-help`

Displays the usage synopsis of the `omnicjutil` command.

`-version`

Displays the version for the `omnicjutil` command

`-file filename`

Defines the file containing multiple single line entries of this command. Each line must conform to the usage of the `omnicjutil` command. Note that no tabs are allowed. If a syntax error is found, none of the commands is executed.

`-host hostname`

Defines the name of the system hosting the Change Journal.

`-volume vol`

Defines the volume name in the form `/C` or `/C:\mounted_folder`.

`-start [-maxsize max -delta del]`

Starts the Change Journal on the specified volume.

The `-maxsize max` option sets the maximum size of the Change Journal in bytes. The highest possible value is 4 GB (4294967296 bytes). Any specified value greater than 4 GB will be rounded down to 4 GB. Note that a reasonable size for a 100 GB drive is an 85 MB Change Journal.

The `-delta del` option specifies the size in bytes to be purged from the Change Journal when it reaches its maximum size. We recommend the value be approximately one-eighth to one-quarter the value of the maximum size but not greater than one quarter the size of the maximum size. This value may be automatically adjusted to better correspond to the volume cluster size.

`-stop`

Stops the Change Journal asynchronously.

The `-wait` specifies that the Change Journal will be stopped synchronously. The call returns only after the Change Journal has been deleted.

`-query`

Queries the status of the Change Journal.

NOTES

If the `-start` option is specified and the Change Journal is already active, the Change Journal is adjusted to the value of the maximum size and delta. Note that these values can only be adjusted to increase.

When starting the Change Journal, if you not specify `-maxsize` and `-delta`, or specify 0 for these parameters, the system chooses a default value based on the volume size.

The command line tool gets the input either directly from the command line or from a file. Using input directly from the command line allows only one operation at a time. To perform more than one operation, create a file using the `-file filename` option and use it as an input. Note that the commands in the file are executed from top to bottom.

As an alternative to the Data Protector `omnicjutil` command, you can also use the Windows `fsutil` command for administering the Change Journal.

EXAMPLES

To start the Change Journal with the maximum size of 8 MB (in bytes) and specify the size of 1 MB (in bytes) to be purged from the Change Journal when it reaches the specified maximum size, run:

```
cjutil -start -maxsize 8388608 -delta 1048576
```

SEE ALSO

`cjutil(1M)`

omnidbcheck

checks the consistency of the Data Protector internal database (IDB)
(this command is available on the Data Protector Cell Manager)

omnidbcheck

SYNOPSIS

```
omnidbcheck -version | -help
omnidbcheck [-quick | -extended]
omnidbcheck -core [-summary]
omnidbcheck -filenames [-summary]
omnidbcheck -bf [-summary]
omnidbcheck -sibf [-detail | dumpmedia] [-summary]
omnidbcheck -smbf [-detail | dumpmessages] [-summary]
omnidbcheck -keystore [-summary]
omnidbcheck -dc [LimitScope] [-detail | -dumpmedia] [-summary]

LimitScope

-hosts host1 [host2 ...] | -media medium1 [medium2...] | -mpos min-max
```

DESCRIPTION

The Data Protector internal database (IDB) consists of: 1) Media Management Database (MMDB), 2) Catalog Database (CDB), 3) Detail Catalog Binary Files (DCBF), 4) Session Messages Binary Files (SMBF), and 5) Serverless Integrations Binary Files (SIBF). The MMDB and CDB objects, object versions and media positions form the core part of the IDB. The CDB filenames, DCBF, SMBF and SIBF form the detail part of the IDB.

The `omnidbcheck` command checks the status of the IDB or only of parts of IDB. The command sends a report to the standard output.

Note that errors found during the core check and encryption keystore check are `Critical`, errors found during the filenames check are `Major`, errors found during the dc and bf checks are `Minor`, errors found during the SIMBF check are `Minor`, and errors found during the SMBF check are `Warning`.

Data Protector creates a log file for each part of the check on the Cell Manager in the directory `Data_Protector_program_data\log\server` (Windows Server 2008), `Data_Protector_home\log\server` (other Windows systems), or `/var/opt/omni/server/log` (UNIX systems):

`Check_bf.txt`

Check_core.txt
Check_filenames.txt
Check_dc.txt
Check_smbf.txt
Check_sibf.txt

There is a timestamp at the beginning of each log file stating when the check was performed.

OPTIONS

`-version`

Displays the version of the `omnidbcheck` command.

`-help`

Displays the usage synopsis for the `omnidbcheck` command.

`-quick`

Checks the core, CDB filenames, presence and size of DCBF parts of the IDB, and displays the summary of the check by executing the `omnidbcheck -core -filenames -bf -summary` command.

`-extended`

Checks the entire IDB with the exception of the SMBF and displays the summary of the check by executing the `omnidbcheck -core -filenames -bf -dc -sibf` command. Full check of the consistency of the database, including detail file information is performed.

`-core`

Performs a core check of the IDB - it checks MMDB and CDB objects, object versions and media positions.

`-filenames`

Performs a check of the CDB filenames. It takes approximately one hour for each GB of the filename tablespace.

`-bf`

Performs a presence and size check of the DCBF. This check takes approximately 10 - 30 seconds.

`-sibf`

Checks if the SIBF are present and if they can be read. This check takes approximately 10 minutes for each GB of the SIBF part.

`-smbf`

Checks the presence of the SMBF. This check takes approximately 5 - 10 minutes. Note that if you have removed a SMBF in any way (e.g. using Data Protector GUI or CLI or deleted the file manually), then this option will report the removed session message as missing. This does not mean that IDB is corrupted - it only indicates that a session has been removed.

`-keystore`

Performs a consistency check of the Data Protector's `keymap` index file and the encryption keys in the keystore. The following information is listed for each encryption key in the cell: key ID, store ID, KeyStore name, KeyFile name
Data_Protector_program_data\db40\keystore\KeyStoreName\KeyFileName
(Windows Server 2008),
Data_Protector_home\db40\keystore\KeyStoreName\KeyFileName
(other Windows systems), or
/var/opt/omni/server/db40/keystore/KeyStoreName/KeyFileName
(UNIX systems), and a result of the check (OK or corrupted).

If the `-summary` option is specified, the command sums up the data and displays the status of the keystore.

`-dc`

Checks a consistency between the Core part and DC part of the IDB. This check takes approximately 10 minutes for each GB of the DC part of the IDB.

`-detail`

Lists all SIBF, SMBF or DCBF and their status (OK or corrupted/missing). If the `-detail` option is not specified (default) for the `-dc` option, all DCBF are listed, but status (corrupted) is displayed only with the corrupted DCBF. If the `-detail` option is not specified (default) for the `-smbf` or `-sibf` option, only the corrupted (SIBF) or missing (SMBF) binary files and their status (corrupted or missing) are listed.

`-dumpmedia`

If this option is specified with the `-sibf` option, it sends the SIBF filenames, object versions information, offset of the data in the SIBF file belonging to an object version and size of the data in the SIBF file belonging to an object version to the standard output. If this option is specified with the `-dc` option, it sends the complete information stored in the DCBF to the standard output.

`-dumpmessages`

This option is used with the `-smbf` option. It sends the session messages in the SMBF to the standard output.

`-summary`

Displays only the summary of the check (OK or failed/missing). The option does not impact the thoroughness of the check.

LimitScope

It is also possible to limit the scope of the DC check to either a set of media or a set of clients.

`-hosts host1 [host2...]`

Only Detail Catalogs for the specified clients are checked.

`-media medium1 [medium2...]`

`-mpos min-max`

Only those media positions (mpos) are checked that are located in DCBF directories with the specified media position (between *min* and *max*).

EXAMPLES

1. To check the DC part of the IDB for the Data Protector client named "machine.company.com", run:
`omnidbcheck -dc -hosts machine.company.com`
2. To perform an extended check of the IDB, run:
`omnidbcheck -extended`
3. To perform a consistency check of the Data Protector's keymap index file and the encryption keys in the keystore, run:
`omnidbcheck -keystore`

SEE ALSO

omnidb(1), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1), omnidbupgrade(1M), omnidbutil(1M), omnidbva(1), omnidbvss(1), omnidbxp(1)

omnidbinit

initializes the Data Protector internal database (IDB)
(this command is available on the Data Protector Cell Manager)

omnidbinit

SYNOPSIS

```
omnidbinit -version | -help  
omnidbinit [-force]
```

DESCRIPTION

The `omnidbinit` command initializes the Data Protector internal database (IDB). All information about sessions, media and objects is lost after the initialization. The command does not delete IDB transaction logs. The command creates a gap in the sequence of IDB transaction logs; when a roll forward operation is performed using the `omnidbrestore` command, the operation applies only the transaction logs created before the initialization of the IDB.

The IDB directory structure has to exist in order to initialize the IDB successfully. You can re-create the IDB directory structure by copying it from the directory *Data_Protector_program_data\NewConfig* (Windows Server 2008), *Data_Protector_home\NewConfig* (other Windows systems), or */opt/omni/newconfig/* (HP-UX or Solaris system) on the Cell Manager.

OPTIONS

`-version`

Displays the version of the `omnidbinit` command

`-help`

Displays the usage synopsis for the `omnidbinit` command

`-force`

Overrides the default safety check for the initialization. By default, the command displays a confirmation request. With this option, there is no confirmation request.

SEE ALSO

`omnidb(1)`, `omnidbcheck(1M)`, `omnidbrestore(1M)`, `omnidbsmis(1)`,
`omnidbupgrade(1M)`, `omnidbutil(1M)`, `omnidbva(1)`, `omnidbvss(1)`, `omnidbexp(1)`

omnidbrestore

performs the restores of the Data Protector internal database (IDB)
(this command is available on the Data Protector Cell Manager)

omnidbrestore

SYNOPSIS

```
omnidbrestore -version | -help
omnidbrestore -autorecover [AutorecoverOptions] [General Options]
omnidbrestore -read OptionFile [GeneralOptions]
omnidbrestore RMA_Options VRDA_Options MediaOptions [GeneralOptions]

RMA_Options (Restore Media Agent options)

-mahost DeviceHostname
-policy LogicalDevicePolicy
-type LogicalDeviceType
-dev PhysicalDevice
[-name DeviceName]
[-description DeviceDescription]
[-blksize BlkSize]
[-ioctl RoboticsDevice]
[-remhost RoboticsHostname]

VRDA_Options (Volume Restore Disk Agent options)

-daid DAID
[-overwrite | -no_overwrite]

Media Options

-maid mediumID1 [mediumID2...]
-slot slot1[:flip1] [slot2[:flip2]...]
-position segment1:offset1 [segment2:offset2...]

General Options

-verbose
-tree path1 [path2 ...]
-preview
-skiprestore
-keyfile Path

Autorecover Options
```

```
-session sessionID
-save OptionFile
-logview
-optview
-replay_only
-firstlog FirstTransactionLog
```

DESCRIPTION

The `omnidbrestore` command is used to restore the Data Protector internal database (IDB) without using the IDB, as opposed to the `omnir -omnidb` command which uses the IDB to retrieve the information needed for the IDB restore. If the IDB was installed on symbolic links, these symbolic links have to be created as they existed before running the `omnidbrestore` command.

The IDB restore using the `omnidbrestore` command consists of four phases: 1) Stopping the Data Protector services/daemons (with the exception of the Data Protector Inet service on Windows) 2) Restore of the IDB files. 3) Roll forward of IDB transactions (if present) stored in the IDB transaction log(s) - a process called `dbreplay`. Before the `dbreplay` is started, you are given the possibility to skip this phase by responding to a prompt. 4) Starting the Data Protector services/daemons.

Every time the backup of the IDB is started or when running `omnidbinit` or `omnidbcheck` commands or when the size of a transaction log reaches 2MB, a transaction log is created on the Cell Manager in the directory `Data_Protector_program_data\db40\logfiles\syslog\` (Windows Server 2008), `Data_Protector_home\db40\logfiles\syslog\` (other Windows systems), or `/var/opt/omni/server/db40/logfiles/syslog/` (UNIX systems). Depending on the value of the *Archiving* parameter in the `rdmserver.ini` file, located on the Cell Manager in `Data_Protector_program_data\db40\datafiles\catalog` (Windows Server 2008), `Data_Protector_home\db40\datafiles\catalog` (other Windows systems), or `/var/opt/omni/server/db40/datafiles/catalog` (UNIX systems), the old transaction log is copied (the *Archiving* parameter is set to 1) or deleted (the *Archiving* parameter is set to 0). In the latter case the `dbreplay` process is not always possible.

The `omnidbrestore` command can operate in three modes:

THE AUTORECOVER MODE

The autorecover mode is invoked using the `-autorecover` option. The `omnidbrestore` command in the autorecover mode scans the `obrindex.dat` file for the *Media Options*, *RMA Options* (Restore Media Agent options) and *VRDA*

options (Volume Restore Disk Agent options) and arguments needed for the restore. When the options and arguments are retrieved, the restore of the IDB is performed using the retrieved options and arguments to the original location overwriting the current files.

The `obrindex.dat` file resides on the Cell Manager in the directory `Data_Protector_program_data\db40\logfiles\rlog` (Windows Server 2008), `Data_Protector_home\db40\logfiles\rlog` (other Windows systems), or `/var/opt/omni/server/db40/logfiles/rlog` (UNIX systems). The `obrindex.dat` file is written to at every backup of the IDB and contains the *Media Options*, *RMA Options* and *VRDA options* and arguments needed for the restore of the IDB and the name of the transaction log created at the IDB backup time. You can create a copy of the `obrindex.dat` file by setting the `RecoveryIndexDir` parameter in the Data Protector global options file to point to a directory where you want to have a copy of the `obrindex.dat` file. If the `obrindex.dat` file is missing or is corrupted, the `omnidbrestore` command will use its copy if the `RecoveryIndexDir` parameter points to the directory with the copy. The Data Protector global options file (`global`) resides on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\Options` (Windows Server 2008), `Data_Protector_home\Config\Server\Options` (other Windows systems), or `/etc/opt/omni/server/options` (UNIX systems).

THE READ MODE

The read mode is invoked using the `-read` option. `omnidbrestore` reads the options and arguments from the file that has been created manually or using the `-autorecover -save OptionFile` option. This is useful in case the restore devices are different from the backup devices (or attached to a different system). In such a case the *OptionFile* has to be manually updated with the appropriate restore device data before the restore is started.

THE MANUAL MODE

The manual mode is used if the `obrindex.dat` file is not available and you have to specify all the needed *Media Options*, *RMA Options* and *VRDA options* and arguments manually.

OPTIONS

`-version`

Displays the version of the `omnidbrestore` command.

`-help`

Displays the usage synopsis for the `omnidbrestore` command.

`-autorecover` [*Autorecover Options*] [*General Options*]
 Starts the restore of the IDB in the autorecover mode. The `omnidbrestore` command in the autorecover mode scans the `obrindex.dat` file for the *Media Options*, *RMA Options* and *VRDA options* and arguments needed for the restore. When the options and arguments are retrieved, the restore of the IDB is performed using the retrieved options and arguments to the original location overwriting the current files.

`-read` *OptionFile* [*General Options*]
 Starts the restore of the IDB in the read mode. `omnidbrestore` reads the options and arguments from the file that has been created manually or using the `-autorecover -save` *OptionFile* command. This is useful in case the restore devices are different from the backup devices (or attached to a different system). In such a case the *OptionFile* has to be manually updated with the appropriate restore device data before the restore is started.

RMA_Options

`-mahost` *DeviceHostname*
 Specifies the client with the attached backup device.

`-policy` *LogicalDevicePolicy*
 Specifies the backup device policy ID. Policy can be defined as 1 (Standalone), 3 (Stacker), 5 (Jukebox), 6 (external control), 8 (Grau DAS exchanger library), 9 (STK Silo medium library) or 10 (SCSI Library).

`-type` *DeviceType*
 Specifies the media type. Media type numbers are specified in the *HP Data Protector product announcements, software notes, and references*.

`-dev` *PhysicalDevice*
 Physical device path.

`-name` *LogicalDeviceName*
 Specifies the backup device name. Note that this is only used in output messages and can be omitted.

`-description` *DeviceDescription*
 Specifies the backup device description. Note that this is only used in output messages and can be omitted.

`-blksize` *BlkSize*
 Specifies the block size that was used when the backup was made.

`-ioctl` *RoboticsDevice*
 Physical path of the library device.

`-remhost RoboticsHostname`

Use the `-remhost` option to specify the client with the attached library device, if the library device is connected to a system other than *mahost* (Media Agent host)

VRDA_Options

`-daid DAID`

Disk Agent ID of the database backup.

`-overwrite | -no_overwrite`

By default, or if the `-overwrite` option is specified, the already existent files on the disk are overwritten by the restored files. If the `-no_overwrite` option is specified, only the files that do not exist on the disk are restored.

Media_Options

`-maid mediumID1 [mediumID2...]`

Lists media IDs needed for the restore.

`-slot slot1[:flip1] [slot2[:flip2]...]`

Lists the slots where media are located. Note that the sequence has to match the sequence in the list created using the `-maid` option.

`-position segment1:offset1 [segment2:offset2...]`

Lists media positions of the database backup. Note that the sequence has to match the sequence in the list created using the `-maid` option.

General_Options

`-verbose`

By default, the MA and DA messages are not displayed. If this option is specified they are displayed.

`-tree path1 [path2...]`

Specifies the IDB directories and their subordinate files and subdirectories to be restored. If this option is not specified, all IDB directories are restored.

`-preview`

Runs the restore preview.

`-skiprestore`

Does not start the actual restore. This option should only be used in combination with the `-save`, `-optview` or `-logview` option.

`-keyfile Path`

Triggers the retrieval of a decryption key. By default, the *IDB-ClientName-key.csv* file is read.

If this file does not exist, enter a full path to the `IDB-ClientName-key.csv` file that resides on the Cell Manager in the directory
`Data_Protector_program_data\Config\Server\export\keys`
(Windows Server 2008),
`Data_Protector_home\Config\Server\export\keys` (other Windows systems), or `/var/opt/omni/server/export/keys` (UNIX systems).

Autorecover Options

`-session sessionID`

Instead of selecting the last valid backup of the database, the backup from the specified session is selected. Note that the specified session must exist in the `obrindex.dat` file.

`-save OptionFile`

Saves the options and arguments generated by the `-autorecover` option in the specified file in order to run the `omnidbrestore` in the read mode later.

`-logview`

Displays the contents of the `obrindex.dat` file. The `obrindex.dat` file resides on the Cell Manager in the directory

`Data_Protector_program_data\db40\logfiles\rlog` (Windows Server 2008), `Data_Protector_home\db40\logfiles\rlog` (other Windows systems), or `/var/opt/omni/server/db40/logfiles/rlog` (UNIX systems).

`-optview`

Displays the restore job options.

`-replay_only`

If this option is specified, only the roll forward of the transactions made to the IDB is performed. The transaction log to start the roll forward operation with is read from the `obrindex.dat` file or specified by the `-firstlog` option. The IDB files are not restored.

`-firstlog FirstTransactionLog`

This option specifies the first transaction log to start the roll forward of the transactions to the IDB with. It is to be used only in combination with the `-replay_only` option. Note that this option can be used only if the archiving of the transaction logs is enabled by setting the *Archiving* parameter in the `rdmsserver.ini` file to 1. The `rdmsserver.ini` file resides on the Cell Manager in the directory

`Data_Protector_program_data\db40\datafiles\catalog` (Windows Server 2008), `Data_Protector_home\db40\datafiles\catalog` (other Windows systems), or `/var/opt/omni/server/db40/datafiles/catalog` (UNIX systems).

NOTES

The `omnidbrestore` command stops (before the restore) and restarts (after the restore) all Data Protector services on UNIX systems and all services except the Data Protector Inet service on Windows systems. This command does not stop the Data Protector services running in a cluster.

EXAMPLES

The following example illustrates how the `omnidbrestore` command works.

1. To start the restore of the IDB in the autorecover mode, run:

```
omnidbrestore -autorecover
```

2. The SCSI backup device with DLT media is connected to the client machine.company.com (with a Media Agent installed on the client) with SCSI address scsi2:0:0:0C, while the robotics device is connected to the client machine2.company.com with SCSI address scsi2:0:0:1. The media ID of the medium needed is 3203110a:3acda75a:0690:0001, the medium is in the 1:-1 slot, position of the IDB backup on the medium is 1:0 and DA ID is 986556451. To restore IDB using the above data, run:

```
omnidbrestore -policy 10 -type 10 -mahost  
machine.company.com -dev scsi2:0:0:0C -daid 986556451  
-remhost machine2.company.com -ioctl scsi2:0:0:1 -maid  
3203110a:3acda75a:0690:0001 -slot 1:-1 -position 1:0
```

3. To start the restore of the IDB in the autorecover mode using the backed up files from a specific session, run:

```
omnidbrestore -autorecover -session 2008/04/12-1
```

4. To start the IDB restore in the autorecover mode of the client system "pollux.hp.com" using encrypted backed up files from a specific session and the corresponding decryption keys from the "IDB-pollux.hp.com-key.csv" file, run:

```
omnidbrestore -autorecover -session 2008/03/16-8 -keyfile  
IDB-pollux.hp.com-key.csv
```

SEE ALSO

`omnidb(1)`, `omnidbcheck(1M)`, `omnidbinit(1M)`, `omnidbsmis(1)`, `omnidbupgrade(1M)`, `omnidbutil(1M)`, `omnidbva(1)`, `omnidbvss(1)`, `omnidbvp(1)`, `omnir(1)`

omnidbupgrade

converts filenames in the IDB to the new internal character encoding used in Data Protector A.06.11 and thus enables the correct handling of non-ASCII characters in filenames in the Data Protector GUI

(this command is available on the Data Protector Cell Manager)

omnidbupgrade

SYNOPSIS

```
omnidbupgrade -version | -help
omnidbupgrade -fname -udp
omnidbupgrade -fname -estimate
```

DESCRIPTION

Omnidbupgrade converts filenames in the IDB to the new character encoding introduced in Data Protector A.06.11. The conversion can be performed only on Windows Cell Manager for all non-Windows clients containing filenames with non-ASCII characters. The command will convert filenames for all clients not marked as already converted from the old character encoding to the new one.

The IDB conversion does not affect backup and restore. If conversion of data for a specific client is running and at the same time backup of the same client is started, no filenames or directories will be logged to the IDB for this client (as if `log none` option in GUI was used for backup).

Back up the IDB before running `omnidbupgrade`.

OPTIONS

`-version`

Displays the version of the `omnidbupgrade` command

`-help`

Displays the usage synopsis for the `omnidbupgrade` command.

`-fname -udp`

Converts filenames in the IDB.

`-fname -estimate`

Estimates the time needed for the conversion. This option is possible only before IDB conversion has been performed.

NOTES

The `omnidbupgrade` command is available on Windows systems only.

Backup will not log files or directories for the client that is being converted while his backup is running. It is recommended to back up the IDB before converting it using `omnidbupgrade`.

SEE ALSO

`omnidb(1)`, `omnidbcheck(1M)`, `omnidbinit(1M)`, `omnidbrestore(1M)`, `omnidbsmis(1)`, `omnidbutil(1M)`, `omnidbva(1)`, `omnidbvss(1)`, `omnidbxp(1)`

omnidbutil

handles various Data Protector internal database (IDB) maintenance tasks
(this command is available on the Data Protector Cell Manager)

omnidbutil

SYNOPSIS

```
omnidbutil -help
omnidbutil -version
omnidbutil -list_dcdirs
omnidbutil -add_dcdir Pathname [-maxsize Size_MB] [-maxfiles Num-
berOfFiles] [-spacelowSize_MB] [-seqNumber]
omnidbutil -modify_dcdir Pathname [-maxsize Size_MB] [-maxfiles
NumberOfFiles] [-spacelowSize_MB] [-seqNumber]
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 [-all]
omnidbutil -free_locked_devs [-all | DevName | MediumID | CartName
PhyLocation | Serial_LDEV | WWW_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 -modifytblspace
omnidbutil -purge {-filenames [host_1 [host_n...]] [-force] | -ses-
sions [NumberOfDays] | -days [NumberOfDays] | -messages [NumberOf-
Days] | -dcbf | -mpos | -daily}
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 CSVFile]
omnidbutil -list_large_mpos MinNumberOfMpos [-top NumOfTopMedia] [-detail] [-csv CSVFile]
omnidbutil -list_mpos_without_overs [-csv CSVFile]
omnidbutil -free_cell_resources

```

DESCRIPTION

The `omnidbutil` command is used for Data Protector internal database (IDB) maintenance tasks. These tasks involve:

OPERATIONS ON DETAIL CATALOG BINARY FILES (DCBF)

The Detail Catalog (DC) is composed of three parts: 1) Catalog Database (CDB) tablespace containing pathnames of backed up files together with client system names. 2) The Detail Catalog Binary Files (DCBF) part, which stores file version information (file size, modification time, attributes/protection, exact position on a medium (block level) and so on). 3) DCBF directories: registered directories that contain DCBF. A DCBF directory is allocated when creating new DCBF using one of three possible allocation algorithms, specified in the Data Protector global options file by the *DCDirAllocation* option. The Data Protector global options file resides on the Cell Manager in the directory

Data_Protector_program_data\Config\Server\options (Windows Server 2008), *Data_Protector_home*\Config\Server\options (other Windows systems) or */etc/opt/omni/server/options* (UNIX systems).

Operations on DCBF include: 1) Registering, removing and updating DCBF directories. 2) Locating DCBF across DCBF directories if they had been moved manually. 3) Removing invalid references to DCBF. Invalid references can occur after the DB recovery during which the replay of IDB transaction logs is executed. In this case CDB is newer than DCBF.

The `omnidbutil` options used for operations on DC are: `-list_dcdirs`, `-add_dcdir`, `-modify_dcdir`, `-remove_dcdir`, `-remap_dcdir` and `-fixmpos`.

EXPORTING AND RE-CREATING THE CONTENTS OF THE MEDIA MANAGEMENT DATABASE (MMDB) AND CDB

The contents of MMDB and CDB can be exported to and re-created from text files. Text files are in the ASCII format on UNIX systems and in the UNICODE format on Windows systems.

The `omnidbutil` options used for exporting and re-creating the contents of MMDB and CDB are: `-readdb` and `-writedb`.

LISTING AND UNLOCKING BACKUP DEVICES, TARGET VOLUMES, MEDIA AND LIBRARY SLOTS

Backup devices, target volumes, media and library slots in use are locked during backup and restore. In certain situations (backup or restore session ends abnormally), devices remain locked, even though the MA, SSEA, SNAPA, or SMISA is not running. By default, such devices are unlocked after 60 min. The user can list all locked and unlock devices, target volumes, media and library slots.

The `omnidbutil` options used for listing and unlocking backup devices, target volumes, media and library slots are: `-show_locked_devs` and `-free_locked_devs`.

MERGING LOCAL MMDB INTO CENTRALIZED MEDIA MANAGEMENT DATABASE (CMMDB)

In larger multi-cell environments with high-end backup devices, you may want to share these devices and media among several cells. This can be achieved by having one centralized MMDB database for all the cells and keeping an individual CDB database for each cell. This allows media and device sharing while preserving the security capabilities of the multi-cell structure. To achieve this, the local MMDB must be merged into the CMMDB.

The `omnidbutil` option used for merging MMDB into CMMDB is `-mergemmdb`.

SYNCHRONIZING CDB AND MMDB

In certain situations, CDB and MMDB may be out of sync (different `readdb` of CDB and MMDB, restore of CMMDB while leaving local CDB intact, etc.). In this case both DBs must be synchronized.

The `omnidbutil` option used for synchronizing CDB and MMDB is `-cdbsync`.

MISCELLANEOUS TASKS

These tasks involve operations such as extending tablespaces, purging the obsolete pathnames from the CDB, displaying the information about the IDB and the IDB upgrade, changing references in object versions from one device to some other device, changing the owner of the CDB to the current Cell Manager, displaying the CDB owner, and more.

The omnidbutil options used for this group of tasks are: `-changebdev`, `-extendfnames`, `-extendtblspace`, `-extendinfo`, `-purge`, `-purge_stop`, `-info`, `-clear`, `-change_cell_name`, `-show_cell_name`, `-set_session_counter`, `-upgrade_info`, `-show_db_files`, `-free_pool_update`, `-list_large_directories`, `-list_large_mpos`, `-list_mpos_without_overs`, `-top`, and `-csv`.

The following options, `-purge`, `-filenames`, `-fixmpos`, and `-purge_failed_copies` require exclusive access to the IDB. Prior to using such options, ensure that no backup, restore, or media management sessions are in progress and that no graphical user interfaces are running in the cell.

OPTIONS

`-version`

Displays the version of the omnidbutil command

`-help`

Displays the usage synopsis for the omnidbutil command.

`-list_dcdirs`

Lists all registered DCBF directories.

`-add_dcdir Pathname [-maxsize Size_MB]`

`[-maxfiles NumberOfFiles] [-spacelow Size_MB] [-seq Number]`

Adds (registers) a new DC directory in the directory specified by this option.

The `-maxsize` option specifies the amount of disk space that can be used for DCBF in this directory. When the specified size is reached, Data Protector stops creating new DCBF files in this directory. If this option is not specified, then the default size of 16384 MB is used.

When you increase the maximum size, you should also adjust the free disk space needed for a DCBF binary file (10 to 15% of the maximum size is recommended) by using `-spacelow` option.

The `-maxfiles` option specifies the number of DCBF that can be stored in the directory. When the specified number is reached, Data Protector stops creating new DCBF in this directory. If this option is not specified, then the default value of 500 files is used. Only values under 10000 are valid.

The `-spacelow` option defines the actual free disk space needed for a DCBF binary file to be created. When the free space falls below the specified free disk space, Data Protector stops creating new DCBF in this directory. If this option is not specified, the default of 2048 MB is used.

The `-seq` option sets the sequence number for the new DCBF directory. Each DCBF directory has a certain position which determines when DCBF will be created in the DCBF directory. The first DCBF directory to be used for DCBF has the lowest sequence number. The order of the DCBF directories to be used is determined by the sequence number. Sequence is used only if the *DCDirAllocation* option in the Data Protector global options file is set to 0. The Data Protector global options file resides on the Cell Manager in the directory *Data_Protector_program_data\Config\Server\options* (Windows Server 2008), *Data_Protector_home\Config\Server\options* (other Windows systems) or */etc/opt/omni/server/options* (UNIX systems). If the `-seq` option is not specified, 0 will be used.

```
-modify_dcdir Pathname [-maxsize Size_MB]
                        [-maxfiles NumberOfFiles] [-spacelow Size_MB] [-seq
                        Number]
```

Modifies a DCBF directory under the specified path.

The `-maxsize` option modifies the amount of disk space that can be used for DCBF in this directory. When the modified size is reached, Data Protector stops creating new DCBF in this directory. If this option is not specified, then the default size of 16384 MB is used.

When you increase the maximum size, you should also adjust the free disk space needed for a DCBF binary file (10 to 15% of the maximum size is recommended) by using `-spacelow` option.

The `-maxfiles` option modifies the number of DCBF that can be stored in the directory. When the modified number is reached, Data Protector stops creating new DCBF in this directory. If this option is not specified, then the default value of 500 files is used. Only values under 10000 are valid.

The `-spacelow` option modifies the actual free disk space needed for a DCBF binary file to be created. When the free space falls below the modified free disk space, Data Protector stops creating new DCBF in this directory. If this option is not specified, the default of 2048 MB is used.

The `-seq` option modifies the sequence of a DCBF directory. Each DCBF directory has a certain position which determines when DCBF will be created in the DCBF directory. Sequence is used only if the *DCDirAllocation* option in the Data Protector global options file is set to 0. The Data Protector global options file resides on the Cell Manager in the directory *Data_Protector_program_data\Config\Server\options* (Windows Server 2008), *Data_Protector_home\Config\Server\options* (other Windows systems) or */etc/opt/omni/server/options* (UNIX systems). If the `-seq` option is not specified, 0 will be used.

```
-remove_dcdir Pathname
```

Removes (unregisters) the given DCBF directory. The directory must not hold any DCBF and will not be removed.

`-remap_dcdir`

Locates DCBF across all DCBF directories and updates DCBF locations in the IDB if they had been moved manually (using the `mv` command or similar) between DCBF directories. This makes the IDB aware of the locations of each DCBF. This option requires exclusive access to the database.

`-fixmpos`

Removes invalid references to DCBF. This option should be used in the case of IDB recovery (after tablespaces `dbreplay` or `-import_logs`) or after a DCBF has been manually removed. This option requires exclusive access to the database.

`-readdb[-mmdb Directory] [-cdb Directory] [-no_detail]
[-check_overs]`

Reads the files in the specified directories and uses this information to rebuild the IDB. As a prerequisite, the files must have been created using the `-writedb` option, and a copy of the DCBF, SMBF and SIBF directories must have been created. The `-mmdb` option specifies a directory to use for the MMDB. The `-cdb` option specifies a directory for the CDB. Only the database for which you specify the directory is imported. Move the copy of the DCBF, SMBF and SIBF directories to their position in the IDB directory structure.

DCBF default location:

On Windows Server 2008: *Data_Protector_program_data\db40\dcbf*

On other Windows systems: *Data_Protector_home\db40\dcbf*

On UNIX systems: */var/opt/omni/server/db40/dcbf*

SMBF default location:

On Windows Server 2008: *Data_Protector_program_data\db40\msg*

On other Windows systems: *Data_Protector_home\db40\msg*

On UNIX systems: */var/opt/omni/server/db40/msg*

SIBF default location:

On Windows Server 2008: *Data_Protector_program_data\db40\meta*

On other Windows systems: *Data_Protector_home\db40\meta*

On UNIX systems: */var/opt/omni/server/db40/meta*

Use the `-no_detail` option to skip the recovery of references to DCBF, SMBF and SIBF. If the recovery of these references is skipped, the copy of DCBF, SMBF and SIBF directories is not needed.

Use the `-check_overs` option to check if object version details are correct. Note that this operation can be very time consuming. Error details are saved on the Cell Manager in the file

Data_Protector_program_data\log\server\readascii.log

(Windows Server 2008),

Data_Protector_home\log\server\readascii.log (other Windows systems), or */var/opt/omni/server/log/readascii.log* (UNIX systems).

`-writedb [-cdb Directory] [-no_detail]`

Writes the IDB tablespaces (without the DCBF, SMBF and SIBF) to files in the specified directories. The `-mmdb` option specifies a directory to use for the MMDB and the `-cdb` option specifies a directory for the CDB. Only the database for which you specify the directory is exported. During the operation, when in prompt mode, manually copy the DCBF, SMBF and SIBF directories to a safe location since the IDB is in consistent state at that moment. To determine which directories to copy, run the `omnidbutil -list_dcdirs` command. Use the `-no_detail` option to skip the writing of references to DCBF, SMBF and SIBF to files. If these references are skipped, the copy of DCBF, SMBF and SIBF directories is not needed.

`-show_locked_devs [-all]`

Lists all locked devices, target volumes, media, and slots in the Data Protector cell. The `-all` option is applicable only when you run the command on the MoM system, in which case locked devices, target volumes, media and slots from all cells are listed.

`-free_locked_devs [-all | DevName | MediumID | CartName
PhyLocation | Serial_LDEV | WWN_LUN]`

Unlocks a specified device, target volume, medium or slot, where *DevName* is the device, *Serial_LDEV* is the target volume where *Serial* is the HP StorageWorks Disk Array XP serial number and *LDEV* is the HP StorageWorks Disk Array XP volume number, *WWN_LUN* is the target volume where *WWN* is the HP StorageWorks (Enterprise) Virtual Array world-wide-name and *LUN* is the logical unit number (LUN), *MediumID* is the medium, *CartName* is the library name and *PhyLocation* is the number of the slot to be unlocked. If none of the above is specified, all devices, target volumes, media and slots in the Data Protector cell are unlocked. The `-all` option is applicable only when you run the command on the MoM system, in which case all devices, target volumes, media and slots from all cells are unlocked.

`-mergemmdb Cell_Server_Hostname`

Merges the local MMDB from the remote Cell Manager *Cell_Server_Hostname* to the CMMDB. For this action there must exist a MoM cell and a remote cell with a local MMDB. If the command reports no errors

you can disable the local MMDB on the remote Cell Manager by removing (and possibly copying to a safe place) the directory

Data_Protector_program_data\db40\datafiles\mmdb (Windows Server 2008), *Data_Protector_home\db40\datafiles\mmdb* (other Windows systems), or */var/opt/omni/server/db40/datafiles/mmdb* (UNIX systems). All duplicated items (stores, media pools, devices) will have "_N" appended to their name, where N represents the number of the duplicate (starting with 1). Note that once the database is merged you will not be able to revert the operation.

`-cdbsync Cell_Server_Hostname`

Synchronizes the MMDB and the CDB on the specified Cell Manager. The MMDB and CDB may be out of sync when: 1) The MMDB and CDB contain information from different periods in time. This may be the result of the importing (the `-readdb` option) the CDB and the MMDB from files that were the result of separate export (the `-writedb` option) sessions. 2) In a MoM environment, when the local CDB and centralized MMDB are out of sync. This may be the result of the centralized IDB restore.

The command must be executed on the system with the MMDB (one Cell Manager in the cell) or with the centralized MMDB (MoM environment) installed.

In a MoM environment, if the centralized MMDB was changed (as a result of IDB restore or import), the command should be run for each Cell Manager in this MoM cell by specifying each Cell Manager in the cell as the

Cell_Server_hostname argument.

`-purge{-filenames [host_1 [host_n...]] [-force] | -sessions [NumberOfDays] | -days [NumberOfDays] | -messages [NumberOfDays] | -dcbf | -mpos | -daily}`

This option allows you to remove obsolete file names, backup, restore, and media management sessions, session messages, and obsolete DCBF files from the IDB.

The `-filenames` option removes all obsolete file names (file names without any file versions) for a specific or all clients from the CDB. This option requires exclusive access to the database. Data Protector does not start the process for removing obsolete file names if the number of obsolete file names does not exceed a specific threshold. When starting removal for the whole cell, use the `-force` option to enable the removal in cases when there are fewer than 5000000 obsolete file names in the IDB. When starting removal for the specified clients, use the `-force` option to enable the removal also for clients which have fewer than 1000000 obsolete file names in the IDB.

The `-sessions` option removes media management sessions, restore sessions, and obsolete backup sessions (backup sessions without backed up data) older than *NumberOfDays*.

The `-days` option removes media management sessions, restore sessions, and obsolete backup sessions (backup sessions without backed up data) older than *NumberOfDays*.

The `-messages` option removes session messages for all sessions older than *NumberOfDays*.

The `-dcbf` option removes DCBF for all media with expired catalog protection.

The `-mpos` option removes all the object versions and media position records for the overwritten tapes. If the *QuickMediaFormat* option is set to 1 in the global options file, Data Protector will not purge any records during a backup or when a media is formatted. Those obsolete records will be explicitly removed when a purge mpos command is run. If *QuickMediaFormat* is not set, the records will be purged from the database during the course of the backup.

The `-daily` option starts the same purge session as started every day at 12:00 (depending on the Data Protector global options file setting) and is a part of Data Protector daily maintenance tasks. This purge session deletes DCBF based on the catalog protection and removes obsolete sessions and their messages, by running the `omnidbutil -purge -sessions KeepObsoleteSessions -messages KeepMessages -dcbf` command, where *KeepObsoleteSessions* and *KeepMessages* are specified in the Data Protector global options file. Default values for these two parameters are 30 and 0, respectively. The Data Protector global options file resides on the Cell Manager in the directory

Data_Protector_program_data\Config\Server\options (Windows Server 2008), *Data_Protector_home*\Config\Server\options (other Windows systems) or */etc/opt/omni/server/options* (UNIX systems). The scheduled time for the `-daily` option to start every day is defined by the *DailyMaintenanceTime* option in the Data Protector global options file.

At least one of these options must be specified. You can change or disable the global option *DailyMaintenanceTime* for the `-daily` option.

`-purge_failed_copies`

In certain circumstances the Data Protector IDB may hold multiple copies of objects made during a backup. Use this option to remove all unrequired copies that may overload an IDB. This option requires exclusive access to the database.

`-purge_stop`

Use this option to stop a running file name purge session. This command only sends a stop request to the Purge Session Manager. The response may not be immediate.

`-extendfnames Pathname -maxsize Size_MB`

Creates additional extent (tablespace). The directory specified by this option must exist and be capable of holding a tablespace of the size specified by `-maxsize` parameter prior to executing this option. The tablespace cannot be larger than 2047 MB.

`-extendtblspace Tablespace Pathname -maxsize Size_MB`

Creates an additional extent for the specified tablespace. The specified directory must exist and be capable of holding an extent of the size specified by the `-maxsize` parameter prior to executing this option. An extent cannot be larger than 2047 MB.

`-extendinfo`

Displays information about existing extents.

`-modifytblspace`

Adjusts the maximum size of database files (`dirs.dat`, `fnames.dat`, `fn?.ext`, and their extension files) to 2 GB.

This command should be used only on HP-UX 11.23 and 11.31 (Itanium) and Linux x86-64 systems, after an upgrade to Data Protector A.06.11 if the IDB files exceed 2 GB.

IMPORTANT: Use this command only as a part of the proper adjustment procedure described in the Troubleshooting chapter of the *HP Data Protector installation and licensing guide*. If you do not perform all necessary steps (exporting and importing), the IDB will become unusable.

`-changebdev FromDev ToDev [-session SessionID]`

Changes all references in object versions from device `FromDev` to device `ToDev`. You can change the device name only for a single session by using the `-session` option.

`-info`

Displays information about the IDB.

`-clear`

Sets the status of all sessions that are actually not running but are marked *In Progress/Failed*, to *failed*. It requires exclusive database access to ensure that no session is running.

`-change_cell_name [old_host]`

This option changes the owner of the CDB to the current Cell Manager. It also changes all references in the CMMDB from `old_host` to the current Cell Manager. It modifies all media entries within the MMDB or CMMDB associated with the original Cell Manager (old host).

If the `old_host` parameter is not specified, `omnidbutil` determines the previous owner of the CDB (old host) from the database itself.

If you want to associate all media in a CMMDB with the current Cell Manager, it is necessary to run the command once for each Cell Manager that has media associated with it, using the *old_host* parameter.

The *old_host* parameter must be specified exactly the same as the owner of the media. If the system's Fully Qualified Domain Name (FQDN) is associated with the media, then you must also use the FQDN with this command. If the *old_host* parameter is not specified correctly, the operation will not be performed.

This command is used after moving databases from one Cell Manager to another or after using `-readdb` on files that were created on another Cell Manager.

`-show_cell_name`

Queries the CDB for its owner. If there is no information available, use the `-change_cell_name` option to update the information.

`-set_session_counter new_session_ID`

Sets a new value for the counter that is used for generating the sessionID. This option is used after the restore and recovery of the IDB to enable the import of tapes that were created on the same day. Suggested value is 100.

`-upgrade_info`

Displays the information about the upgrade of the IDB. The possible return strings are:

- No upgrade in progress.
- Upgrade of core part failed.
- Upgrade of core part finished.
- Upgrade of detail part running.
- Upgrade of detail part finished.

`-show_db_files`

Lists all directories and extension files that are backed up during IDB backup. In effect they contain all components of IDB.

`-free_pool_update`

Finds any free (unprotected) media in pools with the `free pool` and move free media to free pool options set and by default deallocates the found free media to a free pool every day at 00:00.

`-list_large_directories MinNumberOfFiles [-top NumOfTopDirectories] [-detail] [-csv CSVFile]`

Lists top *NumOfTopDirectories* directories that have more than *MinNumberOfFiles* files. By default, only the number of records and the directory name are displayed. With the `-detail` option, additional fields are

displayed: the number of actual files in the directory, the number of used pages, the number of records per page, and the last file key. Every report is logged to the `list_large_dirs.log` file. Optionally, the report can be written to a comma separated values (CSV) file specified with the `-csv` option.

```
-list_large_mpos MinNumberOfMpos [-top NumOfTopMedia] [-detail]
[-csv CSVFile]
```

Lists top *NumOfTopMedia* media that has more than *MinNumberOfMpos* media positions. By default, positions used, pages used, positions/page, and medium are displayed. With the `-detail` option, additional fields are displayed: the total object versions, the data protected object versions, the catalog protected object versions, and the last-write time for medium. Every report is logged to the `list_large_media.log` file. Optionally, the report can be written to a comma separated values (CSV) file specified with the `-csv` option.

```
-list_mpos_without_overs [-csv CSVFile]
```

Lists orphaned media positions. Orphaned media positions are positions that are no longer linked to any object version.

```
-free_cell_resources
```

Frees all resources that were allocated during backup and restore sessions. The option is used if a session ends abnormally or a process is terminated unexpectedly.

EXAMPLES

The following examples illustrate how the `omnidbutil` command works.

1. To create a new DC directory in the `"/var/opt/test"` directory with maximum size 1000 MB, run:

```
omnidbutil -add_dc /var/opt/test -maxsize 1000
```
2. To list all locked devices, target volumes, media, and slots, run:

```
omnidbutil -show_locked_devs
```
3. To unlock a device, a medium, or library slot, respectively, run:

```
omnidbutil -free_locked_devs machine
omnidbutil -free_locked_devs 0a1106452:5a45add9:2548:0007
omnidbutil -free_locked_devs libraryName phyLocation
```
4. To unlock a target volume with the HP StorageWorks Disk Array XP serial number of "30658" and the HP StorageWorks Disk Array XP volume number of "288", run:

```
omnidbutil -free_locked_devs 30658_288
```


5. To manually change the maximum size for DC directory "dcbf16" in the "C:\Program Files\OmniBack\db40" directory to 48 GB and modify the free disk space needed for a DCBF binary file (10 to 15% of the maximum size is recommended), run:

```
omnidbutil -modify_dcdire C:\Program
Files\OmniBack\db40\dcbf16 -maxsize 49152 -spacelow 7372
```
6. To save the IDB without detail catalogs (DC binary files and filenames) as ASCII files to the directories "cdb" and "mmdb" in the "D:\TMP" directory, run:

```
omnidbutil -writedb -no_detail -cdb D:\TMP\cdb -mmdb
D:\TMP\mmdb
```
7. To read the IDB from the ASCII files in the directories "D:\TMP\cdb" and "D:\TMP\mmdb", run:

```
omnidbutil -readdb -cdb D:\TMP\cdb -mmdb D:\TMP\mmdb
```
8. To manually remove expired sessions and session messages older than 30 days, obsoleted data from the DCBF part of the IDB and all the object versions and media position records for the overwritten tapes if the Daily Maintenance is disabled, respectively, run:

```
omnidbutil -purge -sessions 30
omnidbutil -purge -messages 30
omnidbutil -purge -dcbf
omnidbutil -purge -mpos
```
9. To remove all unrequired copies of objects that were made during a backup and may overload the IDB, run:

```
omnidbutil -purge_failed_copies
```

SEE ALSO

omnidb(1), omnidbcheck(1M), omnidbinit(1M), omnidbrestore(1M), omnidbsmis(1), omnidbupgrade(1M), omnidbva(1), omnidbvss(1), omnidbexp(1)

omnidlc

gathers or deletes Data Protector debug, log, and getinfo files from the Data Protector cell or from a MoM environment
(this command is available on the Data Protector Cell Manager)

omnidlc

SYNOPSIS

```
omnidlc -version | -help
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]
omnidlc -localpack [filename]
omnidlc -unpack [filename]
omnidlc -uncompress filename
omnidlc [-hosts list] -del_ctracelog
```

DESCRIPTION

The `omnidlc` command collects Data Protector debug, log, and getinfo files from the Data Protector cell (by default, from every client).

The Data Protector debug files are created during a Data Protector debug session. By default, the command collects debug files from the Data Protector default debug files directory, which is `Data_Protector_program_data\tmp` (Windows Vista, Windows Server 2008), `Data_Protector_home\tmp` (other Windows systems), `/tmp` (UNIX systems), and `OMNI$ROOT:[TMP]` (HP OpenVMS). To collect debugs also from other directories, use the `-debug_loc` option.

Using the command, it is possible to collect Data Protector debug, log and getinfo files from selected clients in the Data Protector cell. In a MoM environment, you can only collect data for each Data Protector cell separately by running the command from the respective Cell Manager. On OpenVMS systems, getinfo files are not collected because the `get_info` utility is not available.

Additionally, the Data Protector debug files to be collected can be limited to debugs that were generated within the specified Data Protector session or to debugs identified by a debugID or by a debug filename (debug postfix).

By default, every collected debug, log and getinfo file is then compressed and sent over the network to the Cell Manager. The final extension `.gz` is added on the Cell

Manager, where all collected files with the `.gz` extension are, by default (if the `-depot` option is not specified), packed and saved in the current directory as the `dlc.pck` file. The file includes a generated directory structure that includes the hostnames, paths and the (compressed) collected files of the clients involved. This directory structure is described further on in this man page.

Optionally, files can be sent over the network to the Cell Manager uncompressed (if the `-no_compress` option is specified). Besides that (if the `-depot` option is specified), the transferred files can be left unpacked in the specified directory on the Cell Manager, in which the directory structure that includes the hostnames, paths and the collected files of the clients involved is generated as follows:

On UNIX:

```
./dlc/system_1/tmp/debug_files
./dlc/system_1/log/log_files
./dlc/system_1/getinfo/get_info.txt
./dlc/system_2/tmp/debug_files
./dlc/system_2/log/log_files
./dlc/system_2/getinfo/get_info.txt
...
```

On Windows:

```
.\dlc\system_1\tmp\debug_files
.\dlc\system_1\log\log_files
.\dlc\system_1\getinfo\get_info.txt
.\dlc\system_2\tmp\debug_files
.\dlc\system_2\log\log_files
.\dlc\system_2\getinfo\get_info.txt
...
```

If the file to be sent over the network is larger than 2GB, the file is split in 2GB chunks before it is compressed (it can be left uncompressed) and sent to the Cell Manager. Every chunk retains the file name and is added the first extension ranging from `s001` to `s999`. The second extension (`.gz`) is not added if the files are not compressed. Additionally, on the Cell Manager side, if the size of all collected compressed or uncompressed files exceeds 2GB, the collected files are packed in 2GB sized (original size) packages and added an extension ranging from `s001` to `s999`.

The collected debug files can also be deleted (if the `-delete_dbg` option is specified), or the disk space required on the Cell Manager for the collected files can be displayed (if the `-space` option is specified). In these two cases, the selected files are neither transferred from the clients to the Cell Manager nor packed on the Cell Manager.

When collecting or deleting files or when displaying the required disk space, additional criteria can be defined to limit the files selection. Thus, it is possible to exclude the `getinfo` file, the log files, the debug files or any combination of the three groups of files from the selection.

Using the command, the collected files can then be additionally packed to be sent to the support center. The command provides also a means of unpacking the packed collected files.

OPTIONS

`-version`

Displays the version of the `omnidlc` command.

`-help`

Displays the usage synopsis for the `omnidlc` command.

`-session sessionID`

Limits the collected debug files to those that were produced during the Data Protector session identified by the *sessionID*. Note that on OpenVMS, the `omnidlc` command run with the `-session` parameter does not collect the debug files produced during specified session, because session names are not part of the OpenVMS debug filename. Instead, all available logs are collected.

`-did debugID`

Limits the collected debug files to those identified by the *debugID*.

`-postfix string`

Limits the collected debug files to the specified debug postfix.

`-no_filter`

Does not limit (select) the collected debug files.

`-hosts list`

Limits the files to be collected to the clients specified in the *list*. The hostnames must be separated by spaces. The debug files collected are still subject to `-session`, `-did` or `-postfix` options.

`-pack filename`

All collected files are, by default (if this option is not specified), packed and saved in the current directory as the `dlc.pck` file. If this option is specified, the collected files are packed and saved in the specified file in the current directory on the Cell Manager. If the full path name is specified, the files are packed and saved in the specified file in the specified directory.

To add files other than the collected files to the package, copy the files to one of the following directories before running the command:

`dlc/client/getinfo`, `dlc/client/log`, or `dlc/client/tmp` (on UNIX), or `.\dlc\client\getinfo`, `.\dlc\client\log`, or `.\dlc\client\tmp` (on Windows). You cannot add directories, but only files. If the files are not copied to one of the specified directories, the package cannot be unpacked during the unpack phase.

`-depot [Directory]`

If the *Directory* is specified, the collected files are not packed and are saved to the `dlc` directory of the specified directory. If the *Directory* is not specified, the files are saved on the Cell Manager in the directory

`Data_Protector_program_data\tmp\dlc` (Windows Server 2008), `Data_Protector_home\tmp\dlc` (other Windows systems), or `/tmp/dlc` (UNIX systems).

`-space`

Displays the disk space required on the Cell Manager for the collected files.

`-delete_dbg`

Deletes the selected files on clients. On OpenVMS, if run together with the `-session` parameter, the command does not delete any debugs from the debug files directory.

`-no_getinfo`

Excludes the `getinfo` file from the selection. For OpenVMS, this parameter is not applicable as OpenVMS systems do not have the `get_info` utility.

`-no_config`

Excludes the configuration information from the selection.

`-no_logs`

Excludes the log files from the selection.

`-no_debugs`

Excludes the debug files from the selection.

`-no_compress`

Disables the compression of the collected files on clients. By default, the compression is enabled.

`-debug_loc dir1 [dir2]...`

Includes debugs not only from the default debug files directory but also from other directories, *dir1*, *dir2*,.... Note that the subdirectories are excluded from the search. If a specified directory does not exist on a particular client, the directory is ignored.

This option is valid only if the `-no_debugs` option is not specified.

`-verbose`

Enables verbose output. By default, verbose output is disabled.

`-add_info path`

Includes the additional information (for example, screenshots, pictures and the like) from a directory on client identified by *path*.

The `-any` option is used when the directory path is the same for all clients. It is important to make sure the path is not host-specific before using this option.

`-localpack [filename]`

Packs the directory structure from the current directory (must be the directory containing the dlc directory generated by the `-depot` option) to the *filename*. If the *filename* is not specified, the `dlc.pck` file is created in the current directory.

This option is equivalent to the `-pack` option, but is to be used only if the data is collected using the `-depot` option.

To add files other than the collected files to the package, copy the files to one of the following directories before running the command:

`dlc/client/getinfo`, `dlc/client/log`, or `dlc/client/tmp` (on UNIX), or `.\dlc\client\getinfo`, `.\dlc\client\log`, or `.\dlc\client\tmp` (on Windows). You cannot add directories, but only files. If the files are not copied to one of the specified directories, the package cannot be unpacked during the unpack phase.

`-unpack [filename]`

Creates the `dlc` directory in the current directory, and unpacks the contents of the *filename* to the `dlc` directory. If the *filename* is not specified, the `dlc.pck` file in the current directory is unpacked.

Use this option when the collected (compressed or uncompressed) data was packed on the Cell Manager either using the `-pack` option or the `-localpack` option.

`-uncompress filename`

Uncompresses the unpacked compressed single file in the current directory.

Use this option after the packed data is unpacked using the `-unpack` option.

`[-hosts list] -del_ctracelog`

Deletes `ctrace.log` files containing the information where (on which clients) debug logs are generated and which debug prefixes are used. If the `-hosts list` option is specified, the command deletes `ctrace.log` files on specified clients only. Otherwise, `ctrace.log` files on all clients in a cell are deleted.

NOTES

The `omnidlc` command cannot be used to collect the Data Protector installation execution traces.

The Data Protector GUI debug files for systems other than Cell Manager can only be gathered using the `-hosts` option.

To collect debug files in a cluster, the command must be run using the `-hosts` option; the cluster nodes hostnames must be specified as the argument for the option. In a cluster, if the `-hosts` option is not specified, the data is collected from the active node.

Paths specified in postfix are not allowed.

EXAMPLES

1. To collect and compress all debug, log and getinfo files from the cell, and pack them in the "dlc.pck" file in the current directory on Cell Manager, using the verbose output, run:

```
omnidlc -no_filter -verbose
```
2. To collect only the log and debug files (without the getinfo files) from the clients "client1.company.com" and "client2.company.com" to the directory "c:\depot" on the Cell Manager, without compressing and packing the files, run:

```
omnidlc -no_filter -hosts client1.company.com  
client2.company.com -depot c:\depot -no_getinfo  
-no_compress
```
3. To collect log, debug, and getinfo files from the client "client1.company.com", compress and pack them to the "c:\pack\pack.pck" file on the Cell Manager, run:

```
omnidlc -hosts client1.company.com -pack c:\pack\pack.pck
```
4. To collect log, debug, and getinfo files from the default location and debugs from the additional directories, "C:\tmp" and "/temp/debugs", from the clients "client1.company.com" and "client2.company.com", and to compress and pack the files on the Cell Manager, run:


```
omnidlc -hosts client1.company.com client2.company.com  
-debug_loc C:\tmp /tmp/debugs
```

5. To delete all debug log files for the session with the ID "2007/08/27-9", run:

```
omnidlc -session 2007/08/27-9 -delete_dbg
```
6. To display disk space needed on the Cell Manager for the uncompressed debug files with the debugID "2351" from the client "client.company.com", run:

```
omnidlc -did 2351 -hosts client.company.com -space  
-no_getinfo -no_logs -no_compress
```
7. To pack the additional file located in the oc:\debug directory on the client oclient1.company.com together with debug log files for the session with the ID o2007/11/17-24 , run:

```
omnidlc -session 2007/11/17-24 -add_info -host  
client1.company.com C:\debug
```
8. To pack the directory structure in the current directory (must be the directory containing the dlc directory generated by the -depot option) to the "dlc.pck" file in the same directory, run:

```
omnidlc -localpack
```
9. To unpack the "dlc.pck" file to the "dlc" directory of the current directory, run:

```
omnidlc -unpack
```

SEE ALSO

omnicc(1), omnicellinfo(1), omnicheck(1M), omniinstlic(1M), omnisv(1M)

omnidr

a general purpose Data Protector disaster recovery command. Based on its input, it decides on what type of restore to perform (online restore using `omnir` or offline restore using `omniofflr`), as well as how to perform the restore (whether or not to use live OS features).

(this command is available on systems with the Data Protector User Interface component installed)

omnidr

SYNOPSIS

```
omnidr -version | -help
omnidr [-srd FileName] [-temp[os]] [-drimini PLS] [-map OrgMnt1
TrgMnt1 [-map OrgMnt2 TrgMnt2 ...]] [-[no_]cleanup] [-msclustdb] [GeneralOptions]

GeneralOptions

-target hostname
-local
-report level
```

DESCRIPTION

The `omnidr` command is a general purpose Data Protector disaster recovery command that can be used in all recovery scenarios. Based on its input, `omnidr` decides what type of restore is going to be performed: online restore using `omnir` or offline restore using `omniofflr`, as well as how the restore is going to be performed (using or avoiding live OS features).

OPTIONS

- version
Displays the version of the `omnidr` command.
- help
Displays the usage synopsis for the `omnidr` command.
- srd *FileName*
Specifies the path to the SRD file that contains all required backup and restore object information to perform the restore.

Note that `omnidr` always requires a valid SRD file with updated object information. By default it searches the working directory for `recovery.srd`. If it is not found, an error is reported. The option `-srd` overrides the default name `recovery.srd`

`-temp[os]`

Specifies whether the restore process will run in a temporary OS installation. This way, `omnidr` can determine how to restore `CONFIGURATION` data. If this parameter is not specified, the active system is assumed.

`-drimini P1S`

This option is used to provide location of P1S file if you have interrupted the `drstart` command during the 30 second pause and selected the `install only` option when performing EADR. In this case, the `drstart` command only installs disaster recovery files and exits. You have to start the `omnidr` command manually and provide the path to the P1S file using the `-drimini` option. The default path is `C:\$DRIM$.OB2\OBRecovery.ini`.

`-map OrgMnt TrgMnt`

Specifies mapping of original volumes to current volumes.

`-[no_]cleanup`

When the `-cleanup` option (default) is specified during disaster recovery of an active operating system, `omnidr` prepares a cleanup script and stores it into the `%ALLUSERSPROFILE%\Start Menu\Programs\Startup` folder. At first logon after the boot, the Data Protector disaster recovery installation is removed. When this option is specified during disaster recovery of a temporary operating system, a cleanup command is written into restored software hive in the registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`. The cleanup command is executed at first logon after the boot and it removes the temporary OS installation together with Data Protector disaster recovery installation.

The cleanup script/command is not generated in the following cases:

- If Data Protector installation was found on the system during `omnidr` initialization.
- If the `-no_cleanup` option has been specified.
- If Data Protector disaster recovery installation does not reside in the `%SystemRoot%` folder (in this case it was most likely not installed during Data Protector disaster recovery).
- If the `-debug` option has been specified, the cleanup is not performed, because you would lose the debug information at next logon.

- if the `Minimal Recovery` option has been selected during EADR or OBDR, meaning that only boot and system disks would be recovered.

When `omnidr` is used on a dual-boot machine, it is strongly recommended to use the `-no_cleanup` option.

`-msclustdb`

If this option is specified, `omnidr` restores the Microsoft Cluster database.

GeneralOptions

`-target hostname`

Specifies the target system name. All objects will be restored to a computer specified by the `-target` parameter. If this parameter is not specified, the data will be restored to the system specified in the SRD file.

This option is used in two cases:

- During Disk Delivery disaster recovery the disks being restored can be installed into a client with a different hostname as original, therefore the name of the client must be specified.
- During Manual Disaster Recovery, it is possible, that DHCP protocol is installed (for example, that is the default choice in Windows 2000 setup). In this case, the hostname can be generated automatically by the DHCP server and is different from the original system hostname.

`-local`

Forces offline recovery from a locally attached device. The `devbra` command is used to automatically scan for and configure attached devices. A list of detected devices is displayed if more than one is found and you must select one of them. If this option is not specified, the device used for the restore is going to be the same as the device used during backup.

`-report level`

Specifies the error level report. This is useful if you want to reduce the number of messages written during recovery. For example, since practically all OS files are overwritten during the active OS recovery, this means that innumerable warnings bringing no useful information will be displayed, thus slowing down the recovery. Messages are classified (in ascending order) as: 1 (warning), 2 (minor), 3 (major) and 4 (critical). For example, if 3 is selected, only major and critical messages are reported. By default, all messages are reported.

NOTES

The `omnidr` command is available on Windows systems only.

EXAMPLES

The following examples illustrate how the `omnidr` command works.

1. To use the SRD file stored on a floppy drive for the restore, run:
`omnidr -srd "A:\recovery.srd"`
2. To use the local backup device, run:
`omnidr -local`

SEE ALSO

`omniiso(1)`, `omniofflr(1M)`, `omnisrdupdate(1M)`

omnihealthcheck

checks the status of Data Protector services, the consistency of the Data Protector internal database (IDB), and if at least one backup of the IDB exists (this command is available on the Data Protector Cell Manager)

omnihealthcheck

SYNOPSIS

```
omnihealthcheck -version | -help  
omnihealthcheck [-config ConfigFile]
```

DESCRIPTION

The `omnihealthcheck` command reads the specified configuration file where each line of the file is treated as a separate command and is executed. The commands must be listed with full pathnames except if they are Data Protector commands located on the Cell Manager in the directory `Data_Protector_home\bin` (Windows systems) or the directory `/opt/omni/bin` or `/opt/omni/sbin` (UNIX systems). With the Windows Cell Manager, the configuration file must be in the Unicode format. If the configuration file is not specified, the default file on the Cell Manager is used:

`Data_Protector_program_data\Config\Server\HealthCheckConfig` (Windows Server 2008),

`Data_Protector_home\Config\Server\HealthCheckConfig` (other Windows systems), or `/etc/opt/omni/server/HealthCheckConfig` (UNIX systems).

If the default file is used, `omnihealthcheck` checks if Data Protector services (RDS, CRS, MMD, UIProxy, KMS, `omnitrig`, and `omniinet`) are active, if the Data Protector MMDB is consistent, and if at least one backup of the Data Protector internal database (IDB) exists.

Exit codes of individual commands are inspected at the end.

There are 3 different exit codes for the `omnihealthcheck` command:

- 0: All listed commands and their exit codes have been executed.
- 1: At least one of the commands in the configuration file could not be executed or has completed with an exit code other than 0.
- 2: The configuration file could not be read.

The final health check exit code is 0 (OK) only if all executed commands from the configuration file completed successfully (exit codes of all executed individual commands from the configuration file are 0).

Output of the `omnihealthcheck` command is saved on the Cell Manager in the file `Data_Protector_program_data\log\server\HealthCheck.log` (Windows Server 2008), `Data_Protector_home\log\server\HealthCheck.log` (other Windows systems), or `/var/opt/omni/server/log/HealthCheck.log` (UNIX systems).

If a timeout occurs, `omnihealthcheck` fails.

`omnihealthcheck` is by default scheduled to run daily at 12:00 (noon) as a part of the Data Protector check mechanism. The default schedule value can be changed by changing the `DailyCheckTime` option in the Data Protector global options file. The global options file (`global`) is located on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\options` (Windows Server 2008), `Data_Protector_home\Config\Server\options` (other Windows systems), or `/etc/opt/omni/server/options` (UNIX systems).

OPTIONS

`-version`

Displays the version of the `omnihealthcheck` command.

`-help`

Displays the usage synopsis for the `omnihealthcheck` command.

`-config ConfigFile`

Specifies an alternative configuration file for the `omnihealthcheck` command. Note that you can define the commands to be executed in the health check.

SEE ALSO

`omnirpt(1)`, `omnitrig(1M)`

omniinetpasswd

manages the local Data Protector Inet configuration on Windows systems where the Inet process must be run under a specific user account, and sets a user account to be used by the Installation Server during remote installation
(this command is available on systems with any Data Protector component installed)

omniinetpasswd

SYNOPSIS

```
omniinetpasswd -version | -help
omniinetpasswd -add {User@Domain | Domain\User...} [Password]
omniinetpasswd -delete {User@Domain | Domain\User...}
omniinetpasswd -modify {User@Domain | Domain\User...} [Password]
omniinetpasswd -list [Domain]
omniinetpasswd -clean
omniinetpasswd -[no_]inst_srv_user {User@Domain | Domain\User...}
```

DESCRIPTION

On specific Windows operating systems, the Data Protector Inet process must be run under a specific operating system user account rather than under the local user account SYSTEM. Additionally, on Windows Server 2008 systems, the Data Protector Installation Server must use a specific operating system user account for remote installation. The `omniinetpasswd` command provides functionality for management of Inet configuration on the local system, and functionality for setting a user account that will be used by the Installation Server during remote installation. Use command options `-add`, `-delete`, `-modify`, `-list`, and `-clean` for local Inet configuration management, and options `-inst_srv_user` and `-no_inst_srv_user` for setting a user account to be used for remote installation.

Note that `omniinetpasswd` does not add, remove, or change user accounts in the operating system configuration.

OPTIONS

`-version`

Displays the version of the `omniinetpasswd` command.

`-help`

Displays the usage synopsis for the `omniinetpasswd` command.

`-add {User@Domain | Domain\User} [Password]`

Adds the specified user account from the local Inet configuration. `Omniinetpasswd` prompts for the password if not specified in the command line.

`-delete {User@Domain | Domain\User}`

Removes the specified user account from the local Inet configuration. `Omniinetpasswd` prompts for the password if not specified in the command line.

`-list Domain`

Lists user accounts from the local Inet configuration: either all or only the accounts belonging to the specified domain.

`-modify {User@Domain | Domain\User} [Password]`

Changes the password for a configured user account. `Omniinetpasswd` prompts for the password if not specified in the command line.

`-clean Domain`

Removes all operating system user accounts from the local Inet configuration.

`-inst_srv_user {User@Domain | Domain\User}`

Sets the specified user in the local Inet configuration to be used by the Installation Server during remote installation.

This option can only be used on Windows Server 2008 systems.

`-no_inst_srv_user {User@Domain | Domain\User}`

Marks the specified user in the local Inet configuration not to be used by the Installation Server during remote installation.

This option can only be used on Windows Server 2008 systems.

NOTES

The `omniinetpasswd` command is available on Windows Vista and Windows Server 2008 systems only.

EXAMPLES

1. To remove the user "User1" from the Inet configuration, run:
`omniinetpasswd -delete CompanyDomain\User1`
2. To delete all operating system accounts from the local Inet configuration, run:
`omniinetpasswd -clean`
3. To set the user "User1" from the domain "CompanyDomain" to be used by Installation Server, run:

```
omniinetpasswd -inst_srv_user User1@CompanyDomain
```


omniinstlic

starts the HP AutoPass utility or synchronizes the Data Protector licenses between Data Protector and HP AutoPass
(this command is available on the Data Protector Cell Manager)

omniinstlic

SYNOPSIS

```
omniinstlic -version | -help  
omniinstlic [-sync]
```

DESCRIPTION

If the command is run without options, the licensing data in HP AutoPass is synchronized with the licensing data in Data Protector, and then the HP AutoPass utility is started. If the `-sync` option is used, it only synchronizes the Data Protector licenses between Data Protector and HP AutoPass, the HP AutoPass utility is not started.

The HP AutoPass utility lets you install passwords for your HP products' purchased licenses directly from the internet. Refer to the HP AutoPass online Help for more information on the HP AutoPass utility.

OPTIONS

`-version`

Displays the version of the `omniinstlic` command.

`-help`

Displays the usage synopsis for the `omniinstlic` command.

`-sync`

Synchronizes the Data Protector licenses between Data Protector and HP AutoPass.

NOTES

In a Manager-of-Managers (MoM) environment, the `omniinstlic` command must be run on the MoM system (if Data Protector centralized licensing is used), or on the Cell Manager for which the passwords are being ordered and installed (if Data Protector centralized licensing is not used). The HP AutoPass utility must be installed on the system.

EXAMPLE

To start the HP AutoPass utility, run:

```
omniinstlic
```

SEE ALSO

omnicc(1), omnicellinfo(1), omnicheck(1M), omnidlc(1M), omnisv(1M)

omniintconfig.pl

configures, updates configuration parameters, and checks the configuration of one or multiple Oracle databases

(this command is available on systems with the Data Protector User Interface component installed)

omniintconfig.pl

SYNOPSIS

```
omniintconfig.pl -version | -help
```

```
omniintconfig.pl [-encode] [-chkconf] [-force]
```

```
{-passwordfile FileName | Param=Value [Param=Value...]}
```

Param

MoM

CellManager

Client

Instance

OSUSER

OSGROUP

TGTUser

TGTPasswd

TGTService

RCUser

RCPasswd

RCSservice

ORACLE_HOME

ClusterNodes

DESCRIPTION

Use the omniintconfig.pl command to configure, update configuration parameters, and check the configuration of one or multiple Oracle databases at the same time.

OPTIONS

-version

Displays the version of the omniintconfig.pl command.

-help

Displays the usage synopsis for the `omniintconfig.pl` command.

-encode

Encodes passwords before they are saved to Data Protector Oracle database specific configuration files. Omit this option if the provided passwords are already encoded.

-chkconf

Performs a configuration check for specified Oracle databases. Provided parameter values are saved to corresponding Data Protector Oracle database configuration files, regardless of whether the check succeeds or not. By default, the session ends if a configuration check for a database fails. However, if you specify the `-force` option, Data Protector continues configuring other Oracle databases.

-passwordfile *FileName*

Specifies that configuration parameters should be read from a file. The file must be in XLS or CSV file format.

Alternatively, parameters can be specified at run time, however, only for one Oracle database at a time. See the parameters description below.

PARAMETERS

MoM

Manager of Managers (optional).

CellManager

Data Protector Cell Manager. Default: Cell Manager of the local client.

Client

Client with Oracle Server installed. In cluster environments, specify the virtual server or, in RAC, one of the cluster nodes. Default: local client.

Instance

Oracle database name (mandatory).

OSUSER, OSGROUP (applicable for UNIX clients)

UNIX user account under which you want the configuration and browsing of Oracle databases to start. This user will be automatically added to the Data Protector admin user group for the client specified in `Client`.

TGTUser, TGTPasswd

Login information for the target database (username and password).

TGTService

Target database service(s). If there is more than one service, separate them with a semicolon (service1;service2...).

RCUser, RCPasswd

Login information for the recovery catalog database (username and password).

RCSERVICE

Recovery catalog database service.

ORACLE_HOME

Oracle Server home directory.

ClusterNodes

Cluster nodes (applicable in cluster environments). The user OSUSER, OSGROUP will be automatically added to the Data Protector admin user group for each cluster node listed here. Separate cluster nodes with a semicolon (node1;node2...).

If you do not specify this parameter, you need to add these users manually.

EXAMPLES

1. Suppose the file "C:\My_documents\Oracle_instances.csv" contains configuration parameters for the Oracle databases "IN1" and "IN2". The passwords in the file are encoded.

To configure the Oracle databases "IN1" and "IN2" using the file "C:\My_documents\Oracle_instances.csv", log in to the Windows client on which the file is saved and run:

```
perl.exe omniintconfig.pl -passwordfile  
C:\My_documents\Oracle_instances.csv
```

2. Suppose you are logged in to a UNIX client. To configure the Oracle database "IN2" by specifying parameters at run time, run:

```
omniintconfig.pl -encode CellManager=galaxy Client=star  
Instance=IN2 ORACLE_HOME=C:\oracle\product\10.2.0\db_1  
TGTUser=system TGTPasswd=BlueMoon TGTSERVICE=IN2_1;IN2_2
```

Note that the password "BlueMoon" is not encoded. Therefore, you must specify the "-encode" option.

3. Suppose you are logged in to a Windows client. To configure and check the configuration of all Oracle databases specified in "C:\My_documents\Oracle_instances.xls", run:

```
perl.exe omniintconfig.pl -chkconf -force -passwordfile  
C:\My_documents\Oracle_instances.xls
```

4. Suppose you are logged in to a UNIX client. To check the configuration of the Oracle database "IN2", run:

```
omniintconfig.pl -chkconf CellManager=galaxy Client=star  
Instance=IN2
```

SEE ALSO

omnicreatedl(1), util_cmd(1M), util_oracle8.pl(1M), util_vmware.exe(1M)

omnikeymigrate

helps you migrate your existing keystore file from the Data Protector A.06.00 client system and imports it into the central keystore file on the Data Protector A.06.11 Cell Manager

(this command is available on the Data Protector Cell Manager)

omnikeymigrate

SYNOPSIS

```
omnikeymigrate -version | -help
omnikeymigrate -client ClientName [-file KeyStoreFile]
omnikeymigrate -datalist ClientName
```

DESCRIPTION

The `omnikeymigrate` command helps you migrate your existing keystore file from the Data Protector A.06.00 client system and imports it into the central keystore file on the Data Protector A.06.11 Cell Manager. After the import, all migrated keys are inactive. The `-encode` option for the specified client system is also transformed into the `-encode aes256` option in all migrated backup specifications.

This command is usually invoked automatically during an upgrade of the client system, if needed it can also be used by the administrator.

OPTIONS

`-version`

Displays the version of the `omnikeymigrate` command.

`-help`

Displays the usage synopsis for the `omnikeymigrate` command.

`-client ClientName`

Migrates all encryption keys from the specified client system. Note that the client systems as well as the Cell Manager should be upgraded from earlier versions of the product to the Data Protector A.06.11 prior to running the command.

If an active encryption key is migrated from the specified client system, all backup specifications that are associated with this client system are automatically migrated with the key.

`-file KeyStoreFile`

Migrates only the specified keystore file. Note that after using this option, you need to run the `omnikeytool -activate EntityName -keyid KeyID StoreID` command to activate the encryption key from Data Protector A.06.00.

`-datalist ClientName`

Migrates all encoded backup specifications from the specified client system and enables the AES encryption.

EXAMPLE

To migrate all encryption keys and activate the active backup key for the client system "antares", run:

```
omnikeymigrate -client antares
```

SEE ALSO

`omnib(1)`, `omnikeytool (1M)`, `omniobjconsolidate(1)`, `omniobjcopy(1)`, `omniobjverify(1)`, `omnir(1)`

omnikeytool

manages keys used for encryption
(this command is available on the Data Protector Cell Manager)

omnikeytool

SYNOPSIS

```
omnikeytool -version | -help
omnikeytool -create EntityName [-description Description]
omnikeytool -activate EntityName -keyid KeyID StoreID
omnikeytool -deactivate EntityName
omnikeytool -export CSVFile ExportOptions
omnikeytool -import CSVFile
omnikeytool -modify -keyid KeyID StoreID -description Description
omnikeytool -list [-active | -unused]
omnikeytool -delete -keyid KeyID StoreID

ExportOptions

-keyid KeyID StoreID
-active
-entity EntityName
-time Day Hour Day Hour
-all

Date= [YY]YY/MM/DD (1969 < [YY]YY < 2038)
Hour= HH:MM
```

DESCRIPTION

The `omnikeytool` command manages keys used for encryption. You must create the key using the `omnikeytool` command prior to performing an encrypted backup.

OPTIONS

`-version`
Displays the version of the `omnikeytool` command.

`-help`
Displays the usage synopsis for the `omnikeytool` command.

`-create EntityName [-description Description]`
 Creates a new encryption key for the specified *EntityName*.
EntityName is a *ClientName* for the specified filesystem, rawdisk, or the IDB, an *AppType:DatabaseID* or *AppType:ClientName:AppName* for the specified application integration, and a *MediumID* if you use drive-based encryption.
 If the `-description` option is specified, you can provide a description string for the new encryption key.

`-activate EntityName -keyid KeyID StoreID`
 Associates the specified encryption key with the specified entity name string and activates the key.

`-deactivate EntityName`
 Disassociates the specified entity name string from the current active backup encryption key.

`-export CSVFile ExportOptions`
 Exports encryption key records into the specified comma separated values (CSV) file. The file is exported only to the directory
Data_Protector_program_data\Config\Server\export\keys (Windows Server 2008),
Data_Protector_home\Config\Server\export\keys (other Windows systems), or */var/opt/omni/server/export/keys* (UNIX systems).
 Exporting does not delete encryption keys from the keystore.

`-import CSVFile`
 Imports encryption key record matching the key number from the specified keystore file. The file is imported to the directory
Data_Protector_program_data\Config\Server\import\keys (Windows Server 2008),
Data_Protector_home\Config\Server\import\keys (other Windows systems), or */var/opt/omni/server/import/keys* (UNIX systems).

`-modify [-description Description]`
 Modifies the description for the specified encryption key.

`-list [-active |-unused]`
 Lists encryption keys related information from the cell.
 The command lists the following information for each encryption key in the keystore file: key status (active, inactive, migrated), key ID, date and time of creation, type of encryption, and the key description. For greater scrutiny, the above-mentioned information is listed for each client in the cell separately.

If the `-active` option is specified, the command just lists currently active keys and the entity names associated with them.

If the `-unused` option is specified, the command lists all encryption keys which are present in the keystore file on the Cell Manager, but have never been used for encryption.

`-delete`

Deletes the record of an inactive encryption key identified by key ID.

Ensure that the key you intend to delete is not in use. If the encryption key is not available, restore of encrypted data is not possible.

ExportOptions

`-keyid KeyID StoreID`

Exports all encryption key records with the specified key ID.

`-active`

Exports all currently active encryption keys.

`-entity EntityName`

Exports only the active key record identified by the *EntityName* string.

`-time Day Hour Day Hour`

Exports all encryption key records in the specified time frame.

`-all`

Exports all encryption key records.

EXAMPLES

1. To activate the encryption key "10B536738F8831478408000000000000 5B9381955B9381955B9381955B938195" for the client system "proxima", run:

```
omnikeytool -activate proxima -keyid
10B536738F8831478408000000000000
5B9381955B9381955B9381955B938195
```

2. To deactivate an encryption key for the client system "stella", run:

```
omnikeytool -deactivate stella
```

3. To modify your description of the encryption key "10B53673B8232747A806000001000000 5B9381955B9381955B9381955B938987", run:

```
omnikeytool -modify -keyid 10B53673B8232747A806000001000000
5B9381955B9381955B9381955B938987 -description key_number_1
```

4. To export the active encryption key "10B53673B8232747A8060000010000005B9381955B 9381955B9381955B938321" to a comma-separated values (CSV) file "a.csv", run:

```
omnikeytool -export a.csv -keyid  
10B53673B8232747A806000001000000 5B9381955B  
9381955B9381955B938321
```

5. To list all encryption keys which are present in the keystore file on the Cell Manager, but have never been used for encryption, run:

```
omnikeytool -list -unused
```

SEE ALSO

omnib(1), omnikeymigrate(1M), omniobjconsolidate(1), omniobjcopy(1), omniobjverify(1), omnir(1)

omnimigrate.pl

helps you migrate your existing Cell Manager from a PA-RISC architecture based HP-UX 11.x system to an HP-UX 11.23 system for the Intel Itanium 2 (IA-64) architecture

(this command is available on the Data Protector Cell Manager)

omnimigrate.pl

SYNOPSIS

```
omnimigrate.pl -help
omnimigrate.pl -prepare_clients New_CM_ClientName
omnimigrate.pl -configure
omnimigrate.pl [-configure_clients] [-configure_idb] [-configure_cm]
```

DESCRIPTION

omnimigrate.pl helps you migrate your existing Cell Manager from a PA-RISC architecture based HP-UX 11.x system to an HP-UX 11.23 system for the Intel Itanium 2 (IA-64) architecture.

First, you need to run omnimigrate.pl on the old Cell Manager and back up the IDB. Then install Disk Agent to the HP-UX 11.23 system (your new Cell Manager) and restore your IDB to the new Cell Manager. Uninstall the Disk Agent from the new Cell Manager and install Data Protector A.06.11 Cell Manager. Finally run the omnimigrate.pl command again on the new Cell Manager.

OPTIONS

-help

Displays the usage synopsis for the omnimigrate.pl command.

-prepare_clients *New_CM_ClientName*

Adds the new Cell Manager's client name to the list of trusted hosts on secured clients. Secured clients accept requests on the Data Protector port (by default 5555) only from trusted hosts.

This option should be used only on the *old* Cell Manager.

-configure_clients

Migrates the clients from the old Cell Manager to the new Cell Manager. The old Cell Manager will keep the clients in the configuration files although it will not be their Cell Manager anymore.

If any of the clients is inaccessible, it will not be imported to the new cell. You can re-run the `omnimigrate.pl` command with this option when the clients are accessible to migrate them to the new Cell Manager.

The old Cell Manager will automatically become a client in the new cell. You can uninstall the Cell Manager component from the old Cell Manager, because it is not necessary anymore.

The option should be used only on the *new* Cell Manager.

`-configure_idb`

Configures the IDB from the old Cell Manager for use on the new Cell Manager.

The option should be used only on the *new* Cell Manager.

`-configure_cm`

Reconfigures the configuration data transferred from the old Cell Manager for use on the new Cell Manager.

The option should be used only on the *new* Cell Manager.

`-configure`

Combines `-configure_clients`, `-configure_idb`, and `-configure_cm` options. This is the recommended way to run the `omnimigrate.pl` command.

The option should be used only on the *new* Cell Manager.

RETURN VALUES

0 Successfully finished.

1-4 An error occurred.

ERRORS

1 A generic error occurred.

2 Migration of IDB catalogs failed.

3 Configuration error (Cell Manager configuration error or an error during the import of clients) occurred.

NOTES

The `omnimigrate.pl` command is available on HP-UX systems only.

EXAMPLES

1. Run the following command on the old Cell Manager to add the new Cell Manager with the client name "dfg.company.com" to the list of trusted hosts on secured clients:

```
omnimigrate.pl -prepare_clients dfg.company.com
```

2. To migrate the IDB, reconfigure the Cell Manager's settings, export all clients from the old Data Protector cell and import them to the new cell, run the following command on the new Cell Manager:

```
omnimigrate.pl -configure
```

SEE ALSO

`ob2install(1M)`, `omnigui(5)`, `omniintro(9)`, `omnisetup.sh(1M)`, `omniusers(1)`, `upgrade_cm_from_evaa(1M)`, `winomnimigrate.pl(1M)`

omniofflr

enables restore of any type of Data Protector backup object in the absence of a working Data Protector internal database (IDB)
(this command is available on systems with the Data Protector User Interface component installed)

omniofflr

SYNOPSIS

```
omniofflr -version | -help
omniofflr DeviceOptions MediaOptions1 [MediaOptions2 ...] Object-
Options1 [ObjectOptions2 ...] [GeneralOptions]

DeviceOptions
-name DeviceName
-dev PhysicalDevice1 [PhysicalDevice2 ...]
-mahost DeviceHostName
-policy LogicalDevicePolicy
-type LogicalDeviceType
[-description DeviceDescription]
[-blksize BlockSize]

MediaOptions
-maid MediumID1 [MediumID2 ...]
[-slot slot1[:flip] [slot2[:flip] ...]]
[-position segment1:offset1 [segment2:offset2 ...]]

ObjectOptions
{-filesystem | -winfs | -omnidb} Client:MountPoint Label
-dauid DAUID
[-merge]
[-[no_]overwrite]
[-move_busy]
[-omit[_deleted_files]]
[-var OptName OptValue]
-tree TreeName1 [TreeOptions1] [-tree TreeName2 [TreeOptions2...]]

TreeOptions
-exclude TreeName1 [TreeName2...] {-as | -into} NewTreeName

GeneralOptions
```

```
-verbose
-preview
-report
-target TargetHostName
-[no]ok[mediumlist]
```

DESCRIPTION

The `omniofflr` command can be used as a standalone utility or - on Windows systems - by a higher level utility `omnidr`, which automatically generates restore object command line options for the `omniofflr` command, based on the SRD file information.

The `omniofflr` command enables the restore of any type of backup object in the absence of the Data Protector internal database (IDB) (due to a disaster or lost connection to the Cell Manager).

Running the `omniofflr` command requires detailed information about the restore device and backup media, including positions of backup objects on the media. Media information can be obtained from the SRD file on the Cell Manager located in the directory `Data_Protector_program_data\Config\Server\dr\srd` (Windows Server 2008), `Data_Protector_home\Config\Server\dr\srd` (other Windows systems), or `/etc/opt/omni/server/dr/srd` (UNIX systems), or you can provide the information manually. To obtain this information, query the IDB using the `omnidb` command after the backup and write down the results. It is also possible to write a script, which queries the IDB and generates another script in which the `omniofflr` command with the proper options is executed.

OPTIONS

```
-version
    Displays the version of the omniofflr command.
-help
    Displays the usage synopsis for the omniofflr command.
```

DeviceOptions

```
-name LogicalDeviceName
    Parameter that specifies the logical device name.
-dev PhysicalDevice
    Specifies the pathname of the device file. For example: c:\temp\dev1,  
scsi1:0:0:0, /dev/tape0...
```

`-mahost DeviceHostName`

Specifies the name of the client, where the restore device is attached and a Media Agent started.

`-policy LogicalDevicePolicy`

Specifies the policy ID for the device specified by the `-dev` option. Policy can be defined as:

- 1 (Standalone),
- 3 (Stacker)
- 5 (6300 MO jukebox)
- 6 (Exchange through cmd execution)
- 8 (GRAU DAS exchanger library)
- 9 (Silo medium library)
- 10 (SCSI exchanger)
- 11 (RSM exchanger)

`-type LogicalDeviceType`

Specifies the media type for the media in the device specified by the `-device` option. Media type numbers are defined in the *HP Data Protector product announcements, software notes, and references*.

`-description DeviceDescription`

This is an optional parameter that specifies the logical device description.

`-blksize BlockSize`

This is an optional parameter that specifies the block size the device is going to use when accessing media.

MediaOptions

`-maid MediumID`

Specifies the medium identification number of the medium that contains the object data; for example `8c04110a:3b0e118b:041c:0001`. If `unknown` is specified, each medium will be accepted as valid and restore will be attempted. Whole medium will be scanned for the requested object and it may take a very long time, if the object is not on the medium. Mount prompt in such case will request the next medium, without specifying the medium label.

`-slot slot1[:flip]`

Specifies the slot identifier of the slot, where the required media is located, thus enabling Data Protector to automatically load media from the exchanger slots. Note that the sequence has to match the sequence in the list created using the `-maid` option.

`-position segment1:offset1`

Specifies the segment and offset position of the restore object data on the medium; for example 67:20. If the position is not specified, the position 1:0 is assumed, thus prolonging the restore time. Note that the sequence has to match the sequence in the list created using the `-maid` option.

ObjectOptions

`-filesystem Client:MountPoint Label`

Selects the filesystem identified with *Client:MountPoint Label* for restore. Client determines the name of the system where the object was backed up.

MountPoint specifies the mount point name of the volume to be restored (for example /C, /tmp, /, etc.). It must be in the same format as stored in the IDB. *Label* specifies the backup/restore objects description that uniquely defines an object (`-filesystem computer.domain.net:/mount label`)

`-winfs Client:MountPoint Label`

Selects the Windows filesystem identified with *Client:MountPoint Label* for restore. Client determines the name of the system where the object was backed up. *MountPoint* specifies the mount point name of the volume to be restored (for example /C, /tmp, /, etc.). It must be in the same format as stored in the IDB. Therefore, for example, on Windows systems C: translates into /C. *Label* specifies the backup/restore object's description that uniquely defines an object (`-winfs computer.domain.net:/C: etc.`)

`-omnidb Client:MountPoint Label`

Selects the files from the IDB identified with *Client:MountPoint Label* for restore. Client determines the name of the system where the object is to be restored. *MountPoint* for IDB is always /. *Label* specifies the backup/restore object's description that uniquely defines an object (`-omnidb computer.domain.net:/C: etc.`).

`-daid DAID`

Specifies the disk agent identification number of the disk agent that backed up an object.

`-merge`

This option merges files from the backup medium to the target directory and replaces older versions that exist in the directory with newer (if they exist on the medium) files. Existing files are overwritten if the version on the medium is newer than the version on disk. No existing directory is deleted. If a directory or file doesn't exist on disk (but is on the backup medium) it is restored (created).

`-overwrite`

By default, or if the `-overwrite` option is specified, the already existent files on the disk are overwritten by the restored files.

`-no_overwrite`

If the `-no_overwrite` option is specified, only the files that do not exist on the disk are restored.

`-move_busy`

This option is used with the `-omit_deleted_files` or `-overwrite` option. A problem can occur if, for example, a file to be overwritten cannot be deleted because it is currently in use. If this option is specified, Data Protector moves busy file *filename* to *#filename* on UNIX systems (adding a hash- mark in front of the filename), or to *filename.001* on Windows system. On UNIX systems the original file can thus be deleted as the lock is transferred to the corresponding file starting with the *#*sign. For example, */tmp/DIR1/DIR2/FILE* would be moved to */tmp/DIR1/DIR2/#FILE*. On Windows system the application only uses the newly-restored file after the file is restored and the system is rebooted.

`-omit_deleted_files`

This option can be only used in combination with the `-overwrite` option.

If this option is specified, Data Protector attempts to recreate the state of the restored directory tree as it was when the last incremental backup was run, while preserving files that were created or modified after the last incremental backup. However, if the directory contains files that did not exist there at the time of the last incremental backup, but their modification time is older than the time of the incremental backup, Data Protector will delete these files as well.

When this option is used in combination with the `-as` or `-into` option, be careful when specifying the new location to prevent accidental deletion of existing files.

If this option is not specified, when restoring a directory from which files were deleted between a full and an incremental backup, these files are also restored.

The time on the Cell Manager and clients must be synchronized for this option to function properly.

`-variable var_name var_value`

This option lets you specify a variable name and its value for proper operation of some platforms and integrations. Setting user definable variables (a variable name and its value) enables flexible operation on some platforms and integrations with Data Protector. The list of variables and their values that are configurable with Data Protector is dynamic and comes with Data Protector patches.

`-tree TreeName [TreeOptions]`

Specifies the starting root directory of data restore. Note that this starting directory is also restored.

TreeOptions

`-exclude TreeName`

Specifies trees excluded from the restore.

`-as NewTreeName`

This is an optional parameter that restores the selected fileset as the specified tree. This parameter is of vital importance for the Disk Delivery disaster recovery, since without it the restore to the original location would be performed.

`-into NewTreeName`

This is an optional parameter that restores the selected fileset into the given directory. This parameter is of vital importance for the Disk Delivery disaster recovery, since without it the restore to the original location would be performed.

GeneralOptions

`-verbose`

Specifies the verbose level of progress reporting.

`-preview`

Specifies that the preview mode of the restore is entered.

`-report`

Displays a report of the disaster recovery using the `omniofflr` command.

`-target`

Specifies the target system name which is different than the original.

`-[no]ok[mediumlist]`

By default the options are parsed and displayed so that the user can check them and confirm the start of restore. This means that the `omniofflr` command used from a script could not be executed because it would wait for the confirmation before starting the restore. This option has to be used to skip confirmation, thus enabling the execution of the `omniofflr` command from a script.

NOTES

The `omniofflr` command is available on Windows systems only.

The `omniofflr` command does not support robotic media loaders. The user must ensure that appropriate media is loaded into specified drives. This can be done using the `uma` agent on the system to which robotics is connected.

EXAMPLES

The following example illustrates how the `omniofflr` command works.

To restore the "c:/temp" directory of the computer "computer.company.com" without the "c:/temp/vnc" directory, which was backed up using an HP Ultrium standalone device on a STK Ultrium drive medium, attached to the Cell Manager "cm.company.com", into the "c:/test/temp directory", run:

```
omniofflr -verbose -name HP:Ultrium -dev scsi2:0:4:0C -mahost  
cm.company.com -policy 1 -type 13 -maid  
9e03110a:3b5ee669:05ac:0001 -computer.company.com:/C C: -daid  
996144004 -tree /temp -exclude /temp/vnc -into c:/test/temp
```

To get the logical device name and its SCSI address, run:

```
devbra -dev
```

The output of the command looks something like this:

```
HP:Ultriumscsi2:0:4:0cLTO : HP LTO drive
```

"HP:Ultrium" is the logical device name of the backup device while "scsi2:0:4:0c" specifies the SCSI address of the device.

To obtain the medium ID (MAID), run the `omnidb` command with the appropriate backup session ID:

```
omnidb -session 2007/09/06-1 -media
```

To obtain all backup session IDs for the winfs computer.domain.com:/C computer.domain.com [/C], run:

```
omnidb -winfs computer.domain.com:/C "computer.domain.com  
[/C]"
```

To obtain the Disk Agent ID (DAID) and the object name, run the `omnimmm` command with the relative MAID:

```
omnimmm -catalog 9e03110a:3b5ee669:05ac:0001
```

SEE ALSO

`omnidr(1M)`, `omniiso(1)`, `omnisrupdate(1M)`

omniresolve

resolves a filesystem object or a list of filesystem objects and writes the results to the standard output or to a Unicode file
(this command is available on systems with any Data Protector integration component installed)

omniresolve

SYNOPSIS

```
omniresolve -version | -help  
omniresolve {-files filename [filename2 ...] | -inputfile datafile}  
[-verbose] [-unicodefile outfile]
```

DESCRIPTION

The `omniresolve` command reads the filesystem structures locating the physical disks (on Windows) or volumes (on UNIX) on which a filesystem object resides. If the files reside on a logical volume which is a part of a volume group (disk group), all volumes in a volume group are displayed.

You can list the filesystem objects to be resolved either in the CLI (on UNIX and Windows systems) or using a Unicode file (on Windows systems only). The results are written to standard output (on UNIX and Windows systems) or to a Unicode file (on Windows systems only).

OPTIONS

`-version`

Displays the version of the `omniresolve` command.

`-help`

Displays the usage synopsis for the `omniresolve` command.

`-files filename [filename2 ...]`

Resolves a list of files separated by spaces and writes the results to the standard output.

`-inputfile datafile`

Resolves all objects listed in *datafile* in and writes the results to the standard output.

Note that on Windows systems, if *datafile* is in the Unicode format, the output is by default written to the file `uniout.dat`. You can redirect the output to a different file by using the `-unicode` option.

`-verbose`

Provides a more detailed report (displaying details such as WWNs, LUNs, or LDEVs) using SCSI inquiry on physical disks.

`-unicodefile outfile`

Defines the file to which the output is redirected if the input file is a Unicode file.

NOTES

The resolve process requires root permissions on UNIX systems to get access to the disk device files. Therefore, the SUID flag is set on for `omniresolve`.

EXAMPLE

To resolve a list of three files ("system01.dbf", "redo01.log", and "control01.ctl") located in "/opt/oracle9i/oradata/dbname", run:

```
omniresolve -f '/opt/oracle9i/oradata/dbname/system01.dbf'
'/opt/oracle9i/oradata/dbname/redo01.log'
'/opt/oracle9i/oradata/dbname/control01.ctl' -v
```

omnirsh

returns the hostnames of the physical and virtual nodes for the specified cluster hostname, or returns the cell information stored in the cell_info file on the specified cluster

(this command is available on the Data Protector Cell Manager)

omnirsh

SYNOPSIS

omnirsh -version | -help

omnirsh *cluster_hostname* {INFO_CLUS | INFO}

DESCRIPTION

The `omnirsh` command returns the hostnames of the physical and virtual nodes for the specified cluster hostname, together with the flag indicating whether a specific node is a physical node or virtual node. The command can also be used to list the contents of the cluster `cell_info` file, residing on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\cell` (Windows Server 2008), `Data_Protector_home\Config\Server\cell` (other Windows systems), or `/etc/opt/omni/server/cell` (UNIX systems).

OPTIONS

-version

Displays the version of the `omnirsh` command.

-help

Displays the usage synopsis for the `omnirsh` command.

cluster_hostname

Sets the hostname of the cluster for this command.

INFO_CLUS

Lists the hostnames of the physical and virtual nodes for the specified cluster hostname, together with the flag indicating whether a specific node is a physical node or virtual node. Flag value 1 indicates a physical node, whereas flag value 8 indicates a virtual node.

INFO

Displays the contents of the `cell_info` file for the system specified by the *cluster_hostname* parameter. The `cell_info` file resides on the Cell

Manager in the directory

Data_Protector_program_data\Config\Server\cell (Windows Server 2008), *Data_Protector_home*\Config\Server\cell (other Windows systems), or */etc/opt/omni/server/cell* (UNIX systems).

SEE ALSO

omniclus(1M)

omnisetup.sh

installs or upgrades a Data Protector UNIX Cell Manager, Installation Server, or client system locally
(this command is available on the Data Protector installation DVD-ROMs for UNIX systems)

omnisetup.sh

SYNOPSIS

```
omnisetup.sh -version | -help
omnisetup.sh [-source directory] [-server name] [-install Component_list] [-CM] [-IS] [-autopass]
Component_list
cc = User Interface
javagui = Java GUI Client
da = Disk Agent
ndmp = NDMP Media Agent
ma = General Media Agent
sap = SAP R/3 Integration
sapdb = SAP DB Integration
emc = EMC Symmetrix Agent
oracle = Oracle Integration
sybase = Sybase Integration
ssea = HP StorageWorks XP Agent
snapa = HP StorageWorks VA Agent
informix = Informix Integration
ov = HP Network Node Manager Integration
lotus = Lotus Integration
db2 = DB2 Integration
smisa = HP StorageWorks EVA SMI-S Agent
vls_am = VLS Automigration
vmware = VMware Integration
docs = English Documentation & Help
jpn_ls = Japanese Documentation & Help
fra_ls = French Documentation & Help
```

DESCRIPTION

The command first checks if Data Protector is already installed on the system.

NEW INSTALLATION OR RE-INSTALLATION OF THE SAME VERSION OF DATA PROTECTOR

If Data Protector is not installed, then the command, depending on the selected options, installs the Cell Manager, Installation Server, or every Data Protector software component specified with the `-install` option. If none of these options are specified, the command issues a prompt for every Data Protector software component supported on the current system OS. Using this prompt, software components supported on the current system OS can be confirmed or rejected for installation, or the execution of the command can be canceled. There is no such prompt if the `-install` option is specified.

UPGRADE FROM AN EARLIER VERSION OF DATA PROTECTOR

To upgrade your cell from the earlier versions of the product to Data Protector A.06.11, proceed as follows:

- Upgrade the Cell Manager
- Upgrade the Installation Server
- Upgrade the clients

To upgrade the all Data Protector components on the system, run `omnisetup.sh` without options. If the Installation Server is installed together with the Cell Manager, or if it is installed without client components, it is upgraded automatically during the Cell Manager upgrade.

If the Installation Server is installed with the client components, it is removed during the Cell Manager upgrade. In this case, a new Installation Server must be installed using the `-IS` option, after the upgrade finishes.

To add a client to the Cell Manager, specify the `-install` option. If the client not residing on the Cell Manager is to be upgraded, the `-install` option does not need to be specified. In this case, the setup selects the same components as were installed on the system before the upgrade without issuing a prompt.

In all cases (new installation, re-installation or upgrade), the following applies when using this command:

- When using the `-install` option, the software components not supported on the current system OS and mistyped software components are skipped.
- On the Cell Manager only, when the installation or upgrade is started, you are prompted to install the HP AutoPass utility (unless the `-autopass` option is specified — if it is, the HP AutoPass utility is installed or upgraded without issuing a prompt). If AutoPass is already installed on the system, it is automatically upgraded, if the prompt is confirmed. When Data Protector is uninstalled from

the system, the HP AutoPass utility is neither unregistered nor uninstalled. It must be uninstalled using UNIX utilities, for example `sd`.

If the HP AutoPass utility is installed in a cluster environment, it must be installed on every node in the cluster.

- After the client (re-)installation or upgrade is finished, the system is imported to a Data Protector cell if the `-server` option was set, or if the `/etc/opt/omni/client/cell_server` (HP-UX, Solaris, and Linux clients) or the `/usr/omni/config/cell/cell_server` (other UNIX clients) file exists on the system.
- The first time any software component is selected for installation or reinstallation, the `core` component is automatically installed (or reinstalled). Similarly, the first time any integration software component is selected for installation or reinstallation, the `core-integ` component is automatically installed (or reinstalled).

OPTIONS

`-version`

Displays the version of the `omnisetup.sh` command.

`-help`

Displays the usage synopsis for the `omnisetup.sh` command.

`-source directory`

Sets the location of the Data Protector installation files (DVD-ROM mountpoint). If this option is not specified, the current directory is set as the location of Data Protector installation files.

`-server name`

Sets the hostname of the Cell Manager of the cell to which the installed or upgraded client is to be imported after the installation or upgrade. If this option is not specified, and the `/etc/opt/omni/client/cell_server` (HP-UX, Solaris, and Linux clients) or the `/usr/omni/config/cell_server` (other UNIX clients) file does not exist on the system, the installed or upgraded client is not imported to any cell and has to be imported manually.

`-install Component_list`

Sets Data Protector software components that you want to install or upgrade on the current system. If more than one software component is to be installed or upgraded, a listing of software components, delimited by comma (without spaces) must be entered as the argument. If this option is not specified (except for the case when the client not residing on the Cell Manager needs to be upgraded), the command issues a prompt for every Data Protector software component supported on the current system OS; prompting whether to install or upgrade

certain Data Protector software component or not. If the client is to be upgraded, this option does not need to be specified. In this case, the setup selects the same components as were installed on the system before the upgrade without issuing a prompt.

-CM

Installs/upgrades the Data Protector Cell Manager.

-IS

Installs/upgrades the Data Protector Installation Server with *all* push packages. Note that the Installation Server can be upgraded only after the Cell Manager in the Data Protector cell is upgraded.

-autopass

If this option is specified, the HP AutoPass utility is automatically installed. If AutoPass is already installed on the system, it is automatically upgraded. This option is to be used only on the Cell Manager.

Note that AutoPass is not available on Linux.

NOTES

This command requires that the

- Data Protector UNIX installation DVD is mounted on the system.
- `DP_DEPOT` and `LOCAL_INSTALL` folders are copied to the disk.

Before running the command make sure that no Data Protector backups or restores are running on the system. The command must be executed using the default POSIX `ksh` or `pdksh` (on Linux) shell.

On MC/ServiceGuard, the HP AutoPass utility must be installed on all nodes.

EXAMPLES

1. To upgrade a system, run:
`omnisetup.sh`
2. To install or re-install the General Media Agent, Disk Agent, SMIS-A and SAP R/3 software components, run:
`omnisetup.sh -install ma,da,smisa,sap`
3. To install the Cell Manager and Installation Server together with the HP AutoPass utility, insert and mount the UNIX installation DVD and run the following command from the `LOCAL_INSTALL` directory:

```
omnisetup.sh -CM -IS -autopass
```

SEE ALSO

ob2install(1M), omnigui(5), omniintro(9), omnimigrate.pl(1M), omniusers(1),
upgrade_cm_from_evaa(1M), winomnimigrate.pl(1M)

omnisrdupdate

updates the System Recovery Data (SRD) file
(this command is available on systems with the Data Protector User Interface component installed)

omnisrdupdate

SYNOPSIS

```
omnisrdupdate -version | -help
omnisrdupdate [-session sessionID] [-cell name]
[-host ClientName] [-location path1 [-location path2 ...]]
[-asr]
```

DESCRIPTION

The `omnisrdupdate` command is used to update System Recovery Data (SRD). An SRD file, which is a text file in the Unicode (UTF-16) format, is generated during CONFIGURATION backup of a Windows system, and saved to the Cell Manager to the directory `Data_Protector_program_data\Config\Server\dr\srd` (Windows Server 2008), `Data_Protector_home\Config\Server\dr\srd` (other Windows systems), or `/etc/opt/omni/server/dr/srd/` (UNIX systems).

The SRD filename is identical to the hostname of the system where it was generated, for example `computer.company.com`. After the CONFIGURATION backup, the SRD contains only the system information required for system configuration and installation of the operating system needed for disaster recovery. To be able to perform a disaster recovery without a working Data Protector internal database (IDB), additional information about backup objects and corresponding media must be added to the SRD by running this command. The name of the updated SRD file is `recovery.srd`.

OPTIONS

`-version`

Displays the version of the `omnisrdupdate` command.

`-help`

Displays the usage synopsis for the `omnisrdupdate` command.

`-session sessionID`

Specifies the session ID of the backup session with the backup object information which an existing SRD file will be updated with. This option must be specified when `omnisrdupdate` is run interactively, and must be omitted when `omnisrdupdate` is run from a post-exec script. In the latter case, Data Protector automatically obtains the required information from the current environment.

Updating the SRD file succeeds only when all critical backup objects (as specified in the SRD file) were actually backed up during the specified session. To view which objects are marked as critical for the SRD update, open the SRD file in a text editor. All critical objects for the SRD update are listed under the `-section objects` section. Note that the database is represented as `"/`.

`-cell name`

Specifies the Cell Manager to connect to in order to obtain the required information about backup objects and the corresponding media from the IDB.

If this option is omitted, Data Protector automatically obtains the required information from the current environment.

`-host ClientName`

Specifies the system for which the SRD file is to be updated.

If this option is omitted, Data Protector automatically obtains the required information from the current environment.

`-location path`

Specifies the location where the updated SRD file is saved. A local directory or a network share can be specified. To create several copies of the updated SRD file on different locations, use multiple `-location path` argument pairs. It is recommended that, in addition to the Cell Manager, the updated SRD file is copied to several safe storage locations as a part of disaster recovery preparation policy. For example, assuming that this storage location is considered safe, you can copy the updated SRD file to the directory

`Data_Protector_program_data\Config\Server\dr\srd` (Windows Server 2008), `Data_Protector_home\Config\Server\dr\srd` (other Windows systems), or `/etc/opt/omni/server/dr/srd/` (UNIX systems) on the Cell Manager.

When `omnisrdupdate` is run from a pre-exec or post-exec script, this option can be omitted. In this case, `omnisrdupdate` updates System Recovery Data internally in the Data Protector session, but does not save it to any SRD file. System Recovery Data updated in such a way can only be used for subsequent processing within the same session.

If you are running the `omnisrdupdate` command in a pre-exec or post-exec script, do not add a backslash at the end of the path.

`-asr`

If specified, the ASR archive file (a collection of files required for proper reconfiguration of the replacement disk packed in a single archive file) is downloaded from the Cell Manager and ASR files are extracted and stored to all destinations, specified by the `-location` option. At least one `-location` option must be specified otherwise the `-asr` option is ignored. If the ASR archive file on the Cell Manager does not exist, `omnisrdupdate` fails and the SRD file is not updated.

NOTES

The `omnisrdupdate` command is available on Windows systems only.

EXAMPLES

1. To update the SRD file with the backup object information belonging to the session "2008/03/02-5", run:

```
omnisrdupdate -session 2008/03/02-5
```

To obtain the session ID, execute the `omnidb` command with the option `-session`. To obtain the latest session ID, run:

```
omnidb -session -latest
```
2. To update the SRD file with the backup object information which belongs to the session "2008/03/02-5" and save the updated SRD file on a diskette as well as to the network share "srdfiles" on the system with the hostname "computer", run:

```
omnisrdupdate -session 2008/03/02-5 -location A: -location //computer/srdfiles
```
3. To update the first diskette from the ASR set with the backup object information and ASR files which belong to the session "2008/03/02-5", ensure the first diskette is not write-protected, insert it into the floppy disk drive, and run:

```
omnisrdupdate -session 2008/03/02-5 -location A: -asr
```

SEE ALSO

`omnidr(1M)`, `omniiso(1)`, `omniofflr(1M)`

omnistoreapputil

acts as a user interface to Storage Appliances, such as VLS
(this command is available on the Data Protector Cell Manager)

omnistoreapputil

SYNOPSIS

```
omnistoreapputil -version | -help
omnistoreapputil [-check_connection] -hostname HostName -port
PortNumber -user UserName -password Password -certificate_name
CertificateName -check_vls
omnistoreapputil [-download_certificate] -hostname HostName -port
PortNumber -user UserName -password Password -certificate_name
CertificateName
```

DESCRIPTION

The `omnistoreapputil` command is used as a user interface for the Storage Appliances, such as VLS. It is used to check the connection to the Storage Appliance.

The `omnistoreapputil` command is part of the Cell Manager package and can be installed on all Data Protector Cell Manager platforms.

OPTIONS

`-version`

Displays the version of the `omnistoreapputil` command.

`-help`

Displays the usage synopsis for the `omnistoreapputil` command.

`-check_connection`

Checks the connection between Data Protector and the Storage Appliance.

`-hostname HostName`

Specifies a name of a VLS client.

`-port PortNumber`

Sets the TCP/IP port number for the Storage Appliance.

`-user UserName`

Sets the username that is used by Data Protector to establish the connection to the Storage Appliance.

`-password Password`

Sets the password for the above specified username.

`-check_vls`

Specifies that the connection to the VLS Device needs to be checked.

`-client ClientHostNameorIPAddress`

Specifies the name or the IP address of the client imported into the Data Protector cell.

EXAMPLES

1. To check the connection to the VLS Device, run:

```
omnistoreapputil -check_connection -hostname  
client.company.com -port 5988 -user Admin -password ***  
-check_vls
```

SEE ALSO

`omnicc(1)`, `uma(1M)`

omnisv

starts, stops, or displays the status of Data Protector daemons (HP-UX, Solaris, or Linux systems) or services (Windows systems)
(this command is available on the Data Protector Cell Manager)

omnisv

SYNOPSIS

```
omnisv -version | -help  
omnisv {-start | -stop | -status | -start_mon}
```

DESCRIPTION

The `omnisv` command enables you to start or stop Data Protector services and display their status.

`Omnisv` can start or stop the RDS, CRS, UIProxy, KMS and MMD services on the Cell Manager. Note that the MMD service can only be started or stopped locally on the Cell Manager with the MMDB.

On the HP-UX or Solaris Cell Manager the `omnisv` command also adds the `omnitrig` process to the cron table and schedules it (the `omnitrig` command on the Windows Cell Manager is started by the CRS service). You can modify the scheduler granularity by changing the `SchedulerGranularity` global variable. By default, the granularity is 15 minutes, but it can be modified to 1 minute.

On the Windows Cell Manager `omnisv` also starts the `Inet` service (the Data Protector `Inet` program (`/opt/omni/lbin/inet`) is on the HP-UX or Solaris Cell Manager started by the system `inet` daemon when an application tries to connect to the Data Protector port, which is by default port number 5555. Normally, these daemons are started automatically during the system's startup).

Stopping of RDS service is logged down in the `RDS.log` located on the Cell Manager in the directory `Data_Protector_program_data\db40\datafiles\catalog` (Windows Server 2008), `Data_Protector_home\db40\datafiles\catalog` (other Windows systems), or `/var/opt/omni/server/log` (UNIX systems) with the `***SERVER SHUTDOWN INITIATED***` message. Each time the RDS service is started a new `RDS.log` is created and the previous `RDS.log` is renamed to `RDS.bak`.

OPTIONS

- version
Displays the version of the `omnisv` command.
- help
Displays the usage synopsis for the `omnisv` command.
- start
Starts the Data Protector services (on Windows) and adds the `omnitrig` command to the cron table, thus configuring it as a cron job (on UNIX).
- stop
Stops the services (on Windows) and removes the `omnitrig` command from the cron table (on UNIX).
- status
Displays the status and PID of the services.
- start_mon
Waits in loop until the `CRS`, `MMD`, `UIProxy`, `KMS` and `RDS` services are up and running. If any daemon or service stops, `omnisv` exits with an exit code 1. Exit code 0 means that all relevant Data Protector daemons/services are up and running, whereas the exit code 1 means that at least one of the relevant Data Protector daemons or services is not running.

NOTES

On Windows systems, only the users in the Data Protector admin group can execute this command. On HP-UX and Solaris systems, only the root user can execute this command. It is not possible to start or stop services on a cluster using this command.

SEE ALSO

`omnicc(1)`, `omnicellinfo(1)`, `omnicheck(1M)`, `omnidlc(1M)`, `omniinstlic(1M)`

omnitrig

triggers Data Protector scheduled backups
(this command is available on the Data Protector Cell Manager)

omnitrig

SYNOPSIS

```
omnitrig -version | -help
omnitrig [-start] [-log]
omnitrig -stop
omnitrig -run_checks
```

DESCRIPTION

The `omnitrig` command checks and triggers scheduled backups.

OPTIONS

`-version`

Displays the version of the `omnitrig` command

`-help`

Displays the usage synopsis for the `omnitrig` command

`-start`

Adds the `omnitrig` command to the cron table and schedules it. You can modify the scheduler granularity by changing the *SchedulerGranularity* global variable. By default, the granularity is 15 minutes, but it can be modified to 1 minute.

`-log`

If this option is specified then `omnitrig` will save information about each start of `omnitrig` command and backups started by `omnitrig` command into the file *Data_Protector_program_data\log\omnitrig.log* (Windows Server 2008), *Data_Protector_home\log\omnitrig.log* (other Windows systems), or */var/opt/omni/server/log/omnitrig.log* file (UNIX systems).

`-stop`

Removes the `omnitrig` command from the cron table.

`-run_checks`

Start checks for the following Data Protector notifications: IDB Space Low, IDB Tablespace Space Low, Not Enough Free Media, Health Check Failed, User Check Failed, Unexpected Events, License Warning, License Will Expire, and IDB Purge Needed.

By default, these checks are started automatically every day at 12:30 P.M. You can change the time of these checks or disable them by changing the *DailyCheckTime* option in the global options file.

SEE ALSO

`omnihealthcheck(1M)`, `omnirpt(1)`

sanconf

auto-configures a library, modifies an existing library or drive configuration, or removes drives from a library configuration within a SAN environment (this command is available on systems with the Data Protector User Interface component installed)

sanconf

SYNOPSIS

```
sanconf -version | -help
sanconf [-mom] -list[_devices] [ListFileName] [-hosts host_1
[host_2...] | -hostsfile HostsFileName]
sanconf [-mom] -configure [ListFileName] -library LibrarySerial-
Number LibraryName [RoboticControlHostName] [DeviceTypeNumber |
".DeviceTypeExtension"] [-hosts host_1 [host_2...] | -hostsfile
HostsFileName] [-drive_template DriveTemplateFileName] [-lib-
rary_template LibraryTemplateFileName] [-[no_]multipath] [-san-
stableaddressing]
sanconf [-mom] -remove_drives LibraryName [-hosts host_1 [host_2...]
| -hostsfile HostsFileName]
sanconf [-mom] -remove_hosts host_1 [host_2 host_3 ...] -library
LibSerNo [-[no_]multipath]
```

DESCRIPTION

The `sanconf` command is a utility that provides easier configuration of libraries in SAN environments. It can automatically configure a library within a SAN environment by gathering information on drives from multiple clients and configuring them into a single library. In MoM environments, `sanconf` can also configure any library in any Data Protector cell that uses CMMDB, provided that the cell in which `sanconf` is run uses CMMDB as well.

The `sanconf` command can be run on the Data Protector Cell Manager or on Data Protector clients. It resides in the `Data_Protector_home\bin` directory on Windows and in the `/opt/omni/lbin` directory on HP-UX and Solaris clients.

You can perform the following tasks using the `sanconf` command:

- Scan the specified Data Protector clients, gathering the information on SCSI addresses of drives and robotic controls connected to the clients in the SAN environment.

- Configure or modify settings of a library or drive for given clients using the information gathered during the scan of Data Protector clients.
- Remove drives on all or the specified clients from a library.

All `sanconf` sessions are logged to the file

`Data_Protector_program_data\log\sanconf.log` (Windows Vista, Windows Server 2008), `Data_Protector_home\log\sanconf.log` (other Windows systems), or `/var/opt/omni/log/sanconf.log` (HP-UX or Solaris systems).

OPTIONS

`-version`

Displays the version of the `sanconf` command.

`-help`

Displays the usage synopsis for the `sanconf` command.

`-mom`

Switches `sanconf` to operate in the MoM mode. This allows listing all devices connected to a MoM environment (see `-list`) and to configure devices in cells utilizing CMMDB (see `-configure`, `-remove_hosts`, `-remove`).

`[-mom] -list[_devices] [ListFileName]`

This option scans Data Protector clients to gather information on SCSI addresses of drives and robotic controls connected to the clients in the SAN environment and lists the gathered information. The information is uploaded to the Media Management Database on the Cell Manager. When `ListFileName` parameter is specified, the information acquired during the scan of clients is saved to the configuration file, which will be then used for configuring the library.

It is recommended to scan all clients that you want to configure, those that can see the robotics and those that can see the drives.

Note: When the option `-mom` is specified, `sanconf` lists clients and devices of all Data Protector cells in the MoM environment, even if they do not use CMMDB.

`-hosts host_1 [host_2...]`

Specify the `-hosts` option if you want to limit the `sanconf` actions only to specified clients. Other clients in the Data Protector cell are skipped.

`-hostsfile HostsFileName`

Specify the `-hostsfile` option if you want to limit the `sanconf` actions only to clients specified in the `HostsFileName`. Other clients in the Data Protector cell are skipped. The `HostsFileName` is comprised of an ASCII list of clients, one client per line. It is recommended that all clients are specified in the clients list before you save the scan information to the configuration file.

For multipath devices, the path order is determined by the order in the given list or file.

`[-mom]-configure [ListFileName]`

This option scans, lists, configures, or reconfigures the specified library. Only one library can be configured with each invocation of the command line. If the *ListFileName* option is not specified, the `sanconf` command will dynamically scan, list, and configure the library. If this option is specified, the scan and data information that was saved to a file during the scan of the specified clients is used to configure the library and scan is not performed. If a client is not scanned, the library will not be configured.

Important: `[RoboticControlHostName]` and `-hosts` or `-hostfile` information must be specified during configuration.

Note: When reconfiguring a library, it is recommended that configuration information is first stored in the configuration file in case of configuration failure. It is also recommended that a different filename is used so that the initial configuration can be restored without any complications. `sanconf` reuses the custom settings when reconfiguring a library.

`-library LibrarySerialNumber LibraryName`

`[RoboticControlHostName]`

`[DeviceTypeNumber | ".DeviceTypeExtension"]`

Specify the `-library` parameter to configure or reconfigure the specified library. Only one library can be configured with each invocation of the command line. `sanconf` creates only one logical library per physical library in the system and all devices on all specified clients. If the *RoboticControlHostName* parameter is specified, the specified client, which is connected to the specified library, will control the robotics for the library being configured. If this parameter is not specified, the library will be created with robotics on all clients, which are connected to the specified library, within the Data Protector cell, the Cell Manager will be used as a control host. If no library is installed on the Cell Manager in a multipath library, another client will be used as a control host.

If the *ListFileName* parameter is used together with the *RoboticControlHost* but without the `-hosts` or `-hostsfile` option specified, the *RoboticControlHost* parameter will be ignored and a library will be created on all clients which are connected to the library.

When the *RoboticControlHostName* is used with the `-hosts` or `-hostsfile` parameter (option) it limits a library configuration on a specified client. Robotics will be configured on the host which is specified with the *RoboticControlHostName* and on the drives on the host specified with the `-hosts` or `-hostsfile` option. The configuration will be successful only in

case that the *RoboticControlHostName* and the *Hosts* have the specified library installed.

In case that you try to configure a library with a robotic control host on a client which does not have a library installed, the configuration will not be successful (parameter `-hosts` is used).

In a MoM environment and with the `-mom` option specified, if the *RoboticControlHostName* parameter is specified without the `-hosts` or `-hostsfile` options, the `sanconf` command will configure a library on all hosts which are connected to it. For example, we have two hosts using the same CMMDB, but they can be on a different Cell Manager. If the hosts are both connected to the same library and only one of them is specified in the *RoboticControlHostName*, `sanconf` will configure two libraries with a robotic control on each host. The same happens in case of a host name which does not have the specified library installed.

If the *ListFileName* parameter is used together with the *RoboticControlHost* but without the `-hosts` or `-hostsfile` option, the *RoboticControlHost* parameter will be ignored and a library will be created on all clients which are listed in the file.

When the *RoboticControlHostName* is used with the `-hosts` or `-hostsfile` parameter it limits a library configuration on a specified client. Robotics will be configured on the host which is specified with the *RoboticControlHostName* and on the drives on the host specified with the `-hosts` or `-hostsfile` option. The configuration will be successful only in case that the *RoboticControlHostName* and the *Hosts* have the specified library installed.

In case that you try to configure a library with a robotic control host on a client which does not have the library installed, the configuration will not be successful.

Additionally, if you try to configure a library on a host which does not use the CMMDB, but its own (local) MMDB, the configuration will fail, whether you try to configure a library which is also installed on clients in the same CMMDB or not.

When the *DeviceTypeNumber* parameter is used, the drives of that type will be configured in the library. When the *DeviceTypeNumber* is not specified, the DLT drive types are used as the default. Only one type number may be specified per library. If you use the `".DeviceTypeExtension"` parameter instead of the *DeviceTypeNumber* parameter, you can specify the device type extension of the tape device to be configured in the library.

In the following table, *DTN* stands for *DeviceTypeNumber*, and *DTE* stands for *DeviceTypeExtension*.

<i>DTN</i>	<i>DTE</i>
------------	------------

1	DDT
2	QIC
3	EXA
4	AIT
5	3480
6	RDSK
7	REGFILE
8	9840
9	TAPE
10	DLT
11	D3
12	3590
13	LTO
14	SDLT
15	VXA
16	DTF
17	9940
18	SAIT
19	3592

When drives in the library are not of the same type as specified, an error is reported.

`-drive_template DriveTemplateFileName`

This option alters the default configuration of each tape device added to the library. You can alter the default configuration of the library only at the initial configuration. After the library is configured, you can no longer change the configuration of the library using the `sanconf` command.

The *DriveTemplateFileName* must be an ASCII file with one parameter specified per line.

Drive template supports the following parameters:

VERIFY

This parameter corresponds to the CRC Check option in the Data Protector GUI.

CLEANME

This parameter corresponds to the Detect dirty drive option in the Data Protector GUI.

RESCAN

This parameter corresponds to the `Rescan` option in the Data Protector GUI.

`SANSTABLEADDRESSING`

This parameter corresponds to the `Automatically discover changed SCSI address` option in the Data Protector GUI.

`-library_template` *LibraryTemplateFileName*

This option alters the default configuration of the library. You can alter the default configuration of the library only at the initial configuration. After the library is configured, you can no longer change the configuration of the library using the `sanconf` command.

The *LibraryTemplateFileName* must be an ASCII file with one parameter specified per line.

Library template supports the following parameters:

`BARCODEREADER`

This parameter corresponds to the `Barcode reader support` option in the Data Protector GUI.

`BUSYDRIVETOSLOT`

This parameter corresponds to the `Busy drive handling: Eject medium` option in the Data Protector GUI.

`BUSYDRIVETOMAILSLOT`

This parameter corresponds to the `Busy drive handling: Eject medium to mail slot` option in the Data Protector GUI.

`SANSTABLEADDRESSING`

This parameter corresponds to the `Automatically discover changed SCSI address` option in the Data Protector GUI.

`-[no_]multipath`

By default or if the `-no_multipath` option is given, `sanconf` does *not* configure multipath devices – a separate logical device will be configured for *each* path.

When reconfiguring a multipath library as a non-multipath library, only one path is created. Multipath drives contained inside a multipath library are not changed, while new drives are created. Only non-multipath drives are modified.

If the `-multipath` option is used, `sanconf` configures all paths pointing to a single physical device as a *single* multipath device.

When reconfiguring a non-multipath library as a multipath library, the library control host is used as the first path. Non-multipath drives are not changed or removed. Instead, new multipath drives are created. Only multipath drives are modified.

`-sanstableaddressing`

Enables automatic discovery of changed SCSI addresses for the devices being configured.

`[-mom] -remove_drives LibraryName`

This option removes all tape devices in the specified library. If you want to remove drives on specific clients, you can use the `-hosts host_1 [host_2...]` or the `-hostsfile HostsFileName` option. This command cannot be used together with the `-multipath` option. Drives that are configured as multipath drives are not removed.

Note: No rescanning is required for this operation.

`[-mom] -remove_hosts`

All paths containing the specified hosts are removed. However, if the specified hosts cover all paths of the library, no paths are not removed from this library, instead a warning is displayed.

To remove paths only from *multipath* devices, add the `-multipath` option.

To remove paths only from *non-multipath* devices, add the `-no_multipath` option.

To remove paths from *both*, multipath *and* non-multipath devices, run the command *without* the `-no_multipath` and `-multipath` options.

Note: No rescanning is required for this operation.

NOTES

The `sanconf` command is available on Windows, HP-UX, Solaris, and Linux systems only.

All drives created with the `sanconf` command are named automatically. Drive names must not be changed manually because the reconfiguration will not work. You must follow the drive naming convention.

- For *non-multipath* devices:

`libname_index_host`

`libname_index_busindex_host`

The `busindex` number is used only if there is more than one path for the drive.

- For *multipath* devices:

`libname_index`

EXAMPLES

The following examples illustrate how the `sanconf` command works.

1. To scan host(s) for robotic control(s) and tape device(s) and create a file that will be used by `sanconf -configure`, run:

```
sanconf -list device.list
```

This will display the serial number for any library discovered in the SUMMARY REPORT.

2. To scan and configure a library using the library serial number and the library name, on all clients on which the library is installed and which use CMMDB, run:

```
sanconf -mom -configure -library US9LS01033 SAN_STORE
```

Clients on which the library is installed and which use a local MMDB are skipped.

3. To scan the specified clients and then create a logical library named "SAN_STORE" with robotics configured on client "host33" and drives for that library configured on clients "host01", "host02" and "host03", run:

```
sanconf -configure -library MPC0100013 SAN_STORE host33  
-hosts host01 host02 host03
```

A device type is `.lto`. An extension parameter does not need to be added.

4. To scan the SAN environment for the configuration information on the specified clients "host01", "host02", "host03", and "host33" which use CMMDB, and save this information into the `mySAN.cfg` file, run:

```
sanconf -mom -list_devices mySAN.cfg -hosts host01 host02  
host03 host33
```

5. To use information stored in the `mySAN.cfg` file and create a logical library named "SAN_STORE" with robotics configured on client `host33` and drives for the library configured on clients "host01", "host02", and "host03", run:

```
sanconf -configure mySAN.cfg -library MPC0100013 SAN_STORE  
host33 -hosts host01 host02 host03
```

6. To scan all clients in the cell and then create a logical library named "SAN_STORE" on client "host33" with the parameters specified in the files `DriveTemplate.txt` and `LibraryTemplate.txt`, run:

```
sanconf -configure -library MPC0100013 SAN_STORE host33  
-hosts host33 -drive_template DriveTemplate.txt  
-library_template LibraryTemplate.txt
```


7. To configure a tape library with the default tape device and library settings using the "device.list" file created by the example above, run:

```
sanconf -configure device.list -library MPC0220423 myLib1
```

8. To configure a library with a specific drive type, run:

```
sanconf -configure -library MPC0100013 SAN_STORE host33  
".9840" -hosts host01 host02
```

This command creates a library named "SAN_STORE" with robotics configured on client "host33" and STK drives configured on clients "host01" and "host02". The drives are named as follows:

```
SAN_STORE_1_host01  
SAN_STORE_1_host02  
SAN_STORE_2_host01  
SAN_STORE_2_host02
```

9. To configure three libraries using the configuration options contained in the library template "myway", run:

```
sanconf -configure -library US9LS02033 mylib5  
-library_template myway  
sanconf -configure -library US9LS02034 mylib6  
-library_template myway  
sanconf -configure -library US9LS02035 mylib7  
-library_template myway
```

10. To configure a multipath LTO library with the serial number "LLL1", named "Library1", and connected to client "host1", run:

```
sanconf -configure -library LLL1 Library1 host1 ".LTO"  
-multipath
```

11. To configure a multipath LTO library with the serial number "LLL1", named "Library1", and connected to client "host1" and "host2", run:

```
sanconf -configure -library LLL1 Library1 host1 ".LTO"  
-hosts "host1" "host2" -multipath
```

This will configure a library and drives with multipath option checked and configured paths on host1 and host2.

12. To update an already configured library with the configuration information for new hosts or tape devices, run:

```
sanconf -configure -library US9LS01023 mylib2
```

13. To reconfigure an already configured library after adding a new host "myhost" to a Data Protector cell, run:

```
sanconf -configure -library US9LS01033 mylib2 -hosts myhost
```

This will scan and configure only the new host.

- 14.** In a MoM environment, to reconfigure an already configured library on "host02" after adding a new host "myhost" to a Data Protector cell, run:

```
sanconf -mom -configure -library US9LS01033 mylib2 host02  
-hosts myhost
```

This will add drives from the host "myhost" to the library "mylib2" which is configured on the host "host2".

- 15.** To configure only LTO Ultrium tape drives and add them into the library "myLTOLib", run:

```
sanconf -list device.list  
sanconf -configure device.list -library MPC0230031 myLTOLib  
"libraryhost" ".LTO"
```

- 16.** To reconfigure a non-multipath library named "SAN_STORE" with serial number "MPC0100013" to a multipath library using the `-hosts` option, when new clients "host04" and "host05" are added to the cell, run:

```
sanconf -configure -library MPC0100013 SAN_STORE host33  
-hosts host04 host05 -multipath
```

- 17.** To delete all tape drives configured in the library "mylib2" related to the clients "host04" and "host05", run:

```
sanconf -remove_drives mylib2 -hosts host04 host05
```

- 18.** To delete all tape drives configured in the library "mylib2", run:

```
sanconf -remove_drives mylib2
```

- 19.** To remove all paths in the multipath library named "SAN_STORE" with serial MPC0230031 that are configured on clients "host04" and "host05", run:

```
sanconf -remove_hosts -hosts host04 host05 -library  
MPC0230031 -multipath
```

SEE ALSO

omniamo(1), omnidownload(1), omnimcopy(1), omniminit(1), omnimlist(1),
omnimmm(1), omnimnt(1), omnimver(1), omniupload(1), uma(1M)

uma

controls the robotics of SCSI compliant autochangers
(this command is available on systems with the Data Protector General Media Agent or NDMP Media Agent component installed)

uma

SYNOPSIS

```
uma -version | -help
uma [-policy LogicalDevicePolicy] -ioctl deviceFile [-interface
{0 | 1}] [-tty] [-barcode] [-device deviceFile_1 [deviceFile_n] -type
DeviceType] [-ddt NDMP_server_name NDMP_port_number backup_type
username password] [-vls_address VLSAddress] [-vls_port VLSPort]
[-vls_username VLSUsername] [-vls_password VLSPassword]
```

Uma command line interface commands:

```
help
inq
init
addr
offl driveID
sense
pos slot
move source_slot destination_slot [0 | 1]
stat [{slot | drive | transport_element | mail_slot}]
modesense [page]
test
bye | exit | quit
doorlock [0 | 1]
enter slot
eject slot
```

DESCRIPTION

The `uma` program is a standalone utility program which can be used to control the robotics of most SCSI compliant autochangers, also those which are not directly supported by Data Protector. It implements a shell-like user command interface and can be used both interactively and in batch mode.

`Uma` is packaged and installed as part of a Data Protector Media Agent filesset. If you have received `uma` as a standalone program or if you run it on a system where

Data Protector has not been installed, the `uma` command is fully functional and behave as documented, but it is probably not able to locate and use Data Protector NLS message catalog.

On HP-UX and Solaris systems, `uma` is located in `/opt/omni/sbin/` directory, and the Data Protector NLS message catalog is located in the `/opt/omni/lib/nls/C/` directory.

On other UNIX systems, `uma` is located in `/usr/omni/bin/` directory, and the Data Protector NLS message catalog is located in the `/usr/omni/lib/nls/C/` directory.

On Windows systems, `uma` is located in `Data_Protector_home\bin` directory, and the Data Protector NLS message catalog is located in the `Data_Protector_home\bin` directory.

`Uma` can be started both interactively or in batch mode. The only obligatory option is the pathname of the device file (UNIX systems) or the SCSI address (Windows systems) that controls the robotics of the target autochanger (the `-ioctl` option). For backup devices with library robotics connected to an NDMP Server (to a supported NAS device), the `-interface` and the `-ddt` options must also be specified.

For your convenience, the `uma` command allows you to specify symbolic instead of physical element addresses (slot IDs). Whenever you need to refer to the 1st drive of the autochanger, you can specify either the physical address '128' or the more convenient, symbolic 'D1'. The output of the `addr` command reflects this addressing convention.

OPTIONS

`-version`

Displays the version of the `uma` command.

`-help`

Displays the usage synopsis for the `uma` command.

`-policy LogicalDevicePolicy`

Specifies the backup device policy ID. Policy can be defined as 6 (external control), 8 (Grau DAS exchanger library), 9 (STK Silo medium library), 10 (SCSI Library), or 13 (VLS).

The default value for the `-policy` option is 10.

`-ioctl deviceFile`

Specifies the pathname of the device file (UNIX systems) or the robotics SCSI address (Windows systems) that controls the robotics of the target autochanger.

`-interface{0 | 1}`

Sets the type of SCSI interface used to access library robotics. This option is to be used only with backup devices with library robotics connected to an NDMP Server. 0 sets the standard SCSI interface (the default value). 1 sets the NDMP protocol interface and must be specified for backup devices with library robotics connected to an NDMP Server. The default value is 0.

`-tty`

Forces the `uma` command to enter the command line interface mode or to read from script. This option is obligatory on UNIX, MPE/iX, and NetWare systems. On Windows systems, this option is not to be used; the command line interface mode is invoked automatically.

`-barcode`

If this variable is set, the `uma` command's `stat` command displays also the barcode information for each medium.

`-device deviceFile_1 [deviceFile_n...]`

Specifies the device file (UNIX systems) or the SCSI address (Windows systems) of one or more autochanger drives. For a multi-drive autochanger, you must specify a list of device files/SCSI addresses which correspond to the autochanger's drives in ascending order. The drives have to be known to `uma` in order for the `offl` command to work. This option is only to be used together with `-type` option.

`-type DeviceType`

Specifies the media type for the media in the device specified by the `-device` option. Media type numbers are defined in the *HP Data Protector product announcements, software notes, and references*. The media type number for VLS is 0.

`-ddt NDMP_server_name NDMP_port_number backup_type username password`

This option is mandatory for backup devices with library robotics connected to an NDMP Server (to a supported NAS device). It specifies the NDMP Server name, port number used by Data Protector to connect to the NDMP Server and username and password used by Data Protector to connect to the NDMP server. The `backup_type` parameter has to be set to `dump`.

`-vls_address VLSAddress`

Specifies the IP address or the hostname of the VLS client.

`-vls_port VLSPort`

Specifies the VLS port number.

`-vls_username VLSUsername`

Sets the username for the specified user, who has sufficient privileges to read attributes and trigger operations on the VLS.

`-vls_password VLSPassword`

Sets the password for the specified user.

Uma command line interface commands:

`help`

Displays the usage synopsis for the `uma` command.

`inq`

Performs a SCSI Inquiry operation on the device file/SCSI address specified with the `-ioctl` option. It returns the device's type, vendor ID, product ID and firmware revision number.

`init`

Performs a SCSI 'initialize element status' operation, which (if applied to an autochanger robotic device) forces the autochanger to reset its internal state and perform an inventory of its repository. This command should not be used if another process is accessing the autochanger at the same time, as the effects are unpredictable.

`addr`

Queries and displays the autochanger's element assignment page. Each addressable item inside the autochanger mechanism (drive, repository slot, robotic arm, import/export slot) has a unique integer number (slot ID) which can be used to address this specific item.

As the element assignment differs among different autochangers, the software, which is to control the movement of media inside the autochanger, must find out and use these numbers to perform move, pos and stat operations.

`offl driveID`

This command can be used only if at least one drive was specified using the `-device` option. If a medium is loaded in the specified drive, it will eject the medium just as if an UNIX `mt offl` command was specified. The mandatory argument is a symbolic drive ID (i.e. D3 for the 3rd drive == the 3rd device file specified with the `-dev` option). If the drive specified is not defined by the `-device` option, then the last drive defined by the `-device` option will be used.

The `offl` command can fail with a message: "No such device or address" if it is issued immediately after the `move` command since it takes a certain time after the `move` command for the drive to be online. Refer to the `move` command for more information.

`sense`

Read the device's sense data and dump them in a hex- dump format.

`pos slot`

Positions the autochanger transport mechanism in front of the specified slot. This operation is only meaningful if the specified slot refers to an import/export, data drive or repository element. The actual meaning of this operation may differ among different autochanger models. This command is generally not required, but is provided for testing purposes and convenience. Both physical as well as symbolic slot addressing may be used.

`move source_slot destination_slot [0 | 1]`

Moves a medium from a source slot into a destination slot. This command has two mandatory arguments, the source and destination slot IDs (address numbers, as reported by the `addr` command described above) and an optional numeric Boolean argument which can be used to instruct the robotics to flip the medium before inserting it into the destination slot. By default (if no flipping argument is specified), flipping is disabled.

Note that when `move` command is issued to move a tape into a drive, it takes a certain time (around 30 seconds) for the drive to become online, because tape load and calibration/selftest have to be performed. The command prompt however, returns immediately after the command is issued.

NOTE: Flipping is supported only for double-sided optical media. For tapes, the effect of the flip command is not defined.

NOTE: Most autochanger do not allow you to `move` a tape from a drive to a repository location if the tape has not been dismounted and ejected by the drive. You might want to use the `offl` command on the drive device file/SCSI address to put the drive off-line before executing the `move` command.

`stat [{slot | drive | transport_element | mail_slot}]`

Queries the device for information about the state of each of its addressable elements. The output of this command is a table of physical and symbolic element IDs and their states, indicating which elements are free (Empty) and occupied (Full).

Additionally, if barcode support is available and enabled, the barcode for each medium is displayed.

The `uma` command recognizes one specific environment variable which can be used to enable barcode support for autochangers which are equipped with barcode reading hardware. By default, `uma` barcode support is disabled. It can be enabled by exporting/setting the `OB2BARCODE=1` environment variable before starting the command or by using the `-barcode` option.

The `stat` command can be used to query the status of a specific slot (i.e. 'stat 290' or 'stat S35') or a related group of slots (i.e. 'stat D' will query all drives, 'stat S' will query all repository slots, etc.).

If no additional arguments are specified, the `stat` command will query and print the status information for all slot IDs it can address.

`modesense [page]`

Reads the vendor specific data and unit settings from the unit and displays them. You can limit the display only to certain pages by using the `page` parameter. If the `page` parameter is not specified, all pages are displayed.

`test`

Checks if the unit is ready. If the unit is not used by any process, then the unit is ready. If it is, however, used either by the robotics, backup or restore processes then it is not ready.

`exit | bye | quit`

Exits the command mode.

`doorlock [0 | 1]`

If the input parameter is 1, this command locks the library mail slot door; if it is 0, it unlocks it.

`-enter slot`

Enters media into a specified library slot.

`-eject slot`

Ejects media from a specified library slot.

NOTES

Do not use the `uma` utility while Data Protector backup or restore is running. On UNIX, MPE/iX, and NetWare systems the `-tty` option is obligatory. On Windows systems it is not used.

EXAMPLES

1. `Uma` can be started both interactively or in batch mode. The only option which needs to be specified (except for backup devices with library robotics connected to an NDMP Server) is the pathname of the device file which controls the robotics of the target autochthons:

```
AMA -octal /Dave/spot/sct10
```

```
*** PROGRAM: UMA VERSION: HP Data Protector A.06.11
```



```

*** Copyright (C) 1999 Hewlett-Packard Company
*** License is restricted for use with licensed
*** HP Data Protector products.
/dev/spt/sctl0> exit

```

2. To start `uma` for a backup device with the library robotics connected to the NDMP Server with the robotics SCSI address "mc2", the NDMP Server hostname "ndmpserver", the port number used by Data Protector to connect to the NDMP Server "10000", and username and password of the user used by Data Protector to connect to the NDMP Server "user password", enter the following command:

```

UMA -ioctl mc2 -interface 1 -ddt ndmpserver 10000 dump
user password

```

3. To let `uma` execute a batch script of its own commands, simply redirect its stdin to a file containing a list of `uma` commands separated with newlines:

```

cat >/tmp/cmdFile
inq
addrstat
<ctrl-D>
uma -ioctl /dev/spt/sctl0 </tmp/cmdFile >/tmp/outFile

```

4. The following output is obtained by executing the `addr` command on the UNIX device file referring to an ACL 4/52 DLT autochanger:

```

/dev/spt/sctl0> addr Element Addresses (T=Transport,
X=Im/Export, D=Drive, S=Storage):
Transport: 1 .. 1 (T1 .. T1)
Im/Export: 64 .. 67 (X1 .. X4)
Data Drive(s): 128 .. 131 (D1 .. D4)
Repository: 256 .. 303 (S1 .. S48)

```

The numbers returned by the `addr` command are the physical element addresses of different elements within the autochanger - i.e. element address "256" would correspond to the 1st repository slot, element address "65" would correspond to the location of the 2nd data drive etc.

5. To start `uma` for the Grau DAS exchanger library with the robotics device file "grauamu", run:

```

uma -pol 8 -ioctl grauamu

```

SEE ALSO

`omniamo(1)`, `omnidownload(1)`, `omnimcopy(1)`, `omniminit(1)`, `omnimlist(1)`,
`omnimm(1)`, `omnimnt(1)`, `omnimver(1)`, `omniupload(1)`, `sanconf(1M)`

upgrade_cm_from_evaa

upgrades the EVADB entries created by the HP StorageWorks EVA Agent (legacy) to the SMISDB entries created by the HP StorageWorks EVA SMI-S Agent (this command is available on the Data Protector Cell Manager)

upgrade_cm_from_evaa

SYNOPSIS

```
upgrade_cm_from_evaa -version | -help
upgrade_cm_from_evaa [-preview]
```

DESCRIPTION

The `upgrade_cm_from_evaa` command needs to be executed on any Cell Manager after completing the Cell Manager upgrade from the EVA Agent (legacy) to the EVA SMI-S Agent. It upgrades the following:

- EVADB login entries into SMISDB logging entries
- EVADB disk group rules into SMISDB disk group rules
- EVAA backup specifications into SMISA backup specifications
- EVADB backup sessions into SMISA backup sessions

OPTIONS

`-version`

Displays the version of the `upgrade_cm_from_evaa` command.

`-help`

Displays the usage synopsis for the `upgrade_cm_from_evaa` command.

`-preview`

Gives a preview of what happens when the command is run.

EXAMPLES

The following examples illustrate how to use the `upgrade_cm_from_evaa` command.

1. To display the version information, run:

```
upgrade_cm_from_evaa -version
```

2. To preview what happens when the upgrade from the EVA Agent (legacy) to the EVA SMI-S Agent is run on the Cell Manager, run:

```
upgrade_cm_from_evaa -preview
```

This command displays a list of actions that will be taken when the upgrade is run but it does not update the EVADB entries.

SEE ALSO

ob2install(1M), omnidbsmis(1), omnigui(5), omniintro(9), omnimigrate.pl(1M),
omnisetup.sh(1M), omniusers(1), winomnimigrate.pl(1M)

util_cmd

sets, retrieves, or lists the parameters stored in the Data Protector Oracle, SAP R/3, SAP DB/MaxDB, Informix, Sybase, and VMware Virtual Infrastructure configuration files. In addition, it encodes passwords.

(this command is available on systems with any Data Protector component installed)

util_cmd

SYNOPSIS

```
util_cmd -version | -help
util_cmd -getconf[ig] {Oracle8 | SAP | SAPDB | Informix | Sybase |
vmware} instance [-local filename]
util_cmd -getopt[ion] [{Oracle8 | SAP | SAPDB | Informix | Sybase |
vmware} instance] option_name [-sub[list] sublist_name] [-local
filename]
util_cmd -putopt[ion] [{Oracle8 | SAP | SAPDB | Informix | Sybase |
vmware} instance] option_name [option_value] [-sub[list] sub-
list_name] [-local filename]
util_cmd -encode Password
```

DESCRIPTION

The `util_cmd` command is used to set, retrieve, or list the parameters stored in the Data Protector Oracle, SAP R/3, SAP DB/MaxDB, Informix, Sybase, and VMware Virtual Infrastructure configuration files. In addition, it can be used to encode passwords.

Data Protector stores the integration parameters on the Cell Manager in the directory `Data_Protector_program_data\Config\Server\Integ\Config\integration_name` (Windows Server 2008),

`Data_Protector_home\Config\Server\Integ\Config\integration_name` (other Windows systems), or

`/etc/opt/omni/server/integ/config/integration_name` (UNIX systems).

ORACLE

For each configured Oracle database, the following configuration files are created:

- Target database configuration file: `client_name%[DB_NAME | INSTANCE_NAME]`
For Oracle Data Guard, `client_name` is `primary_hostname` or `secondary_hostname`

The parameters stored in the target database configuration file are:

- Oracle home directory
- encoded connection strings to the target database, recovery catalog, and standby database
- variables, which are exported when you start a session using the Data Protector GUI or CLI

OB2_RMAN_COMMAND_TIMEOUT (environmental variable)

This variable is applicable when Data Protector tries to connect to a target or catalog database. It specifies how long (in seconds) Data Protector waits for RMAN to respond that the connection succeeded. If RMAN does not respond within the specified time, Data Protector aborts the session. Default: 300 s.

OB2_SQLP_SCRIPT_TIMEOUT (environmental variable)

This variable is applicable when Data Protector issues an SQL*Plus query. It specifies how long Data Protector waits for SQL*Plus to respond that the query completed successfully. If SQL*Plus does not respond within the specified time, Data Protector aborts the session. Default: 300 s.

SBT_LIBRARY

Specifies which Data Protector MML should be used by RMAN, in case you want to override the default Data Protector selection.

- Global database configuration file: *client_name%_OB2_GLOBAL*

The parameters stored in the global configuration file are:

- instance list (all Oracle instances on the Oracle server)
- variables that need to be exported prior to starting a backup and which affect every Oracle instance on the Oracle server.

- In case of zero downtime backup, backup method configuration file:

zdb_methodORACLE_DBID

- In case of zero downtime backup, for backup set method, the file:

client_name%initDB_NAME_bckp.ora

SAP R/3

The SAP R/3 parameters stored are:

- Oracle home directory
- encoded connection string to the target database
- BRTOOLS home directory
- variables, which are exported when you start a session using the Data Protector GUI or CLI

ORA_NLS_CHARACTERSET

After upgrading a Data Protector A.05.50 SAP R/3 client to Data Protector A.06.11, set this variable to the encoding used by the Oracle database.

OB2_MIRROR_COMP

This variable is applicable for ZDB sessions that use the SPLITINT functionality (`-t {online_mirror | offline_mirror}`). Set this variable to 1 if you want BRBACKUP to be started on the backup system and not on the application system. By default, BRBACKUP is started on the application system.

SBT_LIBRARY

Specifies which Data Protector MML should be used by RMAN, in case you want to override the default Data Protector selection.

- concurrency number and balancing (for each backup specification) and number of channels for RMAN backup
- speed parameters (time needed for a specific file to back up - in seconds)
- manual balancing parameters

SAP DB/MaxDB

The SAP DB/MaxDB parameters stored are:

- Username of the SAP DB/MaxDB database user
- Password of the SAP DB/MaxDB database user
- SAP DB/MaxDB version
- SAP DB/MaxDB independent program path parameter that was specified during the installation of SAP DB/MaxDB Server
- Data Protector SAP DB/MaxDB integration related environment variables

INFORMIX SERVER

The Informix parameters stored are:

- Informix Server home directory
- pathname of the `sqlhosts` file
- name of the Informix instance `ONCONFIG` file

SYBASE

The Sybase parameters stored are:

- Sybase home directory
- pathname for the `isql` command
- Sybase backup operator username and password
- name of the Sybase `SYBASE_ASE` directory (Sybase 12.x only)

- name of the Sybase *SYBASE_OCS* directory (Sybase 12.x only)
- environment variables

VMWARE VIRTUAL INFRASTRUCTURE

For each configured VMware datacenter, Data Protector creates the following configuration files:

- Global configuration file
 Name: *VMwareManagementClient%_OB2_GLOBAL*
 Example: *vcvirtual.company.com%_OB2_GLOBAL*
- Virtual machines configuration file
 Name: *VMwareManagementClient%DatacenterPath*
 Example: *vcvirtual.company.com%%2FMyFolder1%2FDatacenter1*
 As seen in the example, the datacenter path (*/MyFolder1/Datacenter1*) is URL-encoded: slashes are converted to *%2F*.

The global configuration file contains the following parameters:

- Security (0 – standard security, 1 – integrated security)
- Username and encrypted password for the VMware management client (in case of standard security)
- Port (optional)
- Web service entry point URI (optional)
- Username (OSUSER) and group (OSGROUP) of the ESX Server system user (this information is included only when you configure the */ha-datacenter*)

The virtual machines configuration file contains the following parameters:

- Username (OSUSER) and group (OSGROUP) of the ESX Server system user (this information is included only when you configure the */ha-datacenter*)
- Information about each virtual machine in the datacenter:
 - Virtual machine path
 - Snapshot handling mode
 - 0 – disabled
 - 1 – single
 - 2 – mixed
 - Backup proxy to be used
 - Mountpoint to be used (optional)

The Data Protector configuration parameters for an integration are normally written to the Data Protector configuration files:

- during the configuration of the integration
- during the creation of a backup specification if the configuration parameters are changed
- when the configuration parameters are changed

All sublist configuration parameters in the configuration files are optional.

RETURN VALUES

The `util_cmd` command displays a short status message after each operation (written to the standard error):

- Configuration read/write operation successful.
This message is displayed when all the requested operations have been completed successfully.
- Configuration option/file not found.
This message appears when either an option with the specified name does not exist in the configuration, or the file specified as the `-local` parameter does not exist.
- Configuration read/write operation failed.
This message is displayed if any fatal errors occurred, for example: the Cell Manager is unavailable, the Data Protector configuration file for a specific integration is missing on the Cell Manager, etc...

OPTIONS

`-version`

Displays the version of the `util_cmd` command.

`-help`

Displays the usage synopsis for the `util_cmd` command.

`-getconf[ig] integration instance`

Lists the Data Protector configuration files parameters for the specified integration and instance to the standard output, unless the `-local` option is specified.

`-getopt[ion] [integration instance] option_name`

Retrieves the parameter (specified by the `option_name`) and its value from one of Data Protector configuration files and writes it to the standard output, unless the `-local` option is specified.

`-putopt[ion] [integration instance] option_name [option_value]`

Sets the specified parameter (specified by the `option_name`) and (optionally) its value to the Data Protector configuration files, unless the `-local` option is used.

To remove a value of a parameter, specify the `option_name`, without the `option_value`. However, if the option is in a sublist, you must specify an empty `("") option_value` to remove a value.

`-sublist SublistName`

Specifies the sublist in the configuration file in which a parameter is written to or taken from.

`-local FileName`

If the `-local` option is used with the `-getconf` option, the command output is written to the file with the filename specified by the `-local` option. If the `-local` option is used with the `-getopt` option, the parameter and its value is taken from the file with the filename specified by the `-local` option. If the `-local` option is used with the `-putopt` option, the parameter and its value is written to the file with the filename specified by the `-local` option.

`-encode Password`

Returns the encoded form of the specified password.

EXAMPLES

The following examples illustrate how the `util_cmd` command works.

1. To set the Data Protector "OB2OPTS" parameter for the Oracle instance "ICE", run:

```
util_cmd -putopt Oracle8 ICE OB2OPTS "-debug 1-200  
INSTANCE.txt" -sublist Environment
```
2. To set the Data Protector "OB2OPTS" parameter for the SAP R/3 instance "ICE", run the following command on the Data Protector SAP R/3 client:

```
util_cmd -putopt SAP ICE OB2OPTS '-debug 1-200  
INSTANCE.txt' -sublist Environment
```
3. To set the "BR_TRACE" parameter for the SAP R/3 instance "ICE" to value "10" in the "Environment" sublist, run the following commands on the Data Protector SAP R/3 client:

```
util_cmd -putopt SAP ICE BR_TRACE "'10'" -sublist  
Environment
```

4. To list the Data Protector configuration file parameters for the Oracle instance "ICE", run:

```
util_cmd -getconf Oracle8 ICE
```

5. To list the parameters from the VMware Virtual Infrastructure configuration file `vcvirtual.company.com%_OB2_GLOBAL`, run:

```
util_cmd -getconf vmware _OB2_GLOBAL
```

To list the parameters from the VMware Virtual Infrastructure configuration file `vcvirtual.company.com%%2FMyFolder1%2FDatacenter1`, run:

```
util_cmd -getconf vmware /MyFolder1/Datacenter1
```

6. To retrieve the value of the "OB2OPTS" parameter for the Oracle instance "ICE", run:

```
util_cmd -getopt Oracle8 ICE OB2OPTS -sublist Environment
```

7. To remove the value of the "OB2OPTS" parameter for the SAP R/3 instance "ICE", run the following command on the Data Protector SAP R/3 client:

```
util_cmd -putopt SAP ICE OB2PTS "" -sublist Environment
```

8. To get the encoded form of the password "BlueMoon", run:

```
util_cmd -encode BlueMoon
```

9. To set the environmental variable "OB2_RMAN_COMMAND_TIMEOUT" to "100" seconds for the Oracle database "INST2", run:

```
util_cmd -putopt Oracle8 INST2 OB2_RMAN_COMMAND_TIMEOUT  
100 -sublist Environment
```

SEE ALSO

`omnib(1)`, `omnicreatedl(1)`, `omniintconfig.pl(1M)`, `util_oracle8.pl(1M)`,
`util_vmware.exe(1M)`

util_oracle8.pl

configures an Oracle database and prepares the environment for backup, and checks the configuration of an Oracle database

(this command is available on systems with the Data Protector Oracle Integration component installed)

util_oracle8.pl

SYNOPSIS

```
util_oracle8.pl -version | -help
util_oracle8.pl -chkconf -dbname DB_NAME [-client CLIENT_NAME]
util_oracle8.pl -chkconf_smb -dbname DB_NAME [-bkphost
BACKUP_SYSTEM] [-client CLIENT_NAME]
util_oracle8.pl -chkconf_ir -dbname DB_NAME [-client CLIENT_NAME]
util_oracle8.pl -config -dbname DB_NAME -orahome ORACLE_HOME
PRIMARY_DB_LOGIN [STANDBY_DB_LOGIN] [CATALOG_DB_LOGIN] [ZDB_OP-
TIONS] [-client CLIENT_NAME]
PRIMARY_DB_LOGIN
-prmuser PRIMARY_USERNAME
-prmpasswd PRIMARY_PASSWORD
-prmservice PRIMARY_NET_SERVICE_NAME_1 [,PRIMARY_NET_SER-
VICE_NAME_2,...]
CATALOG_DB_LOGIN
-rcuser CATALOG_USERNAME
-rcpasswd CATALOG_PASSWORD
-rcservice CATALOG_NET_SERVICE_NAME
STANDBY_DB_LOGIN
-stbuser STANDBY_USERNAME
-stbpasswd STANDBY_PASSWORD
-stbservice STANDBY_NET_SERVICE_NAME_1 [,STANDBY_NET_SER-
VICE_NAME_2,...]
ZDB_OPTIONS
-zdb_method {PROXY | BACKUP_SET}
[-ctlcp_location BACKUP_CONTROL_FILE_COPY_LOCATION]
[-pfile PARAMETER_FILE]
[-bkphost BACKUP_SYSTEM]
```

On Windows systems, you must use the `perl` command to run `util_oracle8.pl`. For example:

```
perl -I..\lib\perl util_oracle8.pl -help
```

DESCRIPTION

Use the `util_oracle8.pl` command to configure an Oracle database and prepare the environment for backup, and to check the configuration of the database.

To back up a standby database, you must provide the `STANDBY_DB_LOGIN` information. For standby database backup, a recovery catalog must be used. Therefore, you must also provide the `CATALOG_DB_LOGIN` information.

To configure an Oracle database for ZDB, you must provide the `ZDB_OPTIONS` information. If your ZDB method is backup set, you must also provide the `BACKUP_SYSTEM` information.

OPTIONS

`-version`

Displays the version of the `util_oracle8.pl` command.

`-help`

Displays the usage synopsis for the `util_oracle8.pl` command.

`-client` *CLIENT_NAME*

Name of the Oracle Server system with the database to be configured. You only need to specify it in a cluster environment.

In an RAC environment: Name of the node or the virtual server of the Oracle resource group. The latter can only be used on HP-UX: Name of the database to be configured.

In an Oracle Data Guard environment: Name of either a primary system or secondary (standby) system.

`-dbname` *DB_NAME*

Name of the database to be configured.

`-orahome` *ORACLE_HOME*

Pathname of the Oracle Server home directory.

`-config`

Configures an Oracle database.

`-chkconf`

Checks the configuration of an Oracle database.

`-chkconf_smb`

Checks if an Oracle database is properly configured for ZDB.

`-chkconf_ir`

Checks if an Oracle configuration is suitable for instant recovery.

`-bkphost BACKUP_SYSTEM`

Name of the backup system.

`-prmuser PRIMARY_USERNAME`

Username for login to the target or primary database. Note that the user must have been granted the SYSDBA privilege.

`-prmpasswd PRIMARY_PASSWORD`

Password for login to the target or primary database. Note that the user must have been granted the SYSDBA privilege.

`-prmservice PRIMARY_NET_SERVICE_NAME_1 [, PRIMARY_NET_SERVICE_NAME_2, ...]`

Net services names for the primary database.

In an RAC environment: Each net service name must resolve into a specific database instance.

`-rcuser CATALOG_USERNAME`

Username for login to the recovery catalog. This is optional and is used only if you use the recovery catalog database catalog as an RMAN repository for backup history.

`-rcpasswd CATALOG_PASSWORD`

Password for login to the recovery catalog. This is optional and is used only if you use the recovery catalog database catalog as an RMAN repository for backup history.

`-rcservice CATALOG_NET_SERVICE_NAME`

Net services name for the recovery catalog.

`-stbuser STANDBY_USERNAME`

Used in the Oracle Data Guard environment for backing up a standby database. Username for login to the standby database.

`-stbpasswd STANDBY_PASSWORD`

Used in the Oracle Data Guard environment for backing up a standby database. Password for login to the standby database.

`-stbservice STANDBY_NET_SERVICE_NAME_1 [, STANDBY_NET_SERVICE_NAME_2, ...]`

Net services names for the standby database.

`-zdb_method {PROXY | BACKUP_SET}`

Configures the Oracle database for ZDB environment and sets the ZDB method to Oracle proxy-copy or Oracle backup set.

`-ctlcp_location BACKUP_CONTROL_FILE_COPY_LOCATION`

The location on the source volumes where a copy of the current control file is made during ZDB to disk. This is optional and if not specified, `ob2rman.pl` will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

If you use a raw logical volume as the

`BACKUP_CONTROL_FILE_COPY_LOCATION`, the raw logical volume must reside on a volume group that will be replicated. If there is no such raw logical volume available, create a new shared disk (volume group) residing on the disk that will be replicated and configure a raw logical volume on it. If you use a raw logical volume, in case of an ZDB to disk, you need to ensure enough free space in the `/var/opt/omni/tmp` directory on the backup host to hold the copy of the raw logical volume.

`-pfile PARAMETER_FILE`

Full name of the PFILE residing on the application system. This is optional and used if backup method is backup set and the database instance uses PFILE (and not SPFILE).

NOTES

- On HP OpenVMS, to invoke the Data Protector CLI, run:

```
$@OMNI$ROOT: [BIN] OMNI$CLI_SETUP.COM
```

- `BACKUP_CONTROL_FILE_COPY_LOCATION`:

This parameter is optional and if not specified, `ob2rman.pl` will copy the copy of the control file from the application system to the backup system when it is needed. Thus, you do not need to create an additional disk for this location if you do not need the control file copy on a replica.

If you use a raw logical volume as the

`BACKUP_CONTROL_FILE_COPY_LOCATION`, the raw logical volume must reside on a volume group that will be replicated. If there is no such raw logical volume available, create a new shared disk (volume group) residing on the disk that will be replicated and configure a raw logical volume on it. If you use a raw logical volume, in case of an ZDB to disk, you need to ensure enough free space in the

`/var/opt/omni/tmp` directory on the backup host to hold the copy of the raw logical volume.

- *PARAMETER_FILE:*

This parameter is optional and used if backup method is backup set and the database instance uses PFILE (and not SPFILE).

EXAMPLES

The following names are used in the examples below:

- database name: `orac1`
- Oracle Server home directory: `app10g/oracle10g/product/10.1.0`
- primary user name: `system`
- primary password: `manager`
- primary net service name 1: `netservice1`
- primary net service name 2: `netservice2`
- recovery catalog user name: `rman`
- recovery catalog password: `manager`
- recovery catalog net service name: `catSERVICE`
- standby user name (Oracle DataGuard only): `system`
- standby password (Oracle DataGuard only): `manager`
- standby net service name 1 (Oracle DataGuard only): `netSERVICESb1`
- standby net service name 2 (Oracle DataGuard only): `netSERVICESb2`
- parameter file: `/app10g/oracle10g/product/10.1.0/dbs/pfile.ora`
- backup system name: `bcksys`

1. The following example illustrates the configuration on HP-UX or Solaris of an Oracle database and its recovery catalog in an Oracle Data Guard environment and using the Oracle backup set ZDB method. The location of the parameter file is also specified:

```
/opt/omni/lbin/util_oracle8.pl -config -dbname orac1
-orahome app10g/oracle10g/product/10.1.0 -prmsuser system
-prmpasswd manager -prmservice netservice1,netservice2
-rcuser rman -rcpasswd manager -rcservice catSERVICE
-stbuser system -stbpasswd manager -stbservice
netservicesb1,netservicesb2 -zdb_method BACKUP_SET -pfile
/app10g/oracle10g/product/10.1.0/dbs/pfile.ora
```

2. The following example illustrates the configuration on HP-UX or Solaris of an Oracle database and its recovery catalog in an Oracle backup set ZDB environment. The location of the parameter file is also specified:

```
/opt/omni/sbin/util_oracle8.pl -config -dbname oracl
-orahome app10g/oracle10g/product/10.1.0 -prouser system
-prmpasswd manager -prmservice net servicel,net service2
-rcuser rman -rcpasswd manager -rcservice cat service
-zdb_method BACKUP_SET -pfile
/app10g/oracle10g/product/10.1.0/dbs/pfile.ora -bkphost
bcksys
```

3. The following example illustrates how to check if an Oracle database is properly configured for ZDB in a Windows environment:

```
perl -I..\lib\perl util_oracle8.pl -chkconf_smb -dbname
oracl -bkphost bcksys
```

SEE ALSO

omnicreatedl(1), omniintconfig.pl(1M), util_cmd(1M), util_vmware.exe(1M)

util_vmware.exe

configures a VMware datacenter, checks the configuration of a VMware datacenter, and lists all configured VMware datacenters
(this command is available on systems with the Data Protector VMware Integration component installed)

util_vmware.exe

SYNOPSIS

```
util_vmware.exe -version | -help
```

```
util_vmware.exe -config
```

```
-security 1 | -security 0 LOGIN_OPTIONS
```

```
[-instance DatacenterPath -vm VMpath VM_OPTIONS [-vm VMpath VM_OPTIONS...]]
```

```
LOGIN_OPTIONS
```

```
-user Username
```

```
-password Password
```

```
[-port WebServicePort]
```

```
[-webroot WebServiceRoot]
```

```
VM_OPTIONS
```

```
-snapshots {0 | 1 | 2}
```

```
-proxy BackupProxy
```

```
-mount ProxyMountPoint
```

```
-default
```

```
util_vmware.exe -chkconf [-instance DatacenterPath]
```

```
util_vmware.exe -app
```

DESCRIPTION

Use the `util_vmware.exe` command to configure a VMware datacenter, check the configuration of a datacenter, or list all configured datacenters.

OPTIONS

-version

Displays the version of the `util_vmware.exe` command.

-help

Displays the usage synopsis for the `util_vmware.exe` command.

`-chkconf`

Checks the connection to the VMware management client. The same check is performed regardless of whether or not you specify the `-instance` option.

`-app`

Lists all configured VMware datacenters.

`-config`

Configures a VMware datacenter.

`-security`

Specifies security type (0 – standard security, 1 – integrated security). For standard security, you need to provide login information.

`-user, -password`

Applicable for standard security. Specifies which operating system user account Data Protector should use to connect to the VMware management client. This user account must have the following VMware Virtual Infrastructure privileges:

`System.View`

`System.Anonymous`

`Folder.Create`

`VirtualMachine.State.CreateSnapshot`

`VirtualMachine.State.RemoveSnapshot`

`VirtualMachine.Interact.Suspend`

`VirtualMachine.Interact.PowerOff`

`VirtualMachine.Interact.PowerOn`

`VirtualMachine.Inventory.Create`

`VirtualMachine.Inventory.Delete`

`-webroot`

Applicable for standard security. Specifies the web service entry point URI.

Default: /sdk

-port

Applicable for standard security. Specifies the TCP port number of the Virtual Infrastructure web service server. Default: 443 (SSL-encrypted HTTP), 80 (unencrypted HTTP).

By default, HTTP/S (SSL-encrypted HTTP) is used. To switch to unencrypted HTTP, configure the VMware management client to allow HTTP connections and set the Data Protector omnirc variable `OB2_VMWARE_HTTP` to 1.

If the option **-port** is not specified, the port number is read from the following file, depending on your VMware management client:

VirtualCenter Server system:

Windows registry: SOFTWARE\VMware, Inc.\VMware
VirtualCenter\

ESX Server system:

/etc/hostd/config.xml

-instance

Specifies the VMware datacenter whose virtual machines you want to configure. Provide the complete datacenter path as seen in the VMware Virtual Infrastructure.

-vm

Specifies the virtual machine you want to configure. Provide the complete virtual machine path as seen in the VMware Virtual Infrastructure.

-snapshots

Specifies the snapshot handling mode (0 – disabled, 1 – single, 2 – mixed) for the **Snapshot** backup method.

-proxy

Specifies the backup proxy system to be used for the **VCBfile** and **VCBimage** backup methods.

-mount

Specifies the mount point on the backup proxy system to be used for **VCBfile** and **VCBimage** backup methods. If this option is not specified, virtual machine disks are mounted to `Data_Protector_home\tmp`.

-default

Changes virtual machine specific settings (snapshot handling mode, backup proxy, and mountpoint) back to default.

EXAMPLES

The following environment is used to illustrate the examples:

Datacenter: /Mydatacenters/Datacenter1

VirtualCenter Server
system: virtualcenter2.company.com

Username: Administrator

Password: vmfdjkljy8767

Backup proxy: proxy2.company.com

Virtual machines: /vm/myfolder/myvm1, /vm/myfolder/myvm2

1. To specify **Standard security** for connection to the VirtualCenter Server system, log in to the VirtualCenter Server system and run:

```
util_vmware.exe -config -security 0 -username Administrator  
-password vmfdjkljy8767
```

2. To configure the virtual machine /vm/myfolder/myvm1 to use the **Single** snapshot handling mode for **Snapshot** backup sessions and the backup proxy proxy2.company.com for **VCBfile** and **VBCimage** backup sessions, log in to the VirtualCenter Server system and run:

```
util_vmware.exe -config -instance  
/Mydatacenters/Datacenter1 -vm /vm/myfolder/myvm1  
-snapshots 1 -proxy proxy2.company.com
```

3. To specify **Integrated security** for connection to the VirtualCenter Server system and to configure both virtual machines to use the default snapshot handling mode, backup proxy, and mount point, log in to the VirtualCenter Server system and run:

```
util_vmware.exe -config -security 1 -instance  
/Mydatacenters/Datacenter1 -vm /vm/myfolder/myvm1 -default  
-vm /vm/myfolder/myvm2 -default
```

SEE ALSO

`omnicreatedl(1)`, `omniintconfig.pl(1M)`, `util_cmd(1M)`, `util_oracle8.pl(1M)`

winomnimigrate.pl

helps you migrate your existing Cell Manager from a 32-bit Windows system to a 64-bit Windows system, or from a 64-bit Windows system to 64-bit Windows Server 2008

(this command is available on the Data Protector Cell Manager)

winomnimigrate.pl

SYNOPSIS

```
winomnimigrate.pl -help
winomnimigrate.pl -prepare_clients New_CM_Name
winomnimigrate.pl -configure [-keep_dcdirs]
winomnimigrate.pl -configure_clients
winomnimigrate.pl -configure_idb [-keep_dcdirs]
winomnimigrate.pl -configure_cm
```

DESCRIPTION

Winomnimigrate.pl helps you migrate your existing Cell Manager from a 32-bit Windows system to a 64-bit Windows system, or from a 64-bit Windows system to a 64-bit Windows Server 2008 system.

Run winomnimigrate.pl on the old Cell Manager and back up the IDB. Install Disk Agent on the 64-bit Windows system or Windows Server 2008 and restore your IDB to the new Cell Manager. Uninstall the Disk Agent from the new Cell Manager and install Data Protector A.06.11 Cell Manager. Finally, run the winomnimigrate.pl command again on the new Cell Manager. For a detailed procedure, see the *HP Data Protector installation and licensing guide*.

On Windows systems, you must use the perl command to run winomnimigrate.pl. For example: perl winomnimigrate.pl -configure

OPTIONS

-help

Displays the usage synopsis for the winomnimigrate.pl command.

-prepare_clients New_CM_Name

Adds the new Cell Manager's client name to the list of trusted hosts on secured clients. Secured clients accept requests on the Data Protector port (by default 5555) only from trusted hosts.

This option should be used only on the *old* Cell Manager.

`-configure`

Combines `-configure_clients`, `-configure_idb`, and `-configure_cm` options. This is the recommended way to run the `winomnimigrate.pl` command.

The option should be used only on the *new* Cell Manager.

`-keep_dcdirs`

If this option is specified, `winomnimigrate.pl` preserves references to additional DCBF directories in the migrated IDB, even if these additional DCBF directories do not exist on the new Cell Manager system. Otherwise, `winomnimigrate.pl` removes such references from the migrated IDB.

This option is only available for migration of the Cell Manager to a Windows Server 2008 system.

`-configure_clients`

Migrates the clients from the old Cell Manager to the new Cell Manager. The old Cell Manager will keep the clients in the configuration files although it will not be their Cell Manager anymore.

If any of the clients is inaccessible, it will not be imported to the new cell. You can re-run the `winomnimigrate.pl` command with this option when the clients are accessible to migrate them to the new Cell Manager.

The old Cell Manager will automatically become a client in the new cell. You can uninstall the Cell Manager component from the old Cell Manager, because it is not necessary anymore.

The option should be used only on the *new* Cell Manager.

`-configure_idb`

Configures the IDB from the old Cell Manager for use on the new Cell Manager.

The option should be used only on the *new* Cell Manager.

`-configure_cm`

Reconfigures the configuration data transferred from the old Cell Manager for use on the new Cell Manager.

The option should be used only on the *new* Cell Manager.

RETURN VALUES

0 Successfully finished.

1-4 An error occurred.

ERRORS

- | | |
|---|---|
| 1 | A generic error occurred. |
| 2 | Migration of IDB catalogs failed. |
| 3 | Configuration error (Cell Manager configuration error or an error during the import of clients) occurred. |
| 4 | Error parsing options. |

NOTES

The `winomnimigrate.pl` command is available on Windows systems only.

EXAMPLES

1. Run the following command on the old Cell Manager to add the new Cell Manager with the client name "computer.company.com" to the list of trusted hosts on secured clients:

```
perl winomnimigrate.pl -prepare_clients  
computer.company.com
```
2. To migrate the IDB, reconfigure the Cell Manager's settings, export all clients from the old Data Protector cell and import them to the new cell, run the following command on the new Cell Manager:

```
perl winomnimigrate.pl -configure
```

SEE ALSO

`ob2install(1M)`, `omnigui(5)`, `omniintro(9)`, `omnimigrate.pl(1M)`, `omnisetup.sh(1M)`, `omniusers(1)`, `upgrade_cm_from_evaa(1M)`

Section 5: Miscellaneous

omnigui

describes usage of the commands that invoke the Data Protector GUI

omnigui

SYNOPSIS

GUICommand [-help]

GUICommand

manager [*ContextOptions*] [-server *HostName*]

javadpgui [*ContextOptions*] [-server *HostName*]

mom [*ContextOptions*] [-server *HostName*]

javadpguimom [*ContextOptions*] [-server *HostName*]

xomni [*ContextOptions*] [-server *HostName*] [-display *HostName:0*]

xomnimom [*ContextOptions*] [-server *HostName*] [-display *HostName:0*]

ContextOptions

-admin

-backup

-clients

-copy

-db

-instrec

-monitor

-report

-restore

-users

DESCRIPTION

These commands are used to start all or any combination of the Data Protector GUI contexts.

To use the Data Protector GUI functionality on UNIX Cell Manager platforms on which the original Data Protector GUI is not supported, you can use the Data Protector Java GUI where it is supported, or use the `omniusers` command to create a remote user account on the Cell Manager. You can then use this user account to start the GUI and connect to the Cell Manager on any other system on which the Data Protector GUI has been installed. For details, see the `omniusers` reference page. For details on supported operating system versions or releases for the user interface, see the *HP Data Protector product announcements, software notes, and references*.

On UNIX systems, the `xomni` and `xomnimom` commands will directly start the Data Protector Java GUI.

For more information on local language support and the usage of non-ASCII characters in file names, see the online Help.

COMMANDS

WINDOWS COMMANDS:

`manager`

Starts the Data Protector GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

`javadpgui`

Starts the Data Protector Java GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

`mom`

Starts the Data Protector Manager-of-Managers GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

`javadpguimom`

Starts the Data Protector Manager-of-Managers Java GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

UNIX COMMANDS:

`xomni`

Starts the Data Protector Java GUI with all Data Protector contexts activated, or, when additional options are specified, starts only the specified Data Protector contexts.

`xomnimom`

Starts the Data Protector Manager-of-Managers Java GUI with all Data Protector contexts activated (with the exception of the Internal Database and Devices & Media contexts), or, when additional context options are specified, starts only the specified Data Protector contexts.

`xomniadmin`

Starts the Data Protector Java GUI with the Clients, Users, Reporting, and Internal Database contexts activated.

`xomnibackup`

Starts the Data Protector Java GUI with the Backup context activated.

`xomnicellmon`

Starts the Data Protector Java GUI with the MoM cell monitoring context activated.

`xomnicopy`

Starts the Data Protector Java GUI with the Object Operations context activated.

`xomniinstrec`

Starts the Data Protector Java GUI with the Instant Recovery context activated.

`xomnimm`

Starts the Data Protector Java GUI with the Devices & Media context activated.

`xomnimonitor`

Starts the Data Protector Java GUI with the Monitor context activated.

`xomnirestore`

Starts the Data Protector Java GUI with the Restore context activated.

OPTIONS

`-help`

Displays the usage synopsis for the specified command.

`-server HostName`

Connects to the specified Cell Manager.

`-display HostName:0`

Redirects the output to the display on the specified system.

`-admin`

Starts the Data Protector GUI with the Devices & Media contexts activated.

`-backup`

Starts the Data Protector GUI with the Backup context activated.

`-clients`

Starts the Data Protector GUI with the Clients context activated.

`-copy`

Starts the Data Protector GUI with the Object Operations context activated.

`-db`

Starts the Data Protector GUI with the Internal Database context activated.

- `-instrec`
Starts the Data Protector GUI with the Instant Recovery context activated.
- `-monitor`
Starts the Data Protector GUI with the Monitor context activated.
- `-report`
Starts the Data Protector GUI with the Reporting context activated.
- `-restore`
Starts the Data Protector GUI with the Restore context activated.
- `-users`
Starts the Data Protector GUI with the Users context activated.

EXAMPLES

1. `manager`
This Windows command will start the Data Protector GUI with all contexts activated.
2. `xomni -display host1:0`
This UNIX command will start the Data Protector Java GUI with all contexts activated on the system with the hostname "host1".
3. `manager -admin -monitor -report -server host3`
This Windows command will start the Data Protector GUI with the Devices & Media, Monitor, and Reporting contexts activated and will connect to the Cell Manager with the hostname "host3".
4. `xomni -admin -monitor -report -server host2`
This UNIX command will start the Data Protector Java GUI with the Devices & Media, Monitor, and Reporting contexts activated and will connect to the Cell Manager with the hostname "host2".

SEE ALSO

`ob2install(1M)`, `omniintro(9)`, `omnimigrate.pl(1M)`, `omnisetup.sh(1M)`, `omniusers(1)`, `upgrade_cm_from_evaa(1M)`, `winomnimigrate.pl(1M)`