Hewlett Packard
Enterprise

HPE Data Protector

Software Version: 10.02

Troubleshooting Guide

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development LP 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. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE 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.

Copyright Notice

© Copyright 2017 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent software updates, go to https://softwaresupport.hpe.com/patches.

To verify that you are using the most recent edition of a document, go to https://softwaresupport.hpe.com/manuals.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support Online web site at https://softwaresupport.hpe.com.

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests

- Download software patches
- Access product documentation
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract.

To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

To find more information about access levels, go to https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

Contents

Chapter 1: About Troubleshooting Data Protector

If you encounter problems when using Data Protector, you can often solve them yourself. This guide is intended to help you.

How to troubleshoot

To solve problems quickly and efficiently:

1. Make yourself familiar with the general troubleshooting information.
2. Check if your problem is described in the HPE Data Protector Help file or the troubleshooting sections of applicable guides:

   - To troubleshoot installation and upgrade, see the *HPE Data Protector Installation Guide*.

   - To troubleshoot application integration sessions, see the *HPE Data Protector Integration Guide*.

   - To troubleshoot zero downtime backup and instant recovery, see the *HPE Data Protector Zero Downtime Backup Administrator's Guide* and *HPE Data Protector Zero Downtime Backup Integration Guide*.

   - To troubleshoot disaster recovery, see the *HPE Data Protector Disaster Recovery Guide*.

3. If you cannot find a solution to your problem, report the problem to the HPE Customer Support Service.

   > **TIP:**
   > For an overview and hints on performance aspects of Data Protector, see the *HPE Data Protector Help* index: "performance".

General checks

Before proceeding, ensure that:

- You are not running into known limitations that cannot currently be overcome. For specific information on Data Protector limitations and recommendations, as well as known Data Protector and non-Data Protector problems, see the *HPE Data Protector Product Announcements, Software Notes, and References*.

- Your problem is not related to third-party hardware or software. In this case, contact the respective vendor for support.

- You have the latest Data Protector patches installed. Patches can be obtained from:
  https://softwaresupport.hpe.com/

  On how to check which Data Protector patches are installed on your system, see the HPE Data Protector Help index: "patches".

- You have appropriate operating system patches installed.

The required operating system patches are listed in the *HPE Data Protector Product Announcements, Software Notes, and References*.

- For application backups, the backup is not failing because the application is down.

- The debug logs or redo logs filesystem has not overflown.

- The application data filesystem has not overflown.

- The system is not running low on memory.

About Data Protector Log Files

If you encounter a problem using Data Protector, the information in the log files can help you determine the problem.

Location of log files

Most Data Protector log files are located in:

Windows Server 2008, Windows Server 2012: *Data_Protector_program_data*\log

Other Windows systems: *Data_Protector_home*\log

HP-UX, Solaris, and Linux systems: /var/opt/omni/log and /var/opt/omni/server/log (the latter only on HP-UX and Linux systems)

Other UNIX systems and Mac OS X systems: /usr/omni/log

Format of log files

Most Data Protector log file entries are of the following format:

time_stamp process.PID.Thread_ID source_file_info Data Protector_version log_entry_ message

Example

```
03/16/2013 8:47:00 AM INET.3048.3036 ["inetnt/allow_deny.c /main/dp61/6":467] 10.02
b330 A request 0 (BDF) came from host computer.company.com (10.17.xx.xxx) which is
not in AllowList: not proceeding with this request!
```

Contents of log files

The table below describes the Data Protector log files:

Data Protector log files

Log file	Description
debug.log	Contains unexpected conditions. While some can help you, the information is mainly used by the support organization.

inet.log	Contains local security related events for the client, such as denied requests. On UNIX systems, it contains also all requests made to the Data Protector Inet service.
enhincr.log	Contains information on enhanced incremental backup activities, for example, detailed error information for problems with the enhanced incremental backup repository.
Ob2EventLog.txt	Contains Data Protector events and notifications. The Event Log represents a centralized Data Protector event depository.
media.log	Each time a medium is used for backup, initialized, or imported, a new entry is created in this log file. The file can be used when recovering the IDB to find the medium with the IDB backup and to find out which media have been used after the last backup of the IDB.
omnisv.log	Contains information on when Data Protector services were stopped and started.
security.log	Contains security related events on the Cell Manager. Some events may be a result of normal operation and simply mean that an operation was attempted that is not allowed by a particular user. On the other hand, events can indicate that deliberate break-in attempts may be in progress.
purge.log	Contains traces of the background purge of the IDB.
PostgreSQL logs	Contain the IDB logs. The files reside on the Cell Manager in: **Windows systems:***Data_Protector_program_data*\server\db80\pg\pg_log **UNIX systems:**/var/opt/omni/server/db80/pg/pg_log
pgbouncer.log	Contains the pgBouncer logs.
Application Server logs	Contain the application server logs for components such as Scheduler and Missed Job Executions. The files reside in: **Windows systems:***Data_Protector_program_data*\log\AppServer **UNIX systems:**/var/opt/omni/log/AppServer
sanconf.log	Contains session reports generated by the sanconf command.
sm.log	Contains details on internal errors that occurred during backup and restore sessions, such as errors in parsing backup specifications.
stats-HPECloud-*year-month*.log	Contains usage log reports generated from the Cloud (Helion) gateways during cloud copy sessions. The files include details on session ID, device name, date and time, and number of requests. The files reside in:

	Windows systems: *Data_Protector_program_data*\log\Server **UNIX systems:**/var/opt/omni/log/Server
stats-Azure- *year-month*.log	Contains usage log reports generated from the Cloud (Azure) gateways during cloud copy sessions. The files include details on session ID, device name, date and time, and number of requests. The files reside in: **Windows systems:***Data_Protector_program_data*\log\Server **UNIX systems:**/var/opt/omni/log/Server
upgrade.log	This log is created during upgrade and contains upgrade core part (UCP) and upgrade detail part (UDP) messages.
DPIDBsetup_ *PID*.log (UNIX systems specific)	This log is created during upgrade and contains traces of the upgrade process.
IS_install.log	Contains a trace of remote installation and resides on the Installation Server.
sap.log, oracle8.log, informix.log, sybase.log, db2.log	Application specific logs contain traces of integration calls between the application and Data Protector. The files reside on the application systems.

About Data Protector Telemetry Files

Data Protector gathers and collects the following high-level information for telemetrics:

- Host OS version
- Data Protector components and its versions
- Devices or Media Servers - Are associated to a client in the Cell Manager. It includes the host name details where the device is attached, name of the device, library name, pool name where the media is placed, and device type.
- Device usage size - The usage size of the device.
- Schedules - The schedule telemetry exposes information grouped by backup and session types. It represents the number of full and incremental backup processes scheduled every year by backup and session types.
- Capacity Based Licensing (CBL) - CBL is leveraged to gather information on capacity. For more information, see the *HPE Data Protector Installation Guide*.
- License categories - Lists the number of licenses available in Data Protector.
- Client usage - The information is collected for each client. This information includes: Hostname, Application name and Total size of data backed up.
- Storage usage - Total data backed up on the device.

> **NOTE:**
> The customer related internal information is gathered, but the Host information is masked or replaced with a character numeric format.

> **NOTE:**
> The Cell Manager performance will not be impacted significantly during the collection of telemetry data.

About Data Protector Error Messages

Many Data Protector error messages have troubleshooting information associated with them, providing detailed explanations of errors and suggestions for correcting problems. Such messages contain an error number that can be used to access this information.

Error messages in the Data Protector GUI

Some error messages in the session output provide the error number, presented as a clickable link. If you click the link, the error message dialog displays more information about the error. Click **Details** for a detailed description of the error and suggested actions.

Sample error message dialog
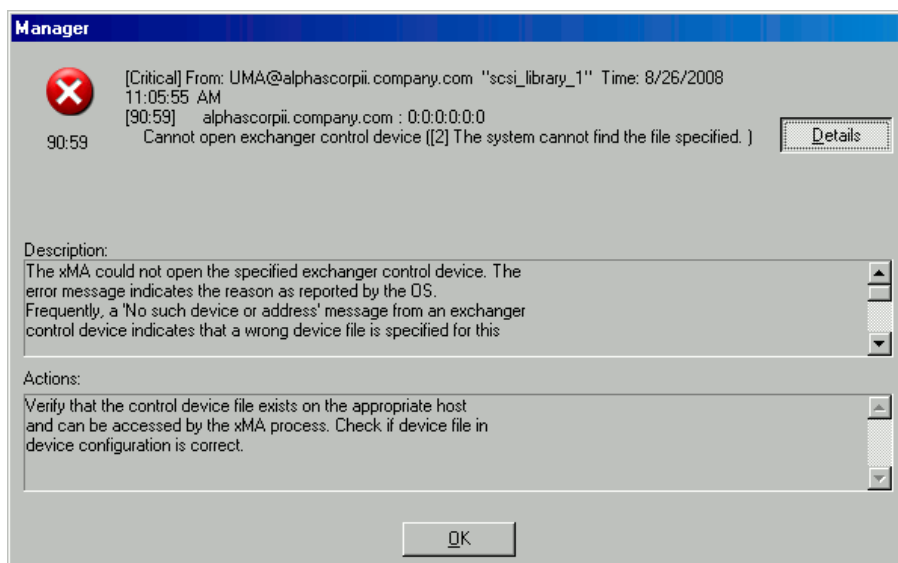
Error messages in the Data Protector CLI

If you receive an error message containing the error number in the Data Protector CLI, you can look up the error details in the troubleshooting file. This is a text file containing all Data Protector error messages, each of them with a description and possible actions.

The troubleshooting file is located on the Cell Manager:

Windows systems: *Data_Protector_home*\help\enu\Trouble.txt

UNIX systems:/opt/omni/gui/help/C/Trouble.txt

Example

```
MESSAGE:
[12:1051] Client security violation. Access denied.

DESCRIPTION:
The target host is secured and has been accessed by a host that is not on its list
of cell authorities.

ACTION:
* Check and update the client's list of cell authorities.
* In case your client has been locked out, edit the allow_hosts file manually.
```

About Data Protector Customization

Sometimes you can solve Data Protector issues by customizing its global or omnirc options.

Global options

Global options are a set of parameters, such as timeouts and limits, that define behavior of the entire Data Protector cell. They can be set on the Cell Manager.

> **NOTE:**
> Most users should be able to operate the Data Protector without changing the global options.

Global options can be set in two ways:

- Customizing the Data Protector Global Options , on page 21
- Customizing Options By Editing The Global File , on page 22

Most often used global options

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

Global option	Description
MaxSessions	Specifies the maximum number of Data Protector sessions (of any type) that can concurrently run in the cell. Default: 1000.
MaxBSessions	Specifies the maximum number of Data Protector backup sessions that can concurrently run in the cell. Default: 100.
MaxMAperSM	Specifies the maximum number of Data Protector backup devices that can be concurrently used in one backup, object copy, object consolidation, or restore session. Default: 100.

`MaxDAperMA`	Specifies the maximum Disk Agent concurrency (device concurrency) for Data Protector backup, object copy, and object consolidations sessions. Default: `32`.
`DCDirAllocation`	Determines the algorithm used for selecting the DC (Detail Catalog) directory for a new DC binary file: `Fill in sequence`, `Balance size` (default), `Balance number`. For more information on the DC directory selection algorithms, see the *HPE Data Protector Help* index: "maintenance of DCBF".
`MediaView`	Changes the fields and their order in the Media Management context.
`InitOnLoosePolicy`	Enables Data Protector to automatically initialize blank or unknown media if the loose media policy is used.
`DailyMaintenanceTime`	Determines the time after which the daily maintenance tasks can begin. Default: `12:00` (noon). For a list of daily maintenance tasks, see the *HPE Data Protector Help* index: "checks performed by Data Protector".
`DailyCheckTime`	Determines the time after which the daily check can begin. Default: `12:30 P.M.`. You can also disable the daily check. For a list of daily check tasks, see the *HPE Data Protector Help* index: "checks performed by Data Protector".
`SessionStatusWhenNoObjectToCopy` and `SessionStatusWhenNoObjectToConsolidate`	Enable you to control the session status of object copy and object consolidation sessions if there are no objects to copy or to consolidate. If the value is set to: • `0` (default), then the session will be marked as failed and a critical error will be displayed. • `1`, then the session will be marked as successful and a warning will be displayed. • `2`, then the session will be marked as successful and a normal message will be displayed.
`SetInitialMediumProtection`	Ensures that the new media is protected. The value must be set to `1` to prevent data loss during the backup or copy sessions of the unprotected media.

Omnirc options

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

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

Windows Server 2008, Windows Server 2012: *Data_Protector_program_data*\omnirc

Other Windows systems: *Data_Protector_home*\omnirc

HP-UX, Solaris, and Linux systems: /opt/omni/.omnirc

Other UNIX systems and Mac OS X systems: /usr/omni/.omnirc

How to use omnirc options?

To set omnirc options:

1. Depending on the platform, copy the template `omnirc.tmpl` or `.omnirc.TMPL` to `omnirc` or `.omnirc`, respectively.
2. Edit the file `omnirc` or `.omnirc`. Uncomment the line of the desired option by removing the "#" mark, and set the desired value.
3. After setting the options:

   - When creating the `omnirc` file (either by copying or by using an editor), verify its permissions. On UNIX systems, permissions will be set according to your umask settings and may be such that some processes may be unable to read the file.

     Set the permissions to `644` manually.

   - When changing the `omnirc` file, restart the Data Protector services/daemons on the Data Protector client where you modified the omnirc file. This is mandatory for the crs daemon on UNIX systems and recommended for Data Protector CRS and Inet services on Windows systems. Specifically on Windows, restarting is not required when adding or changing entries, only when removing entries (or renaming the file).

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

On how to set omnirc options during disaster recovery, see the *HPE Data Protector Disaster Recovery Guide*.

Most often used omnirc options

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

Omnirc option	Description
OB2_SHOW_BTRFS_MOUNTS	To backup the explicitly mounted volumes, you need to export the omnirc variable (OB2_SHOW_BTRFS_MOUNTS) that will force inet to send all volumes back. The OB2_SHOW_BTRFS_MOUNTS variable needs to be set to 1.
OB2_ENCRYPT_PVT_KEY	To use encrypted private keys for secure remote installation, set this option to 1 on the Installation Server. The default value is 0 (not set).
OB2_ENCRYPT_MEDIUM_STRICT	Enables you to control whether to strictly use drive-based encryption in backup, object consolidation, object copy, and automated media copy sessions. The option is only considered when the GUI option Drive-based encryption is selected for the current session. If the value is set to 1, then: • if the selected tape drive does not support encryption, the session will be aborted by default. • if the selected tape drive supports encryption, but the medium in it does not support encryption, a mount request will be issued (in case of a standalone tape drive) or the next available medium will be checked for encryption support first and eventually a mount request will be issued if no media with encryption support are found (in case of a tape library). • if the selected tape drive and the medium in it both support encryption, the data writing operation will be performed in an encrypted mode. If the value is set to 0, then: • if the selected tape drive does not support encryption, the data writing operation will be performed in an unencrypted mode. • if the selected tape drive supports encryption, but the medium in it does not support encryption, the data writing operation will be performed in an unencrypted mode. • if the selected tape drive and the medium in it both support encryption, the data writing operation will be performed in an encrypted mode.
OB2_ENCRYPT_FORCE_FORMAT	Enables you to control the formatting behavior when using Data Protector drive-based encryption. If the value is set to: • 0 (default), a formatting operation aborts. • 1, a formatting operation is forced.
OB2_AES_COMPATIBILITY_MODE	Data restored from AES encrypted backups created using HPE Data Protector versions (DP 7.03_108, 8.14, 8.14_209, 8.14_210, 9.03, and 9.04) is not useful. Correcting this requires a manual intervention. To restore AES-256 software encrypted backups created using

	HPE Data Protector versions (DP 7.03_108, 8.14, 8.14_209, 8.14_210, 9.03, and 9.04), set this option to 1 in the omnirc file on the client that needs to be restored.
	To restore AES-256 software encrypted backups created using other HPE Data Protector versions, set this option to 0 (or) remove this option from the omnirc file, and restart the inet daemon on that specific client.
OB2FORCEPOSTEXEC	Enables you to force the execution of post-exec script.
	If the value is set to:
	• 0 (default), the execution of post-exec script is not enforced.
	• 1, the post-exec script is always executed, even if the pre-exec script fails.
OB2BLKPADDING_n	Specifies the number of empty blocks written to media at the initialization time. When copying media, this helps to prevent the target media from running out of space before all data is copied.
OB2DEVSLEEP	Changes the sleep time between each retry while loading a device.
OB2ENCODE	Enables you to always use data encoding, regardless of how the backup options are set in the backup specification.
OB2OEXECOFF	Enables you to restrict or disable any object `pre-` and `post-exec` scripts defined in backup specifications for a specific client.
OB2REXECOFF	Enables you to disable any remote session `pre-` and `post-exec` scripts for a specific client.
OB2CHECKCHANGETIME (UNIX systems specific)	Defines when to use the "last inode change" time for incremental backups.
OB2INCRDIFFTIME (UNIX systems specific)	Specifies an "incremental latency" period that is enforced when checking the "last inode change" time with incremental backups. This option takes effect only when the `OB2CHECKCHANGETIME` option is set to 2.
OB2RECONNECT_ACK	Defines how long Data Protector should wait for a message of acknowledgment (default: 1200 seconds). If the agent does not get an acknowledgment in this time, it assumes that the socket connection is no longer valid.
OB2RECONNECT_RETRY	Defines how long a Data Protector Disk Agent or Media Agent should try to reconnect after a connection failure. Default: 600 seconds.
OB2SHMEM_IPCGLOBAL	This option should be set to 1 on HP-UX clients that have both the Disk Agent and a Media Agent installed in case the following error occurs during backup:
	`Cannot allocate/attach shared memory (IPC Cannot Allocate Shared Memory Segment)`

	`System error: [13] Permission denied) => aborting`
OB2VXDIRECT	Enables direct reading (without cache) for Advanced VxFS filesystems, which improves performance.

OB2ODIRECT_BACKUP	This option configures Data Protector to use the `O_DIRECT` flag when opening files for reading and writing, thus avoiding the use of the file system cache. This option is only applicable to FS backups, on Linux and AIX.
	
	`OB2ODIRECT_BACKUP=0|1`
	
	`Default:0`

OB2ODIRECT_RESTORE	This option configures Data Protector to use the `O_DIRECT` flag when opening files for writing, thus avoiding the use of the file system cache. Since the cache is not used, this may lead to slower restore speed. This option is only applicable to FS restores, on Linux and AIX. Different filesystems are supported as per the HPE Data Protector Platform and Integration Support Matrix.
	
	`OB2ODIRECT_RESTORE=0|1`
	
	`Default:0`

OB2ODIRECT_RESTORE_ MINIMUM_SIZE	When this option is set, restore will use `O_DIRECT` flag only if the file size is greater than the specified value. OB2ODIRECT_RESTORE_MINIMUM_SIZE=<min_file_size_in_bytes> `Default:0`
OB2_CLP_MAX_ENTRIES (Windows systems specific)	Sets the number of entries the Windows NTFS Change Log Provider can hold in memory. The amount of memory that the Change Log Provider uses depends on the filename length of all entries. Minimum: `15 000` entries (this represents approximately 25 MB of RAM). Default: `100 000` entries (approximately 120 MB of RAM). If the number is changed to a smaller value so that not all entries can be kept in memory, the backup time may increase.
OB2_CLP_CREATE_EI_ REPOSITORY (Windows systems specific)	Specifies whether the Windows NTFS Change Log Provider creates the Enhanced Incremental Repository the first time it runs. Set this option to `1` to create the Enhanced Incremental Repository. Default: `0` (not created). With this option set, the backup time increases, since the Enhanced Incremental Repository is always updated. However, this enables a fallback to a conventional enhanced incremental backup.
OB2_ENHINC_SQLITE_ MAX_ROWS	Specifies the maximum number of rows in the enhanced incremental backup database (SQLite on Windows, HP-UX, and Linux systems) that can be stored in the internal memory cache. If the backup consists of a large number (millions) of directories, this option is used to improve the Disk Agent performance by increasing the maximum number of rows stored in the cache.

OB2SANCONFSCSITIMEOUT (Windows systems specific)	Sets the timeout for `sanconf` related operations. It must be set on all clients affected by `sanconf` before running the command. Default: `20` seconds.
OB2PORTRANGE	Limits the range of port numbers that Data Protector uses when allocating listen ports dynamically. This option is typically set to enable the administration of a cell through a firewall. Note that the firewall needs to be configured separately and that the specified range does not affect the `Inet` listen port.
OB2PORTRANGESPEC	Limits the range of port numbers that specific Data Protector processes use. Note that the firewall needs to be configured separately and that the specified range does not affect the Inet listen port. For examples of port range configuration, see the *HPE Data Protector Help* index: "firewall support".
OB2HSMBACKUPALL	To backup files with offline attribute, set this option to 1. The default value is 0 (not set) and therefore, the backup process skips all files with offline attribute. After you enable this option to 1, the Disk Agent checks for all files with offline attribute on Storage Optimizer, and performs the backup operation. In case of a file with a reparse point, only a stub backup is performed on Windows operating systems. Storage Optimizer creates soft links in case of Linux operating systems. In case of files with offline attribute that do not have a reparse point, it depends on the Hierarchical Storage Management (HSM) product whether a data re-call and re-hydration is performed before backing up. This can cause high I/O traffic and system overload. For more information, see HSM product documentation. **NOTE:** Reparse point refers to the location from where the external files are considered.

Customizing the Data Protector Global Options

In the Data Protector global options file, you can modify values of global options or add new ones.

Prerequisites

- Your user account must be a member of a Data Protector `Admin` user group.

Setting the global options using GUI

Steps

To set global options using the GUI:

1. In the Context List, click **Internal Database**.

2. In the Scoping Pane, under **Internal Database**, click **Global Options**.

   In Results area, the **Data Protector Global Options** table is displayed, consisting of six columns:

   - Group - represents the contextual section the option belongs to.

   - In use - indicates the status of an option. Selected options are active, while the empty check box indicates the inactive options that are commented out in the global options file.

   - Name

   - Origin - indicates the file which the option is loaded from.

   - Value - represents the value to which the option is currently set.

   - Description - informs you how to use the option.

3. To modify an option - in the Results Pane, in the Value column - click on the value you want to change, click the Edit icon and enter a new one. Click **Save** to save the option.

   To add an option, click the Add icon , fill in the dialog box with option parameters and click **Add**.

4. At the top of the Results Pane, click the Save icon .

You can also modify multiple rows before saving.

To change the table appearance, use the filters in the table headings.

In case anything goes wrong during the saving process, a copy of the original global options file named `global.old` is made in the global options folder.

Customizing Options By Editing The Global File

Besides using the GUI, you can edit the `global` file in a text editor to set the Data Protector global options.

> **CAUTION:**
> HPE recommends using the GUI to set the global options, as it ensures validation of changes upon saving and reduces the chance of issues arising from the out-of-range or invalid settings, accidental deletions, typographical or spelling errors.

Steps

1. Open any text editor

2. In the text editor, open the `global` file, located in the default Data Protector server configuration directory, in the `options` subdirectory.

3. To activate an option, remove the # mark in front of its name and set it to the desired value.

4. Save the file in the Unicode format.

Chapter 2: Troubleshooting Networking and Communication

Hostname resolution problems

An important aspect of the TCP/IP configuration process is the setup of a hostname resolution mechanism.

For successful communication, host A needs to resolve host B by its fully qualified domain name (FQDN). Resolving a host means that host A can interpret the FQDN of host B and determine its IP address.

Hostname resolution must be provided at least for the following:

- Each client must be able to resolve the address of the Cell Manager and the clients with Media Agents.
- The Cell Manager must be able to resolve the names of all clients in the cell.
- The MoM Server, if used, must additionally be able to resolve the names of all Cell Managers in the MoM environment.

Checking the TCP/IP setup

Once you have the TCP/IP protocol installed, you can use the `ping` and `ipconfig` (Windows systems) or `ifconfig` (UNIX systems) utilities to verify the TCP/IP configuration.

Note that on some systems the `ping` command cannot be used for IPv6 addresses, the `ping6` command should be used instead.

Testing DNS resolution

Test DNS resolution among hosts by running:

`omnicheck -dns`

This will check all DNS connections needed for normal Data Protector operation.

For more information on the command, see the `omnicheck` man page or the *HPE Data Protector Command Line Interface Reference*.

Connected system presents itself as client X

Problem
The response to the `omnicheck` command is:
client_1 connects to *client_2,* but connected system presents itself as *client_3*
The `hosts` file on `client_1` is not correctly configured or the hostname of `client_2` does not match its DNS name.

Action
Consult your network administrator. Depending on how your environment is configured to perform name resolution, the problem needs to be resolved either in your DNS configuration or the `hosts` file on the affected clients, located in: **Windows systems:***%SystemRoot%*`\system32\drivers\etc` **UNIX systems:**`/etc`

Client A failed to connect to client B

Problem
The response to the `omnicheck` command is: *client_1* `failed to connect to` *client_2* The `hosts` file on `client_1` is not correctly configured or `client_2` is unreachable (for example disconnected).
Action
Configure the `hosts` file correctly or connect the disconnected system.

Cannot connect to client X

Problem
The response to the `omnicheck` command is: *client_1* `cannot connect to` *client_2* This means that the packet has been sent, but not received because of a timeout.
Action
Check for network problems on the remote host and resolve them.

Checking time settings in the cell

Problem
Data Protector uses timestamps extensively for communication between various cell components (Cell Manager, clients). If the system clocks on the Cell Manager and clients differ significantly, such as weeks or even months (for example, if you changed settings for testing purposes, the system clock was not updated after a restore of a virtual machine and so on), unexpected results may occur, including communication errors, failures to search or restore backups, and similar.

Action
Check the system time settings and make sure that the system clocks do not differ significantly. Note that if the clock on the client is not synchronized with the clock on the Cell Manager, the certificate may become invalid, thus resulting in failed authentication. For example, when the clock on the Cell Manager is ahead of the clock on the client, the certificate created during installation is not yet valid for the client attempting to connect to it.

Recovering from power outages

The IDB is not reachable after a system recovery

Problem
The database is capable to recover into a consistent state after such unexpected events as power outages, severe operating system or hardware failures, and so on. However, the first access to the database (after the system recovery) might fail with an internal error. This is a temporary problem which occurs only once.
Action
Reaccess the database.

HPE Data Protector sessions are actually not running but remain marked as `In Progress`

Problem
In the Internal Database context of the Data Protector GUI, the session status of one or more Data Protector sessions that are actually not running remains marked as `In Progress`.
Action
1. Close the Data Protector GUI. 2. Execute the `omnidbutil -clear` command to set the status of all sessions that are actually not running but are marked as `In Progress` to `Failed`. 3. Restart the Data Protector GUI.

The hpdp-idb-cp service fails to start

Problem
The hpdp-idb-cp service does not start.

Action

1. Stop the Data Protector services.
 	
2. Delete the following file:
 	
    Windows systems: *Data_Protector_program_data*\log\hpdp-idb-cp.pid
 	
    UNIX systems: /var/opt/omni/log/pgbouncer.pid
 	
3. Restart the Data Protector services.

Novell Open Enterprise Server (OES) problems

TSA login denied

Problem
The following message is displayed: From: VRDA@computer.company.com "/media/nss/NSS_VOLUME_5" TSA: Cannot connect to Target Service (login denied).
Action
Run the HPLOGIN utility /usr/omni/bin/hplogin with the correct user credentials.

Other problems

Client fails with "Connection reset by peer"

Problem
On Windows systems, default configuration parameters of the TCP/IP protocol may cause problems with connectivity. This may happen due to a high network or computer use, unreliable network, or especially when connecting to a different operating system. The following error is reported: [10054] Connection reset by peer.
Action
You can configure the TCP/IP protocol to use 8 instead of the default 5 retransmissions. It is better not to use higher values because each increment doubles the timeout. The setting applies to all network connections, not only to connections used by Data Protector. If the Cell Manager is running on a Windows system, apply the change on the Cell Manager system first. If the problem persists or if the Cell Manager is running on a UNIX system, apply the change to

the problematic Windows clients.

1. Add the `DWORD` parameter `TcpMaxDataRetransmissions` and set its value to `0x00000008(8)` under the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\Tcpip\Parameters`

2. Restart the system.

> **CAUTION:**
> Making a mistake when editing the registry may cause your system to become unstable or even unusable.

Client fails with "The client is not a member of any cell"

Problem

When performing a Data Protector operation on a client and the Cell Manager information is not found on the client, the operation fails with the following error:

`The Client is not a member of any cell.`

Action

- If the client is listed in the Clients context of the Data Protector GUI:

  1. In the Clients context, expand **Clients**, right-click the client, and click **Delete**.
  2. A dialog asks you if you also want to uninstall Data Protector from the client. Click **No**.
  3. Right-click **Clients** and click **Import Client**.
  4. Specify the client and click **Finish**.

- If the client is not listed in the Clients context:

  1. In the Clients context, right-click **Clients** and click **Import Client**.
  2. Specify the client and click **Finish**.

Excessive logging to the inet.log file

Problem

If clients are not secured and the Cell Manager is configured in the HPE Serviceguard environment or has multiple names or IP addresses, the `inet.log` file may contain many entries of the following type:

`A request 3 (vbda.exe) came from host computer.company.com which is not a cell manager of this client.`

This happens because a client that is not secured recognizes only the primary hostname of the Cell Manager. Requests from any other client are allowed, but are logged to the `inet.log` file.

Action

Secure the client. Requests from the clients listed in the `allow_hosts` file will not be logged to `inet.log`. Requests from other clients will be denied.

If this workaround is for any reason not possible in your environment, you can secure the clients and specify * as an IP address range for the systems you want to allow access. This means that your clients will accept requests from all systems (any IP address) and will practically not be secured, but you will resolve the excessive logging issue.

> **IMPORTANT:**
> All possible hostnames for the Cell Manager nodes should be listed in the `allow_hosts` file on each client that is being secured. This enables access to the client also in case of a failover. If you accidentally lock out a client, you can manually edit the `allow_hosts` file on that client.

Chapter 3: Troubleshooting Data Protector Services and Daemons

Introduction

The Data Protector services (Windows systems) and daemons (UNIX systems) run on the Cell Manager. Run the `omnisv -status` command to check whether services/daemons are running.

If the Data Protector services/daemons seem to be stopped or have not been installed on the target Data Protector client, make sure that you do not have a name resolution problem.

A list of Data Protector processes

The following table shows which processes run while Data Protector is idle or performing some basic operations, such as a backup, a restore, or a media management session.

		Always	Backup	Restore	Media management
Cell Manager	**Windows**	omniinet.exe mmd.exe crs.exe kms.exe hpdp-idb hpdp-idb-cp hpdp-as	bsm.exe	rsm.exe	msm.exe
	UNIX	mmd crs kms hpdp-idb (postgres) hpdp-idb-cp (pgbouncer) hpdp-as (standalone.sh)	bsm	rsm	msm
Disk Agent client	**Windows**	omniinet.exe	vbda.exe	vrda.exe	
	UNIX		vbda	vrda	

Media Agent client	Windows	omniinet.exe	bma.exe	rma.exe	mma.exe
	UNIX		bma	rma	mma

Problems starting Data Protector services on Windows

You do not have permission to start the services

Problem

The following error displays:
 	
`Could not start the ServiceName on SystemName.`
 	
`Access is denied.`

Action
The system administrator should grant you the permission to start, stop, and modify services on the system that you administer.

Changed service account properties

Problem

If the service account does not have the permission to start the service or if the service account properties (for example, the password) have been changed, the following error displays:
 	
`The Data Protector Inet service failed to start due to the following error:`
 	
`The service did not start due to a logon failure.`

Action
In the **Windows Control Panel** > **Administrative Tools** > **Services**, modify the service parameters. If the problem persists, contact your system administrator to set up the account with appropriate permissions. The account should be a member of the `Admin` group and should have the `Log on as a service` user right.

A specific service has not been found

Problem
The location of the service is registered in the `ImagePath` registry key. If the executable does not

exist in the location specified under this key, the following error displays: `Could not start the `*`ServiceName`*` on `*`SystemName`*`. The system can not find the file specified!`
Action
Reinstall Data Protector on the Cell Manager, preserving the IDB.

MMD fails upon starting the CRS service

Problem
If the Data Protector CRS service fails to start and `mmd.exe` invokes a `Dr.Watson` diagnosis, the database log files are probably corrupted.
Action
1. Delete the `mmd.ctx` file from the default Data Protector Internal Database directory. 2. Restart the services using the `omnisv -stop` and `omnisv -start` command.

Problems starting Data Protector daemons on UNIX

The following daemons run on the UNIX Cell Manager:

- In the directory `/opt/omni/lbin`:

  - Data Protector CRS daemon: `crs`

  - Data Protector IDB daemons: `hpdp-idb (postgres)`, `hpdp-idb-cp (pgbouncer)`, `hpdp-as (standalone.sh)`

  - Data Protector Media Management daemon: `mmd`

Normally, these daemons are started automatically during the system startup.

The Data Protector Inet process (`/opt/omni/lbin/inet`) is started by the system inet daemon when an application tries to connect to the Data Protector port (by default 5565).

To manually stop, start, or check the status of the Data Protector daemons, log on to the Cell Manager as `root` and from the `/opt/omni/sbin` directory, run:

- `omnisv -stop`
- `omnisv -start`
- `omnisv -status`

Data Protector Cell Manager daemon could not be started

Problem
The output of the `omnisv -start` command is: `Could not start the Cell Manager daemon.`
Action
See the `omni_start.log` file for details. The file resides at the default Data Protector temporary files directory. Ensure that the following configuration files exist: • `/etc/opt/omni/server/options/global` • `/etc/opt/omni/server/options/users/UserList` • `/etc/opt/omni/server/options/ClassSpec`

The hpdp-idb service fails to start, reporting shared memory deficiency

Problem

On HP-UX systems, the hpdp-idb service fails to start and the following error is logged to the PostgreSQL log file (`/var/opt/omni/server/db80/pg/pg_log`):
 	
`FATAL: could not create shared memory segment: Not enough space`
 	
`DETAIL: Failed system call was shmget(key=7112001, size=2473459712, 03600).`
 	
The issue appears because the hpdp-idb service cannot obtain the requested amount of shared memory due to memory fragmentation on the system.

Action
Restart the system to defragment the memory.

MMD fails upon starting the CRS service

Problem
The Data Protector CRS service fails to start and the following error is displayed: `[Critical] From: CRS@computer.company.com "" Time: 03/04/13 11:47:24 Unable to start MMD: Unknown internal error..`

The database log files are probably corrupted.

Action

1. Delete the `mmd.ctx` file from the default Data Protector Internal Database directory.
2. Restart the services using the `omnisv -stop` and `omnisv -start` command.

Other problems with Data Protector processes

Data Protector performance on UNIX is impacted if Name Server Caching is disabled

Problem

Data Protector performance on UNIX systems can be negatively affected if the Name Server Caching (nscd) daemon is disabled.

UNIX and Windows systems do not have a default name server cache. Data Protector operations create many DNS requests which may be impacted if the Name Server Caching (nscd) daemon is disabled.

Action

1. Ensure that the Name Server Caching (nscd) daemon is enabled and configured.

   The configuration of nscd varies by platform. For more information, see your platform's documentation.

2. Check the DNS settings and ensure that the DNS search order is correctly configured with the local domain first in the `etc/resolv.conf` file.

3. Restart the services using the `omnisv -stop` and `omnisv -start` command.

When performing a backup, the backup session stops after a certain period of time and the BSM stops responding

Problem

This issue may be caused by firewall closing an inactive connection.

Action

Ensure that the connection remains active so that the firewall does not close it. Set the following omnirc options:

```
OB2IPCKEEPALIVE=1
OB2IPCKEEPALIVETIME=number_of_seconds
```

```
OB2IPCKEEPALIVEINTERVAL=number_of_seconds
```

OB2IPCKEEPALIVETIME specifies how long the connection may remain inactive before the first keep-alive packet is sent and OB2IPCKEEPALIVEINTERVAL specifies the interval for sending successive keep-alive packets if no acknowledgment is received. The options must be set on the Cell Manager system.

Chapter 4: Troubleshooting User Interface

Graphical user interface problems

Data Protector graphical user interface problems are usually a result of services not running or not installed, or problems with network communication.

Connectivity and accessibility problems

No permission to access the Cell Manager

Problem
The following message displays:

`Your Data Protector administrator set your user rights so that you do not have access to any Data Protector functionality.`
 	
`Contact your Data Protector administrator for details.`

Action
Contact the Data Protector administrator to add you as a user and give you appropriate user rights in the cell. On how to configure user groups, see the *HPE Data Protector Help* index: "user groups".

Connection to a remote system refused

Problem
On Windows, the response of the `telnet` *hostname* `5565` command is `Connection refused`.
Action
• If the `Data Protector Inet` service is not running on the remote system, run the `omnisv -start` command to start it. • If Data Protector is not installed on the remote system, install it.

Inet is not responding on the Cell Manager

Problem
The following message displays:

Cannot access the system (inet is not responding). The Cell Manager host is not reachable, is not up and running, or has no Data Protector software installed and configured on it.

Action

If the problem is not communication between the systems, check the installation using `telnet`.

Some components may not have been installed (properly). Check the installation steps in the *HPE Data Protector Installation Guide*.

If the installation is correct, run the `omnisv -status` command to check whether the services on the Cell Manager are running properly.

Unable to start the filesystem browse agent

Problem

The following error occurs when a Data Protector user with sufficient privileges tries to save the backup specification and start the backup:

`Unable to start filesystem browse agent`

Action

The Data Protector user must have the impersonation details configured properly in Inet.

Command-line interface problems

Data Protector commands cannot be invoked

Problem

After you attempt to invoke a Data Protector command in the Command Prompt or Terminal window, the command-line interpreter reports that the command cannot be found.

Action

Extend the value of the `PATH` environment variable in your operating system configuration with the paths to the command locations. This action enables you to invoke the Data Protector commands from any directory. If the value has not been extended, the commands can only be invoked from their locations, listed in the `omniintro` reference page in the *HPE Data Protector Command Line Interface Reference* and the `omniintro` man page.

Chapter 5: Troubleshooting Backup and Restore Sessions

Full backups are performed instead of incrementals

You specified an incremental backup, but a full backup is performed. There are several possible reasons for this behavior:

No previous full backup

Problem
Before performing an incremental backup of an object, Data Protector requires a full backup as a base for comparison to determine which files have changed and consequently need to be included in the incremental backup. If a protected full backup is not available, a full backup is performed.
Action
Ensure that a protected full backup of the object exists.

The description has changed

Problem
A backup object is defined by the client, mount point, and description. If any of these three values changes, Data Protector considers it as a new backup object and performs a full backup instead of an incremental.
Action
Use the same description for full and incremental backups.

Trees have changed

Problem
A protected full backup already exists but with different trees than the incremental backup. There are two possible reasons for this:

- You have changed the trees in the backup specification of the protected full backup.
- You have created multiple backup specifications with the same backup object but different trees specified for the backup object.

Action

If you have multiple backup specifications with the same backup object, change the (automatically generated) universal description of the backup object. Data Protector will consider them as new objects and a full backup will be run. After a full backup is performed, incremental backups will be possible.

The backup owner is different

Problem
If your backups are configured to run as private, the user starting the backup is the owner of the data. For example, if user A performs a full backup and user B tries to start an incremental backup, the incremental backup will be performed as a full backup. This is because the data for user A is private and cannot be used as a base for user Bs incremental backup.
Action
Specify backup ownership in the advanced backup specification options. The backup owner should be in the Admin user group. This user will become the owner of all backups based on this backup specification, regardless of who actually starts the backup session. For instructions, see the *HPE Data Protector Help* index: setting backup options   .

Enhanced incremental is not performed after the upgrade

Problem
This problem may occur on Windows, HP-UX, and Linux systems. If you upgraded Data Protector from version A.06.11, the old enhanced incremental backup repository cannot be used with the new product version anymore. Therefore, a full backup is performed. During a the full backup, a new enhanced incremental backup repository is created at the following location: **Windows systems:**`Data_Protector_home`\enhincrdb **UNIX systems:**`/var/opt/omni/enhincrdb`
Action
Run the full backup. The new enhanced incremental backup repository will be created and you will be able to perform enhanced incremental backups.

A ZDB filesystem backup with Enhanced Incremental backup results in a full backup

Problem
A ZDB filesystem backup with the **Enhanced incremental backup** option enabled will result in full backup, if the ZDB is configured to add the **session ID** directory to the mount path.

Action
Use **Hostname** option for directories to be added to the mount path under **Backup system** option section. Ensure that mount path is free before the next session by using **Automatically dismount filesystems at destination mountpoints** option or be sure that **Leave the backup system enabled** is not selected.

Data Protector fails to start a session

Interactive session fails to start

Problem
Every time a backup is started, the permission to start a backup session is required and checked for the user who is currently running Data Protector. If the user does not have this permission, the session cannot be started.

Action
Make sure the user is in a user group with appropriate user rights.
On how to configure user groups, see the *HPE Data Protector Help* index: user groups   .

Scheduled sessions no longer run

Problem
Scheduled sessions no longer run since the Data Protector system account, which is supposed to start scheduled sessions, is not in the `Admin` user group on the Cell Manager.
This account is added to the Data Protector Admin group on the Cell Manager at installation time. If this is modified and the permission for this account is removed, or if the service account changes, scheduled sessions no longer run.

Action
Add the Data Protector account to the `Admin` user group on the Cell Manager.

Session fails with status No licenses available

Problem
A backup session is started only after Data Protector has checked the available licenses. If no licenses are available, the session fails and Data Protector issues the session status `No licenses available`.

Action
Obtain information on available licenses by running:
`omnicc -check_licenses -detail`
Request new licenses and apply them. For licensing details, see the *HPE Data Protector Installation Guide*.

Scheduled backups do not start (UNIX systems specific)

Problem
On a UNIX system, scheduled backups do not start.
Action
Stop and start the Data Protector daemons by running `omnisv -stop` and `omnisv -start`.

Mount request is issued although media are in the device

During a backup session, Data Protector issues a mount request, although media are available in the backup device. There are several possible reasons for this:

The media in the device are in a media pool that has the Non Appendable policy

Problem
Although there is still available space on the media, the media will not be used because of the `Non Appendable` policy of the pool.
Action
Modify the media pool policy to `Appendable` to enable the appending of backups until the media are full.

The media in the device are not formatted

Problem
By default, media are not formatted automatically. If no formatted media are available, a mount request is issued.

Action
Format the media. For instructions, see the *HPE Data Protector Help* index: formatting media   .

The media in the device are different from those in the preallocation list

Problem
The media in the device are formatted but are different from those in the preallocation list of the backup specification, and the media pool specified has the `Strict` policy. If you use a preallocation list of media in combination with the `Strict` media policy, the exact media specified in the preallocation list need to be available in the device when a backup is started.
Action
- To use media available in the device in combination with the preallocation list, modify the media pool policy to `Loose`.   - To use any available media in the device, remove the preallocation list from the backup specification. Do this by changing backup device options in the backup specification.

Mount request is issued for a file library

File library device disk full

Problem
When using a file library device, you may receive a mount request with the following message: `There is no disk space available for file library File Library Device. Add some new disk space to this library.`
Action
Create more space on the disk where the file library is located: - Free some space on the disk where the files are being backed up.   - Add more disks to the system where the file library device resides.

File name problems

File names or session messages are not displayed correctly in the Data Protector GUI

Problem
Some file names or session messages containing non-ASCII characters are displayed incorrectly. This happens when an inappropriate character encoding is used to display file names and session messages in the Data Protector GUI.
Action
Specify the appropriate encoding. From the View menu, select **Encoding** and select the appropriate coded character set.

Cluster problems

IDB services are not synchronized

Problem
On UNIX systems, when performing a restore of the IDB to a different location in an HPE Serviceguard environment and one or more cluster nodes are offline, the IDB services are not synchronized for all nodes after the session completes.
Action
To synchronize the location of the IDB data files for all nodes in a cluster environment, execute the `omnidbutil -sync_srv` command on the active cluster node.

An incremental filesystem backup of a cluster shared volume using the Windows NTFS Change Log Provider falls back to a full backup after a cluster failover

Problem
When performing an incremental filesystem backup of a cluster shared volume that has the option **Use native Filesystem Change Log Provider if available** selected in a backup specification, a full backup is performed instead and the following error message is displayed:
`[Major] From: VBDA@Host Name "F:" Time: Date Time`

> The Change Log Provider could not use the Directory Database. This session will
> use the normal file system traversal.

Action

To make sure that incremental backups are correctly performed, create a symbolic link of the Change Log Provider database to a separate cluster shared volume as follows:

1. Select a shared disk to which you can direct the Change Log Provider database for shared volumes. In case of the Data Protector cluster Cell Manager, you can choose the Data Protector shared disk.

2. Create a directory on the shared disk, for example: `E:\Omniback\clp`.

3. Go to the directory *Data_Protector_home*`\clp` and create a symbolic link to the created directory.

    For example, to back up a shared disk `J`, execute

    `mklink /D J E:\Omniback\clp\J`

    where `E:\Omniback\clp\J` is a symbolic link created for a shared disk `J`, and `E` is a cluster shared volume accessible from the other cluster nodes.

Create the Change Log Provider database link for the shared volume on all cluster nodes on which incremental backups are performed after a cluster failover.

Restore problems if the Cell Manager is configured in a cluster

Problem

A backup with a cluster-aware Data Protector Cell Manager was performed with the `Restart backup of all objects` backup option enabled. A failover occurred during the backup and the backup session was restarted on another cluster node and successfully finished. When trying to restore from the last backup, the following error is reported although the session finished successfully:

`You have selected a version that was not successfully completed. If you restore from such a backup, some or all the files may not be restored correctly.`

If the system times on the Cell Manager cluster nodes are not synchronized, it is possible that the failed backup has a newer timestamp than the restarted backup. When selecting data for restore, the last backup version is selected by default, resulting in a restore from the failed backup.

Action

To restore from the last successful backup, select the correct backup version for restore.

To prevent such errors, it is recommended to configure a time server on your network. This will ensure automatic synchronization of the system times on your Cell Manager cluster nodes.

Backup of CONFIGURATION object of a Microsoft Cluster Server node fails

Problem

On a Windows Server 2008 or Windows Server 2012 system, backup of the CONFIGURATION object on a cluster node fails with the following error:
 	
`[Minor] From: VBDA@computer.company.com "CONFIGURATION:" Time:` *Date Time*
 	
`[81:141] \Registry\0.Cluster`
 	
`Cannot export configuration object: (Details unknown.) = backup incomplete`

Action
Restart the Data Protector Inet service under the user account that is used to run Cluster Service, and restart the backup.

IDB restore on HP-UX and Linux Cell Managers

The IDB restore could fail on HP-UX and Linux cell managers. There are several possible reasons for this behavior and are outlined in this section.

IDB restore on a different cell manager could fail

Problem
IDB restore on a different cell manager could fail with the message: `Recovery of the Internal Database failed.`
Action
Change the user ID and group ID of the Operating System user on the cell manager where restore fails to match the user ID and group ID of the Operating System user on the cell manager where IDB backup was taken.

IDB restore fails at the end of a restore process

Problem
IDB restore fails at the end of restore process with the message: `cannot execute omnidbutil -clear command`
Action

Problem

This could happen under the following circumstances in a HP-UX cell manager: When restoring to a different cell manager or on the same cell manager, but postgres passwords have changed after the backup session was restored or after a fresh cell manager installation.

> **NOTE:** In a Linux environment, restore will complete successfully. This is because Linux mostly uses Operating System authentication on databases in contrast to HP-UX, which uses password authorization and in this case passwords files are not restored correctly. However the workaround should be applied in the Linux environment too, to have the correct password files.

Steps

1. Restore only the configuration files to another location `<restore-conf>` up to the point in time you are planning to restore whole IDB.

2. Restore the whole IDB but don't choose to restore DCBFs or else restore the whole DCBFs to the original location.

3. Save a backup of `/etc/otp/omni/server/idb/idb.config` to `idb.config.bkp`

4. Perform file copies from the `<restore-conf>` location to the original location:

   a. `cp <restore-conf>/etc/opt/omni/server/idb/idb.config`
      `/etc/opt/omni/server/idb/idb.config`

   b. `cp <restore-conf>/etc/opt/omni/server/idb/ulist`
      `/etc/opt/omni/server/idb/ulist`

   c. `cp <restore-conf>/etc/opt/omni/server/AppServer/standalone.xml`
      `/etc/opt/omni/server/AppServer/standalone.xml`

5. Modify the following fields in `idb.config` to point to the correct location (correct locations are stored in `idb.config.bkp`)

   a. `PGDATA_PG='/space/restore1/pg';`

   b. `PGDATA_IDB='/space/restore1/idb';`

   c. `PGDATA_JCE='/space/restore1/jce';`

   d. `PGWALPATH='/space/restore1/pg/pg_xlog_archive' ;`

6. Stop and start HPE Data Protector services.

   a. run `omnisv stop` (this could take a while)

   b. run `omnisv start`

   c. run `omnidbutil -clear`

After completing a restore operation, connecting from the HPE Data Protector GUI to the cell manager fails

Problem

After completing a restore operation and after applying the workaround provided for the following

Problem
issues: *IDB restore on a different cell manager could fail*, and *IDB restore fails at the end of a restore process*,   connecting from the GUI to the cell manager fails with the error :   `A server error has occurred. Reported error message: couldn't connect to host.`
Action
1. Take a backup of `/etc/opt/omni/server/AppServer/standalone.xml` file   2. Replace all keystore and truststore passwords in `/etc/opt/omni/server/AppServer/standalone.xml` with ones stored in `/etc/opt/omni/client/components/webservice.properties`

IDB restore on Windows Cell Managers

The IDB restore could fail on Windows cell managers. There are several possible reasons for this behavior and are outlined in this section.

IDB restore on a different cell manager could fail

Problem

IDB restore on different Cell Manager fails at the end of restore process if restore of DCBFs to different location has been chosen, with the following error message:
 	
 `An internal error occurred`
 	
 `R6025`
 	
 `- pure virtual function call`

Action
The user must choose to restore the DCBFs to original location or not to restore them at all.

Other problems

Restore of Storage Optimizer stubs reports error

Problem
The HPE Data Protector fails to restore the Storage Optimizer stubs even when the target file already exists on the system, and it reports the following error:

"File cannot be replaced"
Action
This issue may occur if you recently opened the existing file. You can perform one of the following actions:
a) Restore the file to another location
b) Wait until Storage Optimizer releases the file, and then retry
c) Rename the existing file

Backup protection expiration

Problem
When scheduling backups, you have set the same protection period for full and incremental backups, which means that incremental backups are protected for the same duration as the relevant full backup. Consequently, your data will actually only be protected until the full backup expires. You cannot restore incremental backups that are based on expired full backups.
Action
Configure the protection for your full backups so that they are protected for longer than your incremental backups.
The time difference between the protection for the full backup and the incremental backup should be the amount of time between the full backup and the last incremental backup before the next full backup.
For example, if you run incremental backups Monday through Friday and full backups on Saturday, you should set the protection of the full backup to at least 6 days more than for the incremental backups. This will keep your full backup protected and available until your last incremental backup expires.

Enhanced incremental backup fails because of a large number of files

Problem
On HP-UX systems, enhanced incremental backup fails when a large number of files is being backed up.
Action
To enable that a Disk Agent accesses more memory for the enhanced incremental backup, set the tunable kernel parameter `maxdsiz` as follows:
HP-UX 11.11 systems:

```
kmtune set maxdsiz=2147483648

kmtune set maxdsiz_64bit=2147483648
```

HP-UX 11.23/11.31 systems:

```
kctune set maxdsiz=2147483648

kctune set maxdsiz_64bit=2147483648
```

Intermittent connection refused error

Problem
The backup session aborts with a critical error: `Cannot connect to Media Agent on system computer.company.com, port 40005 (IPC Cannot Connect System error: [10061] Connection refused)` This problem may occur if a Media Agent is running on a non-server edition of Windows and the Disk Agent concurrency is set to more than 5. Due to the TCP/IP implementation on non-server editions of Windows operating systems, the operating system can accept only 5 incoming connections simultaneously.
Action
Set the Disk Agent concurrency to 5 or less. It is recommended to use server editions of Windows for systems involved in intensive backup operations, such as the Cell Manager, Media Agent clients, application agent clients, file servers, and so forth.

Unexpected mounted filesystems detected when restoring a disk image

Problem
When restoring a disk image, you get a message that the disk image being restored is a mounted filesystem and will not be restored: `Object is a mounted filesystem = not restored.` This happens when an application on the disk image leaves some patterns on the disk image. The patterns confuse the system call that verifies whether the filesystem on the disk image is mounted or not, so the system call reports that there is a mounted filesystem on the disk image.
Action
Before you start a restore, erase the disk image on the Data Protector client with the disk image being restored: `prealloc null_file 65536`

```
dd if=null_file of=device_file
```

where *device_file*is a device file for the disk image being restored.

Problems with application database restores

Problem
When trying to restore a database, it fails with one of the following messages: • `Cannot connect to target database` • `Cannot create restore set` A poorly configured DNS environment could cause problems with database applications. The problem is as follows: When backing up a database, the agent that starts on the client where the database is located logs the client name to the database as *computer.company.com*. At restore time, the Restore Session Manager tries to restore to *computer.company.com*, but it cannot because it knows this client only as *computer*. The client name cannot be expanded to the full name because the DNS is improperly configured. This situation can also be the other way around, where DNS is configured on the Cell Manager and not on the Application Client.
Action
Set up the TCP/IP protocol and configure DNS properly. For information, see Appendix B in the *HPE Data Protector Installation Guide*.

Backup failure on HP-UX

Problem

The following error occurs during the backup:
 	
`Cannot allocate/attach shared memory (IPC Cannot Allocate Shared Memory Segment)`
 	
`System error: [13] Permission denied) = aborting`

Action
Set the `OB2SHMEM_IPCGLOBAL omnirc` option to 1 on HP-UX clients that have both, the Disk Agent and a Media Agent installed, or have one of the supported integration and a Media Agent installed.

Asynchronous reading does not improve backup performance

Problem

With the **Asynchronous reading** (Windows specific) option selected in the backup specification, there is no backup performance improvement, or there may even be performance degradation.

Action

1. Check if the omnirc option `OB2DAASYNC` is set to 0. Either set the option to 1 to always use asynchronous reading, or comment out the option and use the **Asynchronous reading** option in the backup specification.

2. Consider if asynchronous reading is suitable for your backup environment. In general, asynchronous reading is suitable for files larger than 1 MB. Additionally, you can try to fine-tune the omnirc option `OB2DAASYNC_SECTORS`. As a rule, the size of your files (in bytes) should be 2-3 times larger than the value of the option.

Backup of the IIS configuration object fails on Windows systems

Problem

On a Windows Server 2008 or Windows Server 2012 system, while backing up the IIS configuration object, Data Protector reports the following error:

```
[Minor]

From: VBDA@computer.company.com "CONFIGURATION:" Time: Date & Time [81:141]

\IISDatabase Cannot export configuration object: (Details unknown.) = backup
incomplete.
```

Action

Install the **IIS 6 Metabase Compatibility** component under **IIS 6 Management Compatibility** and restart the backup.

Restore of a subtree from a volume with hard links present fails

Problem

Restore of a subtree from a volume with hard links present fails with the following error message:

```
Lost connection to Filesystem restore DA named ""

incomplete.
```

Action

Set the global option `RepositionWithinRestoredObject` to `0` if you are restoring trees with hard links.

Although setting this option to 0 may make the restores slightly slower, it is needed whenever

restoring hard links. By default, this option is set to 1.

On Mac OS X, backup sessions fail due to insufficient amount of shared memory

Problem

On Mac OS X, if you increase the device block size, the backup session may fail with the following error message:

```
[80:1003] Cannot allocate/attach shared memory (IPC Cannot Create Shared Memory
Segment System error: [12] Cannot allocate memory ) => aborting.
```

Action

Increase the kernel parameter `kern.sysv.shmmax` (maximum size of a shared memory segment) to a larger value. HPE recommends to set the parameter to 32 MB.

Backup of the system reserved partition that is mirrored may fail

Problem

When trying to backup a system reserved partition and multiple full volume objects, the backup may fail with either of the following error messages:

```
Fallback to legacy filesystem backup was not allowed. Aborting the backup.
```

```
Not a valid mount point => aborting.
```

> **NOTE:**
> The problem occurs only if the VSS option is enabled, and the system reserved partition is mirrored.

Action

Set the omnirc variable `OB2_DISABLE_REGLIST_FOR_FULL_VOLUME` to 1, and restart the backup.

Interrupted file backup or file cannot be found

Problem

When trying to backup a system reserved partition and multiple full volume objects, the backup fails with either of the following error message:

```
- Cannot read <number> bytes at offset <number>(:1): ([21] The device is not
ready. ).
```

Problem
- Cannot open: ([2] The system cannot find the file specified.) => not backed up. > **NOTE:** > The problem occurs only if the VSS option is enabled and if the system reserved partition does not have enough space to hold multiple snapshots.

Action
Set the omnirc variable `OB2_DISABLE_REGLIST_FOR_FULL_VOLUME` to `1` and restart the backup. If the error persists, see the following Microsoft webpage for information on how to resolve this problem: http://support.microsoft.com/kb/2930294

Scheduler fails when trying to schedule backups

Problem
Scheduler fails when trying to schedule backups with different timings.

Action
This may be happening because of Java services. Perform the following steps: 1. Close the Data Protector GUI. 2. Execute `omnisv stop`. 3. End the Java Services from the Task Manager. 4. Execute `omnisv start`. 5. Start the Data Protector GUI.

A ZDB filesystem backup of a windows deduplicated volume without the data deduplication feature fails

Problem

A ZDB filesystem backup of a Windows deduplicated volume on a Windows backup host, without installing the data deduplication feature, fails with the following error message:
 	
`[Warning] From: VBDA@computer.company.com "<volume label>" Time: <Date Time>`
 	
`[81:77] <Path name>`
 	
`Cannot open: ([1920] The file cannot be accessed by the system. ) => not backed up.`

Action

Problem

1. Install the Windows data deduplication feature on the backup host.
 	
2. Ensure that there are no data deduplication jobs during the ZDB backup by:
 	
    • Scheduling data deduplication jobs before or after the ZDB backup process.
 	
    • Implementing pre-exec scripts that will stop data deduplication jobs before the backup and post-exec scripts that will start them after the backup.

Pre- and post-exec scripts fail with error message

Problem

The `pre-` and `post-exec` scripts fail with the following error messages:
 	
`[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`..\script.bat`
 	
`Illegal command format. Command not executed.`
 	
`[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time: <DATE><TIME>`
 	
`[131:104] Script returned error. (Return value: -1).`

Action
The error message indicates that the `pre-` and `post-exec` scripts are not available at the correct location. Ensure that the `pre-` and `post-exec` scripts are located in the following directories: • Windows systems: _Data_Protector_home_`\bin` directory, or its sub-directories. • Unix systems: `/opt/omni/lbin` directory, or its sub-directories. The problem statement here lists the error message for SQL agent. Similar error messages are displayed for all integration and ZDB modules during the failure of `pre-` and `post-exec` scripts.

Pre- and post-exec scripts fail when OB2OEXECOFF is set

Problem

Execution of `pre-` and `post-exec` scripts fails with the following error messages:
 	
`[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`OB2OEXECOFF variable value prevents execution of pre/post-exec scripts on this host.`

Action
The error message indicates that the `OB2OEXECOFF` variable in `omnirc` file is enabled for this client. Setting this variable disables the execution of `pre-` and `post-exec` scripts. To disable `OB2OEXECOFF` variable, set the value to `0`.

Post-exec scripts are not run if pre-exec scripts fail

Problem

The `post-exec` scripts are skipped if `pre-exec` scripts fail for a client with the following error messages:
 	
`[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`..\script.bat`
 	
`Illegal command format. Command not executed.`
 	
`[Major] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`[131:104]      Script returned error. (Return value: -1).`
 	
`[Warning] From: OB2BAR_SQLBAR@hostname.com "1"  Time:<DATE><TIME>`
 	
`Pre-exec script failed. Skipping Post-exec !`

Action

Set the `OB2FORCEPOSTEXEC` variable in `omnirc` file to `1` to ensure that the `post-exec` scripts are always run, even if the `pre-exec` scripts fail for a client.
 	
After you enable the `OB2FORCEPOSTEXEC` variable, and run the backup specification, the following messages appear:
 	
`[Normal] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`Starting post-exec script 'script.bat'...`
 	
`[Normal] From: OB2BAR_SQLBAR@hostname.com "(<Instance>)"  Time:<DATE><TIME>`
 	
`Script executed successfully.`
 	
The messages indicate that even though the `pre-exec` script failed, the `post-exec` script was successfully run for the client.

Chapter 6: Troubleshooting Devices and Media

Backup devices are subject to specific Data Protector licenses. For details, see the *HPE Data Protector Product Announcements, Software Notes, and References*.

Problems involving device SCSI addresses are explained in detail in *Appendix B* of the *HPE Data Protector Installation Guide*.

General device and media problems

Free pool media is not automatically reformatted when data formats are incompatible

Problem
Backup or restore session aborts with the following warning:
`[Warning] From: BSM@cell_manager.com "xtest" Time: 4.4.2014 11:45:41`
`[60:1023] Medium "200011ac:533e6a06:0134:0001" labeled "[MTV341L4] MTV341L4"`
`of data format NDMP - Hitachi is not compatible with device "EML-Tape1" of dataformat OB2 - Generic.`

Action
The backup or restore session might abort, if the user has a media pool for standard filesystem backups, a separate pool for NDMP backups and both share a common free pool.
Set the global parameter `CheckNDMPDataFormatType` to 1.

Insufficient StoreOnce Fibre Channel devices on the Media Agent client

Problem
If a Media Agent lacks sufficient number of StoreOnce Fibre Channel (FC) devices, the following error message appears while backing up a high number of objects or while running several concurrent sessions:
`|Major| From: BMA@abc.com "DEV_FC_gw2 [GW 23117:0:6931224894398172655]" Time: <DATE> <TIME>`
`|90:54| \\abcd\FC/75232e10_5322f96a_445f_01b1`
`Cannot open device (StoreOnce error: StoreOnce device offline, network error occurred`

or secure communication failed while contacting the StoreOnce device)
Action
Increase the number of available FC devices on the Media Agent client. For example, if a Media Agent connected to FC has only 16 StoreOnce FC devices available and if you need to concurrently backup 200 objects, then you should increase the available FC devices to 200 or more, as Data Protector requires 200 connections. To increase the available FC devices on the Media Agent client: 1. Open the HPE B6200 StoreOnce Backup System application. 2. Expand **HPE StoreOnce**, and then expand **StoreOnce Catalyst**. 3. In the Fibre Channel Settings tab, scroll down to the Devices section and click **Edit**. 4. Set the desired value for the **Devices per Initiator Port** field (for each port). In Windows, you can verify the available number of StoreOnce FC devices in the Device Manger window. Note that the number of devices visible on the Media Agent client is equal to the sum of the Device per Initiator Port value for all FC ports.

Cannot access exchanger control device on Windows

Problem
Data Protector uses the SCSI mini-port driver to control backup drives and libraries. Data Protector may fail to manage devices if other device drivers are loaded on the same system. When device operations such as media formatting or scanning are started, the following error displays: `Cannot access exchanger control device`
Action
On the system where the devices are located, list all physical devices configured on the system: *Data_Protector_home*\bin\devbra -dev If any of the SCSI addresses have the status value `CLAIMED`, they are used by another device driver. Disable the Windows robotics driver. For instructions, see the *HPE Data Protector Help* index: "robotics drivers".

SCSI device remains locked and session fails

Problem
SCSI drive or robotic control remains locked due to an incomplete SCSI reserve or release operation. The following message is displayed: `Cannot open device` If there is a Media Agent failure, the reserved device cannot be released again. Data Protector may

fail to unlock the SCSI drive or robotic control and the subsequent session cannot use it.
Action
Ensure that no other application is using this device. To unlock the SCSI drive or SCSI robotic control, the device has to be power cycled.

Device open problem

Problem
When trying to use a DDS device, the following error displays: `Cannot open device (not owner)`
Action
Check whether you are using a medium that is incompatible with the Media Recognition System. Media used with DDS drives must comply with the Media Recognition System.

Using unsupported SCSI HBAs/FC HBAs on Windows

Problem
The system fails due to the usage of unsupported SCSI HBAs/FC HBAs with backup devices. Typically, the problem occurs when the SCSI device was accessed by more than one Media Agent at the same time or when the length of the transferred data defined by the devices block size was larger than the length supported by the SCSI HBA/FC HBA.
Action
You can change the block size of the device. For instructions, see the *HPE Data Protector Help*: "setting advanced options for devices and media". For information on supported SCSI HBAs/FC HBAs, see the *HPE Data Protector Product Announcements, Software Notes, and References*.

Library reconfiguration failure

Problem
Configuration errors are reported during modification of an existing library configuration using the `sanconf` command after the device list file has been altered. The library configuration remains only partially created.
Action

You can recover the previous library configuration if you reuse the file with a list of hosts in your SAN environment and scan the hosts with `sanconf` again.

1. Scan the hosts in the cell:

   `sanconf -list_devices mySAN.txt -hostsfile hosts.txt`

2. Configure your library using the saved configuration file:

   `sanconf -configure mySAN.txt -library` *LibrarySerialNumberLibraryName* [*RoboticControlHostName*] [*DeviceTypeNumber*] `-hostsfile hosts.txt`

   The previous successful library configuration is automatically recovered.

If you add, remove, or modify the library later and configuration with the `sanconf` command fails, you can repeat the above procedure to restore the successful configuration.

An encrypted medium is marked as poor after a read or write operation

Problem

During a read or write operation on a medium that was written to using drive-based encryption, the session fails and the medium is automatically marked as poor.

The following error displays:

`Cannot read from device ([5] I/O error)`

This happens if a read or write operation was performed on a platform that does not support drive-based encryption. The medium quality is not affected. For an up-to-date list of supported platforms, see the latest support matrices at https://softwaresupport.hpe.com/.

Action

To correct the media condition status, reset the media condition by using the `omnimm -reset_poor_ medium` option.

For details, see the `omnimm` man page or the *HPE Data Protector Command Line Interface Reference*.

Creating null devices using Data Protector GUI and CLI

Problem

In operating systems such as UNIX , a null device is a special file that removes all the data written to it. Hence data is not available to any process that reads from this file and results in end-of-file immediately. However, the report for this write operation is shown as successful.

For troubleshooting purposes, if no actual data output is needed, null devices can be created upon request by HPE support. This document provides information on creating null devices using the Data Protector GUI and CLI.

Action
Caution: Null devices should be created and used as a temporary solution, and removed after successfully completing the troubleshooting operation. Otherwise, if used accidentally for production backups, this process results in immediate data loss.

Complete the following steps in Data Protector GUI:

1. In the Context List, click **Devices & Media**.

2. In the Scoping Pane, right-click **Devices** and then click **Add Device** to open the wizard.

3. In the **Device Name** text box, enter the name of the device.

4. In the **Description** text box, enter a description (optional).

5. In the **Device Type** list, select the Standalone device type.

6. Click **Next**.

7. Specify the name null and click **Add**.

8. Click **Next**.

9. In the **Media Type** list, retain the default values.

10. For the **Default Media Pool**, retain the default values.

11. Click **Finish** to exit the wizard.

    The name of the device is displayed in the list of configured devices. You can scan the device to verify the configuration.

12. After creating a null device using theData Protector GUI, export the configuration of the specified backup device to an ASCII file. You can export the configuration using the following CLI command:

    `omnidownload -device BackupDevice [-file FileName]`

    For example, `omnidownload -device ThisIsNULLDevice -file NULL.dev`

Creating null devices using CLI

Null devices that are created using the Data Protector GUI can be replicated on another system using the CLI.

The `omnidownload` command enables you to display information about backup devices or to download the configuration of the specified backup device to an ASCII file. This command downloads information about a backup device and a library from the Data Protector Internal Database (IDB). This command is available on systems that have the Data Protector User Interface component installed.

Used together with the `omniupload` utility, this command enables you to create and maintain backup devices using the Command-Line Interface.

The `omniupload` utility, 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.

For details, see the *HPE Data Protector Command Line Interface Reference*.

Complete the following steps:

1. After creating a file device using theData Protector GUI, use the following command to list the available devices:

    ```
    omnidownload -list_devices
    ```

    This command displays information about the Data Protector backup devices. The report includes the following information for each device: device name, client, device type, and pool.

2. Download or export the configuration of the created backup device to an ASCII file using the following CLI command:

    ```
    omnidownload -device BackupDevice [-file FileName]
    ```

    For example: `omnidownload -device ThisIsNULLDevice -file NULL.dev`

    This command updates the ASCII file or text file with all the backup device configuration details.

    For example:

    ```
    NAME "ThisIsNULLDevice"

    DESCRIPTION " "

     HOST dppvt5140.company.com

     POLICY Standalone

     TYPE File

    POOL "Default File"

     ENCRCAPABLE

    DRIVES

    "null"

    DEVSERIAL ""

    RESTOREDEVICEPOOL NO

    COPYDEVICEPOOL NO
    ```

    > **NOTE: Note**: Ensure that the value specified for HOST is a regular client in the Cell Manager. If you export the device on one cell manager and import it to a new or different Cell Manager, then you must change the HOST name to the new media agent host, which is part of the new Cell Manager.

3. If a new or different Cell Manager is being used, then modify the hostname in the ASCII or text file and then upload the ASCII file to the system using the following command:

    ```
    omniupload -create_device FileName
    ```

    For example: `omniupload -create_device NULL.dev`

Various media problems

Problem
Various media problems.
Action
Use the Medium Quality Statistics functionality to detect problems with media while they are still in their early stages.

Before each medium is ejected from a drive, Data Protector uses the `SCSI log sense` command to query medium read and write statistical information. The information is written to the `media.log` file.

The medium quality statistics feature is disabled by default. To enable it, set the global option `Ob2TapeStatistics` to `1`.

For instructions, see .

If you receive media related errors during read or write operations, or if the medium is marked as poor, you can check the `media.log` file for media errors statistics.

`Media.log` contains the following error statistics, where `n` is the number of errors:

Error statistics	Description
`errsubdel=n`	errors corrected with substantial delays
`errposdel=n`	errors corrected with possible delays
`total=n`	total number of re-writes
`toterrcorr=n`	total number of errors corrected and recovered while writing
`totcorralgproc=n`	total number of times correction algorithm processed
`totb=n`	total bytes processed (write)
`totuncorrerr=n`	total number of uncorrected errors (write)

If a parameter has the value `-1`, the device does not support this statistics parameter. If all parameters have the value `-1`, either an error occurred during the tape quality statistics processing or the device does not support medium quality statistics.

For `total bytes processed`, statistical results are reported in bytes for most devices. However, LTO and DDS devices report data sets and groups, respectively, and not bytes.

Examples

Here are a few examples from the `media.log` file for different device types.

DLT/SDLT devices

Log sense write report for DLT/SDLT devices - total bytes processed.

```
Media ID from tape= 0fa003bd:3e00dbb4:2310:0001; Medium Label= DLT10; Logical
drive= dlt1; Errors corrected no delay= 0; Errors corrected delay= 0; Total=
13639; Total errors corrected= 13639; Total correction algorithm processed= 0;
Total bytes processed= 46774780560; Total uncorrected errors= 0
```

46774780560 bytes of native data after compression were processed (a full DLT8000 tape).

LTO devices

Log sense write report for LTO devices - total data sets processed.

```
Media ID from tape=0fa003bd:3e0057e6:05b7:0001; Medium Label= ULT2; Logical
drive=ultrium1; Errors corrected no delay= 0; Errors corrected delay= 0; Total=
0;Total errors corrected= 0; Total correction algorithm processed= 0; Total bytes
processed= 47246; Total uncorrected errors= 0
```

One data set is 404352 bytes. To calculate the amount of total bytes processed, use the following formula:

```
47246 data sets * 404352 bytes = 19104014592 bytes after compression (a full
tape)
```

DDS devices

Log sense write report for DDS devices - total groups processed.

```
Media ID from tape= 0fa0049f:3df881e9:41f3:0001; Medium Label= Default DDS_5;
Logical drive= DDS; Errors corrected no delay= -1; Errors corrected delay= -1;
Total= -1; Total errors corrected= 0; Total correction algorithm processed= 154;
Total bytes processed= 2244; Total uncorrected errors= 0
```

DDS1/2: One group is 126632 bytes.

DDS3/4: One group is 384296 bytes.

To calculate the amount of total bytes processed, use the following formula:

```
2244 groups * 126632 bytes = 284162208 bytes after compression (a 359 MB backup
on DDS2)
```

359 MB of data was backed up, resulting in 271 MB of native data on tape.

Medium header sanity check errors

Problem

By default, Data Protector performs a medium header sanity check before a medium is ejected from a drive.

In case the medium header sanity check detects any header consistency errors on the medium, an error message is displayed. All objects on this medium are marked as failed, and the status of sessions that include objects from this medium, are also changed.

If the medium header is corrupt, all objects on the affected medium are marked as failed and the medium is marked as poor.

Action

Export the medium from the IDB and restart the failed session using a different medium.

Problems with device serial number

Problem

When performing any operation involving the problematic backup device (such as backup, restore, format, scan, and so on) or robotics, the following error displays:

`Device DeviceName could not be opened (Serial number has changed).`

The error is reported when the device path points to a device with a different serial number than the number stored in the IDB. This can happen in the following cases:

- You misconfigured the device (for example, using the omniupload command, or if you configured an incorrect device file).
- You replaced the physical device without updating the corresponding logical device (reloading the new serial number).
- You physically replaced a SCSI tape drive located in a SCSI library. Either the option **Automatically discover changed SCSI address** is not enabled or the omnirc option `OB2MADETECTDRIVESWAP` is set to 0.
- A path in a multipath device is misconfigured.

Action

1. In the Data Protector GUI, switch to the Devices & Media context.
2. In the Scoping Pane, expand **Devices**, right click the problematic device, and click **Properties**.
3. Click the Control tab and enable the **Automatically discover changed SCSI address** option.
4. Click **Reload** to update the device serial number in the IDB.

   In case of a physically replaced SCSI tape drive located in a SCSI library, make sure that the omnirc option `OB2MADETECTDRIVESWAP` is set to 1 (Default). You do not need to reload the device serial number.

Cannot restore or copy corrupt data

Problem

By default, CRC values are always checked when available on a tape and data found corrupt by

CRC mismatch is never restored or copied. However, in certain situations, you may still want to restore or copy such data.
Action
Temporarily set the omnirc option `OB2CRCCHECK` on the Media Agent host to 0. After the recovery of corrupt objects (data) revert the setting to the default value (1).

Common hardware-related problems

Problem
Common hardware-related problems.
Action
Check the SCSI communication between the system and the device, such as adapters or SCSI cables and their length. Try running an OS-provided command, such as `tar`, to verify that the system and the device are communicating.

Failing connections to StoreOnce software

Problem
In the session using StoreOnceSoftware session with multiple objects, some of the objects fail with the following error message:
`[Major] From: RMA@hostname.com "soda_gw1 [GW 18437:17:5373994507538143831]" Time: 09/18/2017 01:15:12 PM`
`[90:54] \\hostname.com\store/0d09310a_59bfa4e3_666d_0012`
Cannot open the device.
StoreOnce error: `StoreOnce device offline, network error occurred or secure communication failed while contacting the StoreOnce device.`
Action
Set the omnirc variable `OB2UNSECURE_STOREONCESOFTWARE=1` on the host where the StoreOnceSoftware is running and restart the StoreOnceSoftware service.

ADIC/GRAU DAS and STK ACS libraries problems

ADIC/GRAU DAS library installation failed

Problem
ADIC/GRAU DAS library installation failed.
Action

1. Install a Media Agent on the client controlling the GRAU robotics (PC/robot).

2. Install a Media Agent on the clients where a drive is connected (PC/drive).

3. Copy `aci.dll` + `winrpc.dll` + `ezrpcw32.dll` to *%SystemRoot%*`\system32` and *Data_ Protector_home*`\bin` directory.

4. Create the `aci` directory on PC/robot.

5. Copy `dasadmin.exe`, `portmapper`, and `portinst` to the `aci` directory.

6. Start `portinst` to install `portmapper` (only on PC/robot).

7. Install the `mmd` patch on the Cell Manager.

8. Restart the system.

9. In Windows **Control Panel** > **Administrative Tools** > **Services**, check if `portmapper` and both `rpc` services are running.

10. On the OS/2 system within the GRAU library, edit the file `/das/etc/config`. Add a client called `OMNIBACK` containing the IP address of the PC/robot.

You cannot see any drives

Problem
You cannot see any drives.
Action

Run the following commands from PC/robot:

1. `dasadmin listd`

2. `dasadmin all DLT7000 UP` *AMUCLIENT*

3. `dasadmin mount` *VOLSER* (then push the `UNLOAD` button on the drive)

4. `dasadmin dismount` *VOLSER* or `dasadmin dismount -d` *DRIVENAME*)

Where:

- *AMUCLIENT* = `OMNIBACK`

- *VOLSER*, for example `001565`

- *DRIVENAME* , for example `DLT7001`

- `all`, stands for allocate

If you are not successful with these commands (communication to DAS Server (OS/2)), try running these commands on the OS/2 system from the `/das/bin/ directory`.

When running these commands from the OS/2 system, use *AMUCLIENT* = AMUCLIENT.

1. Log in to the AMU client. Common logins are:

   `user: Administrator pwd: administrator`

   `user: Supervisor pwd: supervisor`

2. It may be necessary to set the media type:

   set `ACI_MEDIA_TYPE` set `ACI_MEDIA_TYPE=DECDLT`

3. Restart the library:

   a. Shut down OS/2 and then switch off the robotics.

   b. Restart OS/2 and when OS/2 is ready, the AMU log will display that the robotics is not ready. Switch on the robotics.

GRAU CAPs are not configured properly

Problem
GRAU CAPs are not configured properly.
Action

You can only move media from the CAP to a slot and then to a drive using the devices robotics. Use the `import` and `export` commands, for example:
 	
`import CAP: I01`
 	
`import CAP range: I01-I03`
 	
`export CAP: E01`
 	
`export CAP range: E01-E03`

The library operations fail

Problem
The library operations fail.
Action
Use the following syntax when using the Data Protector uma utility to manage the GRAU and STK library drives: `uma -pol POLNUMBER -ioctl LIBRARYNAME -type MEDIATYPE`

where *POLNUMBER* is 8 for GRAU and 9 for STK.

For example: `uma -pol 8 -ioctl grauamu`

The default media type is DLT.

Cloud device problems

Communication errors with Cloud (Helion) and Cloud (Azure)

Problem
The Cloud (Helion) and Cloud (Azure) devices encounter errors in while communicating with the Cloud object store. The Cloud (Helion) and Cloud (Azure) devices retries the operations if errors are encountered. When communication errors occur, the following error displays: `Error in communication with cloud [ERROR], retrying`
Action
The default retry count for the Cloud is 5. Set the omnirc option `OB2_CLOUDDEV_MAXRETRIES` on the Media Agent host to higher than 5.

Unable to configure Cloud (Helion) device with HPE Data Protector 9.00

Problem
The Cloud (Helion) device encounters problems during configuration when attempting to configure with HPE Data Protector 9.00 or earlier.
Action
Cloud (Helion) devices are not supported by earlier versions of HPE Data Protector. Ensure that all Cell Managers, GUI servers, Installation Servers, and Media Agents are updated to the General Release Patch or later.

Unable to configure Cloud (Azure) device with HPE Data Protector versions before 10.02

Problem
The Cloud Azure device encounters problems during configuration when attempting to configure with HPE Data Protector 9.08 or earlier.
Action
Cloud (Azure) devices are not supported by earlier versions of HPE Data Protector. Ensure that all Cell Managers, GUI servers, Installation Servers, and Media Agents are updated to the General Release Patch or later.

Chapter 7: Troubleshooting Object Operations Sessions

Object copy problems

Fewer objects are copied than expected

Problem
With post-backup or scheduled object copy, the number of objects that match the selected filters is higher than the number of objects that are actually copied. The following message is displayed: `Too many objects match specified filters.`
Action
• Tighten the criteria for object version selection. • Increase the maximum number of objects copied in a session by setting the global option `CopyAutomatedMaxObjects`.

Not all objects in the selected library are copied

Problem
With post-backup or scheduled object copy, some objects that reside on media in the selected library are not copied. This happens if an object does not have a complete media set in the selected library.
Action
Insert the missing media into the selected library, or select the library that has a complete media set for these objects.

Mount request for additional media is issued

Problem
In an interactive object copy session from the Media starting point, you selected a specific medium. A mount request for additional media is issued. This happens if an object residing on the medium spans to another medium.
Action

Insert the required medium into the device and confirm the mount request.

When creating an object copy, the protection end time is prolonged

Problem
When creating an object copy, the protection end time is not inherited from the original object. The protection length is copied, but the start time is set at the object copy creation time and not at the object creation time. This results in a longer protection then for the original. The more time passes between the original backup and the object copy session, the bigger the difference between the protection end times.
For example, if the object was created on September 5, with the protection set to 14 days, the protection will expire on September 19. If the object copy session was started on September 10, the object copy protection will expire on September 24.
In some cases, such behavior is not desirable and the protection end time must be preserved.
Action
Set the global option `CopyDataProtectionEndtimeEqualToBackup` to `1` to ensure that the object copy protection end time is equal to backup object protection end time. By default, the option is set to 0. Increase the maximum number of allowed files.

Replicating session with multiple objects stops responding

Problem
When replicating a session onto another device, the session stops responding. The session output provides the following information:
`[Normal] From: BMA@company.com "d2d1_1_gw1 [GW 26177:1:15198446278003495809]" Time: 3/21/2013 9:13:06 AM`
`COMPLETED Media Agent "d2d1_1_gw1 [GW 26177:1:15198446278003495809]"`
The problem is known to occur in a dual IP stack network configurations with HP-UX Media Agent.
Action
When configuring a dual IP stack network, add a separate entry for IPv6 localhost addresses to the `/etc/hosts` file on the Media Agent client.
For example, you have the following entry in your `hosts` file:
`::1 localhost loopback`
To resolve the issue, add the following line for IPv6 addresses:
`::1 ipv6-localhost ipv6-loopback`

Replication session on Data Domain Boost devices is unable to respond to Abort operation during retry period

Problem
When replicating a session from one Data Domain Boost backup device to another when the device does not have enough available streams, the replication session is unable to respond to Abort operations during the retry period.
Action
The problem is known to occur when the `omnirc` `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT` is set to `0`, which is not supported. This variable defines how many seconds the replication session will wait before beginning another retry when the Data Domain Boost device does not have enough available streams. If the interval is too large or is set to `0`, the session will be unable to respond to Abort operations. The default for `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT` is 60 seconds. See the `omnirc` file for a complete description of `DP_DDBOOST_SLEEP_SECOND_FOR_STREAM_LIMIT`.

Object consolidation problems

Object consolidation of many points in time opens too many files

Problem

If you start an object consolidation operation with many points in time, Data Protector reads all media necessary to complete the operation. This opens all files at the same time. When Data Protector opens more files than the number allowed by your operating system, a message similar to the following one is displayed:
 	
`|Major| From: RMA@computer.company.com "AFL1_ConsolidateConc2_bs128" Time: time /omni/temp/Cons_Media/AFL1/`
 	
`0a1109ab54417fab351d15500c6.fd`
 	
`Cannot open device ([24] Too many open files)`

Action
Increase the maximum number of allowed files. **HP-UX systems:** 1. Set the maximum number of open files using the System Administration Manager (SAM):   a. Select **Kernel Configuration > Configurable parameters** and then, **Actions** > **Modify**

> **Configurable Parameter**.
>
>   b. Enter the new **maxfiles_lim** and **maxfiles** values in the **formula/value** field.
>
> 2. Restart your computer after applying the new values.
>
> **Solaris systems:**
>
> 1. Set the maximum number of open files by editing the `/etc/system` file. Add the following lines:
>
>   `set rlim_fd_cur=value`
>
>   `set rlim_fd_max=value`
>
> 2. Restart your computer after applying the new values.

Object consolidation to B2D devices fails in the second attempt

Problem
After the first object consolidation, if you perform an incremental backup and then perform the second object consolidation, the operation fails.
Action
To ensure that the second consolidation succeeds, perform a full backup after the first object consolidation. Thereafter, perform an incremental backup, which can be consolidated later.

Chapter 8: Troubleshooting the Data Protector Internal Database

You can find a list of IDB directories in the `omniintro` reference page of the *HPE Data Protector Command Line Interface Reference.*

Problems due to missing directories

Cannot open database/file or database network communication error

Problem
If one or several IDB data files or directories are missing, the following errors are displayed when Data Protector tries to access the IDB: • `Cannot open database/file`   • `Database network communication error`
Action
Reinstall the IDB data files and directories: 1. Reinstall Data Protector.   2. Restart the Cell Manager.

Cannot access the Cell Manager

Problem
When the Data Protector GUI tries to connect to the Cell Manager, the following error message is displayed if the Data Protector temporary directory is missing: `Cannot access the Cell Manager system. (inet is not responding) The Cell Manager host is not reachable or is not up and running or has no Data Protector software installed and configured on it.`
Action
1. On the Cell Manager, close the Data Protector GUI.   2. Initiate the maintenance mode: `omnisv -maintenance`   3. Manually create the directory `tmp` in:

> **Windows systems:***Data_Protector_program_data*
>
> **UNIX systems:**`/var/opt/omni`
>
> 4. Quit the maintenance mode:
>
>   `omnisv -maintenance -stop`
>
> 5. Restart the Data Protector GUI.

Problems during backup or import

IDB backup failure reports incorrect archive log file name format

Problem
After upgrading to the HPE Data Protector 9.00 patch, the IDB backup fails with the following message: "`The archive log filename format is incorrect.`"
Action
Perform the following steps: 1. Run `omnisv stop`. 2. Manually change the path of the IDB location in the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\hpdp-idb\ImagePath` to point to the new restored IDB location, because after upgrading, the path in the registry points to the old IDB location. 3. Run `omnisv start`. 4. Run `omnidbutil -set_schema_crc`. > **NOTE: Note:** Every IDB schema has an associated CRC file. After changing the IDB location (as mentioned in Step 2), you must modify the CRC file to match the schema of the new IDB location. The last step creates the CRC file that matches the new IDB schema.

File names are not logged to the IDB during backup

Problem
When performing backups using Data Protector, file names are not logged to the IDB if: - You have selected the `No Log` option for backup. - The DCBF part of the IDB is running out of space, or the disk where the IDB is located is running low on disk space. An error in the session output informs you about this.
Action

- Check if you have selected the `No Log` option for backup.
- Check the session messages of the backup session for warnings and errors.

The BSM or RSM is terminated during the IDB backup or import

Problem

If the BSM or RSM get terminated during the IDB backup or import session, the following error is displayed:

`IPC Read Error System Error: [10054] Connection reset by peer`

In the Internal Database context of the Data Protector GUI, the session status is still marked as `In Progress` but the session is actually not running.

Action

1. Close the Data Protector GUI.
2. Execute the `omnidbutil -clear` command to set the status of all sessions that are actually not running but are marked as `In Progress` to `Failed`.
3. Execute the `omnidbutil -show_locked_devs` command to see if any devices and media are locked by Data Protector.
4. If there are, execute the `omnidbutil -free_locked_devs` to unlock them.
5. Restart the Data Protector GUI.

The MMD is terminated during the IDB backup or import

Problem

If the media management daemon (MMD) is terminated during the IDB backup or import session, the following errors are displayed:

- `Lost connection to MMD`
- `IPC Read Error System Error: [10054] Connection reset by peer`

If the MMD services/processes are not running:

- The output of the `omnisv -status` command indicated that the MMD service/process is down.
- You notice the following:

    Windows systems: In the Windows Task Manager, the Data Protector MMD process (`mmd.exe`) is not displayed.

    UNIX systems: When listing the Data Protector processes using the `ps -ef | grep omni` command, the Data Protector MMD process (`/opt/omni/lbin/mmd`) is not displayed.

Action

1. Close the Data Protector GUI.

2. Execute the `omnisv -stop` command to stop the Data Protector services/processes.

3. Execute the `omnisv -start` command to start the Data Protector services/processes.

4. Execute the `omnisv -status` command to check if all the services/processes are running.

The DC binary files are corrupted or missing

Problem

When browsing backed up objects in the Restore context of the Data Protector GUI, the following error displays:

```
Open of Detail Catalog Binary File failed
```

- The `omnidbcheck -bf` command reports that one or several DC binary files are missing or are of incorrect size, or the `omnidbcheck -dc` command reports that one or several DC binary files are corrupted.

- The `debug.log` file on the Cell Manager contains one or several entries on Data Protector not being able to open a DC binary file.

Action

Recreate DC binary files by importing catalog from media.

For instructions, see the *HPE Data Protector Help* index: "minor IDB corruptions in DCBF".

The Internal Database backup fails

Problem

The session for backing up the Data Protector Internal Database fails with the following error:

```
[Critical] From: OB2BAR_POSTGRES_BAR@computer.company.com "DPIDB" Time: 4/2/2013
4:05:20 PM

                Error while running the PSQL script
[Normal] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM

                OB2BAR application on "computer.company.com" disconnected.
[Critical] From: BSM@computer.company.com "idb" Time: 4/2/2013 4:05:20 PM

                None of the Disk Agents completed successfully. Session has
failed.
```

If the Data Protector Inet service is running under a domain user account, the problem is most probably caused by insufficient Security Policy privileges for that account.

Action

Grant the Windows domain user account that is used for the Data Protector Inet service the following

> Windows operating system Security Policy privileges, and restart the session afterwards:
>
> - Impersonate a client after authentication
> - Replace a process level token
>
> For more information, see the *HPE Data Protector Help* index: "Inet user impersonation".

Performance problems

Browsing for restore is slow

Problem
When browsing object versions and single files for restore in the Data Protector GUI, it takes a long time before the information is read from the IDB and displayed. This happens because the number of object versions of the selected object in the IDB is too large.
Action

Set the time interval for browsing object versions for restore:
 	
• For a specific restore, set the **Search interval** option in the Source page.
• Globally, for all subsequent restores:
 	
  1. In the File menu, click **Preferences**.
  2. Click the **Restore** tab.
  3. Set the **Search interval** option and click **OK**.

Problems with the IDB growth

The IDB is running out of space

Problem
A part of the IDB is running out of space. The IDB Space Low notification is issued.
Action
Extend the IDB size.

The DCBF part of the IDB is growing too fast

Problem

In the `Client Statistics` report, the **Data Written [GB]** or the **# Files** figures are `considerably` larger for some systems.
Action
To reduce the size of the DCBF part of the IDB, purge the DCBF for all media with expired catalog protection in the IDB, by running the `omnidbutil -purge -dcbf` command on the Cell Manager. Be sure that no Data Protector sessions are running during the purge session. To reduce the growth of the DCBF part of the IDB, change the **Logging** level to **Log Directories**.

Other problems

Interprocess communication problem because Database Session Manager is not running

Problem
While the Data Protector GUI is accessing the IDB, if the Database Session Manager process on the Cell Manager dies or is terminated, the following error displays: `Interprocess communication problem` On the Cell Manager, you notice the following: **Windows systems:** In the Windows Task Manager, the Data Protector process `dbsm.exe` is not displayed. **UNIX systems:** When listing the Data Protector processes using the `ps -ef	grep omni` command, `/opt/omni/lbin/dbsm` is not displayed.
Action
Restart the Data Protector GUI.

MMDB and CDB are not synchronized

Problem
In a MoM environment, the MMDB and CDB may be out of sync as a result of the CMMDB restore.
Action
On the system with the CMMDB installed, execute: `omnidbutil -cdbsync CellManagerHostname` If the CMMDB was changed, execute the command for each Cell Manager in this MoM cell by specifying each Cell Manager in the cell as the *CellManagerHostname* argument.

IDB is corrupted

Problem
Any of the following messages can be displayed:

- `Database is corrupted.`
- `Interprocess communication problem.`
- `Cannot open Database/File.`
- `Error - Details Unknown.`

Action
Recover the IDB.

Merging of a MMDB into the CMMDB fails

Problem
After executing the `omnidbutil -mergemmdb` command, merging of a MMDB into the CMMDB fails with the following error:

`Could not establish connection.`

Action

Before using the `omnidbutil -mergemmdb`, a remote database connection needs to be enabled. To enable establishing a connection, modify the configuration file and restart the services:

1. On MoM client, navigate to the `pg` subdirectory of the defaultData Protector Internal Database directory.
2. Open the `pg_hba.conf` file in text editor and add the following line:

   `host hpdpidb hpdpidb_app` *MoM_Server_IP_Address*`/32 trust`
3. Restart the services on MoM client:

   `omnisv -stop`

   `omnisv -start`

During IDB restore the session completes with errors

Problem
Backup the IDB to a standalone device . When doing IDB restore, the session completes with errors.

After completing upgrade, files for the patch are added in the following location:

`C:\ProgramData\OmniBack\Config\Server\install`

For example `patch_CC`

This is backed up by IDB backup. However, when you try to restore that file (overwrite) you get "`Access denied`" error.

Action

If restoring HPE Data Protectorconfiguration files to original location do the following:

1. Go to `<dp_data>\Config\Server\install\` and identify following files:

   `patch_CC, patch_CORE, patch_CS, patch_DA, patch_DOC, patch_MA, patch_NETAPP, patch_SMISA, patch_VEPA`

2. For all these files, deselect the hidden flag option.
3. Perform IDB restore.
4. Set hidden flag again for the files mentioned earlier.

> **NOTE: Note:** This problem only exists on Windows CMs thus workaround is applicable only for Windows. The same workaround applies if files are restored to another location and these files already exist on those locations.

The DC binary file reports error for DCBF segments

Problem

After preforming IDB restore using the restored database as a new Internal Database, `omnidbcheck -dc` reports errors.

Action

Perform the export and re-import of media where the IDB backup objects are placed.

Point-in-time recovery of PDB Oracle fails with error

Problem

While performing Point-in-time recovery of PDB Oracle, displays the following error:

`PLS-00306: wrong number or types of arguments in call to 'GETCNCTSTR'`

Issue is present in Oracle Bundle patch when performing point-in-time recovery of PDB.

Action

To resolve this problem look for the newer Oracle Patch bundle or contact HPE/Oracle support.

3PAR Oracle ASM IR restore fails after manual abort restore

Problem
In the case of manual abort of IR ASM Oracle database restore and recovery, restart of the session fails with an error.
Action
After failure mount the ASM diskgroups and perform manual recovery from RMAN.

Backup of Pluggable database fails with error: Pluggable database does not exist

Problem
In case where PDB has been dropped from CDB following error displays: ORA-65011: Pluggable database does not exist.
Action
This bug is Oracle specific. Login to Oracle Support page and search for the Bug ID **18967466**. `Bug 18967466 : ALTER DATABASE BEGIN BACKUP" COMMAND FAILS DUE TO ORA-65011 IF PDB HAS BEEN DROPED`

Duplicate reports due to incorrect NLS settings

Problem

When error is reported while performing Oracle restore to a specific date, then check the value of `NLS_LANG` variable of Oracle user and the output of the following SQL commands:
 	
`SELECT * FROM NLS_SESSION_PARAMETERS;`
 	
`SELECT * FROM NLS_INSTANCE_PARAMETERS;`
 	
`SELECT * FROM NLS_DATABASE_PARAMETERS;`
 	
The problem might be due to conflicting `NLS_LANG`, `NLS_LANGUAGE`, `NLS_DATE_FORMAT` or `NLS_DATE_ LANGUAGE` settings.

Action
The NLS settings must be consistent. Export the `NLS_LANG` variable to the value appropriate to the language or character set in the database.

Chapter 9: Troubleshooting Reporting and Notifications

Reporting and notification problems

Data Protector GUI stops responding when the send method is e-mail on Windows

Problem
If you use Microsoft Outlook XP with the latest security patch installed, the following problem appears: when you add a report to a report group specifying e-mail as a send method, and then try to start the report group, the GUI stops responding. The same happens if you configure a notification and select the e-mail send method.

The cause of the problem is that Outlook requires user interaction before sending an e-mail notification. This feature cannot be disabled since it is a part of the Outlook security policy. |
| **Action** |
| - If an SMTP server is available on your network, specify `E-mail (SMTP)` as the send method. This method is the recommended e-mail send method.

- Use the Data Protector CLI to start reports:

  `omnirpt -report licensing -email` *email_address*

  When a warning asking whether you allow sending e-mail on your behalf appears, click **Yes** to receive the report.

  For more information on how to customize security settings, see the *HPE Data Protector Product Announcements, Software Notes, and References*. |

SNMP send method fails

Problem
When sending a report as an SNMP trap, the report does not reach the destination.
Action
Use the SNMP trap send method only for reports that do not exceed the maximum size of the configured SNMP trap.

Chapter 10: Troubleshooting HPE Data Protector Help

Introduction

The HPE Data Protector Help consists of two parts:

- Help topics provide conceptual information, step-by-step procedures, and examples.
- Context-sensitive Help is the dynamic, context-sensitive part of the Help, explaining screens and options in the Data Protector GUI. It is displayed by the Data Protector GUI component called Help Navigator.

The Help is available in two formats: Microsoft HTML Help and WebHelp. Current preferences for the Help viewer in the Data Protector GUI determine which format is used.
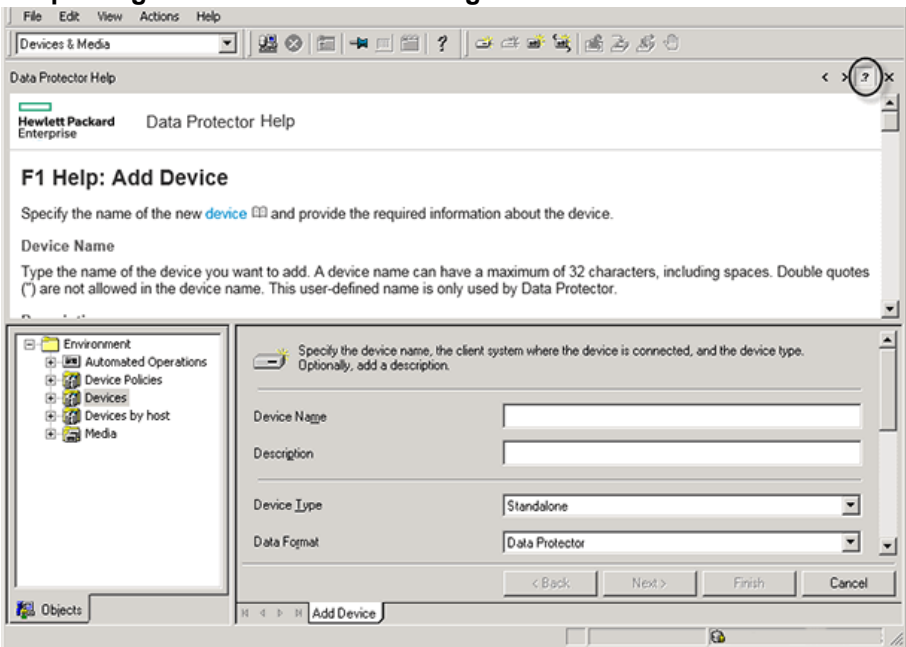
Troubleshooting Help

The Help Navigator contents do not change in parallel with the Data Protector windows

Problem

The Help Navigator contents do not change in parallel with the Data Protector windows.

Help Navigator contents do not change

Action

- If you use the Microsoft HTML Help viewer for viewing the *HPE Data Protector Help* in the HTML Help format (default selection), ensure that the button shown in the figure Troubleshooting HPE Data Protector Help , on the previous page is selected.

- If you use the system default web browser for viewing the *HPE Data Protector Help* in the WebHelp format, go to **File** menu, click **Preferences** and select the **Enable context-sensitive Help Navigator** option. Then restart the Help Navigator.

Chapter 11: Before Calling Support

Before Calling Your Support Representative

If you cannot solve your problem, report it. Before contacting the HPE Customer Support Service, ensure that:

- You have performed the general checks.

  See General checks, on page 10.

- You have also checked if your problem is described in the troubleshooting sections of applicable user guides.

- You have collected the relevant data about the problem you will send to the HPE Customer Support Service: a description of your problem, including the session output (or equivalent output, depending on the type of problem), and a description of your environment.

The HPE Customer Support Service will then provide you with further instructions. You might be asked to:

1. Run Data Protector in the debug mode.
2. Prepare the generated data for sending to the HPE Customer Support Service.

These procedures are described in the following sections. Note that you only need to perform these procedures when the HPE Customer Support Service requests this.

About Debugging

Collect debugs only when the support organization requires them to resolve a technical issue. When Data Protector runs in the debug mode, it creates debug information that consumes a large amount of disk space. Consult the support organization about the required detail level and environmental conditions for debugging.

Enabling debugging

You can start Data Protector in the debug mode in different ways. For debugging options, see Debug syntax, on the next page.

> **IMPORTANT:**
> When Data Protector runs in the debug mode, debug information is generated for every action. For example, if you start a backup session in the debug mode, Disk Agents deliver output on each client backed up in this backup specification.

> **NOTE:**
> To enable debugging of network share backup and restore sessions on Windows Server 2008 and Windows Server 2012 systems, write permissions for the operating system account running such sessions must be assigned to the folder *Data_Protector_program_data*\tmp.

Using the Data Protector GUI

In the File menu, click **Preferences**, and then click the **Debug** tab. Specify the debug options and restart the GUI. The GUI will restart in the debug mode.

Using the OB2DBG variable

The cell server omnirc file

Run debugs on the cell server or on a specific client.

```
OB2DBG=1-200 MA.txt "BMA@computer1.company.com,UMA@computer2.company.com"
```

The client omnirc file

When a program starts it will always verify is a omnirc variable is set locally. Run debugs only locally on the client.

```
OB2DBG=1-200 bma.txt "BMA,UMA"
```

Using the OB2OPTS variable

Debugging parameters for Data Protector integrations can be set using the OB2OPTS environment variable. You will be instructed how to set this variable by your Support Representative.

To change the default location of debug files on a per-system basis, use the omnirc option OB2DBGDIR.

Debug syntax

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

```
-debug 1-200[,C:n][,T:s][,U] XYZ Progname[@hostname]
```

where:

- 1-200 is the debug range. Specify the range 1-200 unless instructed otherwise. Specify optional parameters as a part of the range parameter, separated by commas:

  - C:n limits the size of debug file to n kilobytes. The minimum value is 4 (4 kB) and the default value is 1024 (1 MB). For more information, see .

  - T:s is the timestamp resolution, where the default value is 1000.

    On some platforms, millisecond resolution might not be available.

  - U is the Unicode flag. If it is specified, the debug files on Windows are written in the Unicode format.

- *XYZ* is the debug postfix, for example DBG_01.txt.
- *host* is a list of clients where debugging is turned on.

Use this option to run the debugging only on the clients specified. Delimit multiple clients by spaces. Enclose the list in quotes, for example: `"computer1.company.com computer2.company.com"`.

Compressing the log files

You can choose to compress the debug log files by specifying the gz option after the range, (1-200,gz). This will create logs in a compressed format and not in plain text format. The logs will be created with the **.gz** extension, and you can use any commercial tool to extract the log files.

Limitations

- This feature is supported only on CM platforms.
- On the Windows VEPA session, the CDpSessionLogerSingelton and the Lotus components ignore the gz flag and will not create the compressed logs.
- This feature will not work with combinations of circular debugging.
- The debug log archive is not usable during an abnormal termination.

Debug Options

- **Range**: 1-200 is the debug range. Specify an extended range when instructed. Specify optional parameters as a part of the range parameter, separated by commas. When setting a large range the debug files will be large. Make sure there is enough space in the debug files repository. The range can be split. The separator can be a ",", or a "space" within a double quoted string. For instance, `-debug "1-99 104-140" debug.txt` can be used.
- **Circular debugs**: C:n limits the size of debug files to n kilobytes. The minimum value is 4 (4kB) and the default value is 1024 (1 MB).
- **Timestamp in seconds and milliseconds**: T:s is the timestamp resolution, accepted values are 0,1 and 1000, where the default value is 1, 1000 means the resolution is one millisecond and 0 means timestamps are turned off.
- **Debug files in Unicode format**: U is the Unicode flag. If it is specified, the debug files on Windows are written in the Unicode format.
- **Postfix**: XYZ is the debug postfix, for example *My_debug.txt*.

  > **NOTE: Note**: The postfix can be used to redirect the debug files to another directory. The destination directory must exist and the permissions to the full path need to be correct for the process writing the debugs. For example, `<DirPath>/My_debug.txt`.

- **Program and hostname**: *select* is a list of clients where debugging is turned on. Use this option to run the debugging only on the clients specified. Delimit multiple clients by spaces. Enclose the list in quotes. For example, `progname[@hostname] [;progname@[@hostname]]`.

Necessary debug files

General debugs

In most cases general debugs are 1-200 range. The full debugs can be large, specific with DA and MA debug files.

Veagent debug log files

If a problem is related to the VEAgent backup host the following general setting is recommended. From the GUI Preferences Debug tab, execute `-debug 1-199`.

If the problem is within the VEAgent, the unwanted BMA debugs will be very large. In order to limit the debugs the following is recommended.

Create a VEAgent backup host omnirc file or add the following line:

```
OB2DBG=1-199,240 VM.txt "VEPA_BAR,VEPALIB_VMWARE_EXECUTION_THREAD,VEPALIB_
VMWARE,VEPALIB_VMWARE_THREAD"
```

The range 1-199 is sufficient; the 240 range is adding the omni_cell content in the vepa_bar debug file. If networking details are needed use the following range 0-199,240-270.

VMware VDDK log files

For versions 6.21, 7.01 and 8.0, when the vmware integration fails the vddk log files could reveal more information on the root case. To enable, on the VEagent backup host, go to

`C:\ProgramData\OmniBack\Config\client`. Or on linux, `/etc/opt/omni/client`. Edit the file *vepa_vddk.config*, and change the LogLevel to the highest, 6.

VMware Trivia transport logs

To enable TRIVIA debugs you must update *vepa_vddk.config* file. This file is under `/etc/opt/omni/client` or `C:\ProgramData\OmniBack\Config\client` on the Vepa backup host. Edit the file with log level 6. To collect the trivia output from VMware you should enable debugs for the VEAgent. The transport logs are interlaced with the executed commands in the `VEPALIB_VMWARE_EXECUTION_THREAD` file.

VMware log files

The Management agent (hostd), VirtualCenter Agent Service (vpxa), and VirtualCenter (vpxd) logs are automatically rotated and maintained to manage their growth. Information in the logs can be lost if the logs are rotated too quickly. For more information, see http://kb.vmware.com/kb/1001457.

VMware ESX(i) log files

The esx(i) host has log files of all activities performed, e.g. snapshot creation, removal …etc. The log files are text files starting with hostd and are zipped once full. hostd.log is the active log file. The files are located physical on datastore (e.g. `/var/log ->/scratch/log->/vmfs/volumes/4e265cdb-6b91f4b2-bc38-e4115b13545a/log`).

vCenter Server trivia log files

Enabling trivia level logging is normally done by navigating to Administration > vCenter Server Settings > Logging Options > Trivia.

Vepa_bar localdump in case of crash on Windows

See http://msdn.microsoft.com/en-us/library/windows/desktop/bb787181%28v=vs.85%29.aspx. Edit the registry, and add *vepa_bar.exe* under LocalDumps.

Media Agent debugs

For Media Agent specific problems, the following general guidelines can be applied:

- 1-200 for most common cases
- 19

- 1-300 for SHMIPC
- 1-350 for consolidation
- 1-505 for memory tracking

Limiting the maximum size of debugs

Data Protector can run in a special debug mode called circular debugging. In this mode, debug messages are added until the size of the debug file reaches a preset size (*n*). The counter is then reset and the oldest debug messages are overwritten. This limits the debug file size, but does not affect the latest records.

Using this mode is recommended only if the problem occurs near the end of the session or if Data Protector aborts or finishes soon after the problem has occurred.

With circular debugging turned on, an estimate of the maximum required disk space is as follows:

System	Maximum disk space required
Media Agent client	2*n [kB] for each running Media Agent in a backup or restore session
Disk Agent client	2*n [kB] for each mount point in a backup or restore session
Cell Manager	2*n [kB]
Integration client	2*n [kB] * *Parallelism*

For Inet and CRS debugging, the upper limit cannot be reliably determined because separate debug files are produced for various actions.

Names and locations of debug files

The debug postfix option is used for creating debug files in the default Data Protector temporary files directory:

On Windows systems: *Data_Protector_program_data*\tmp

UNIX systems: /tmp

The files are named

OB2DBG_*DID__Program_Host_PID_XYZ*

where:

- *DID* (debugging ID) is the process ID of the first process that accepts the debugging parameters. This is the ID of the debugging session and is used by all further processes.
- *Program* is the code name of the Data Protector program writing the debug file.
- *Host* is the client where the debug file is created.
- *PID* is the process ID.
- *XYZ* is the postfix as specified in the -debug parameter.

Once the backup or restore session ID *SID* is determined, it is added to the file name:

OB2DBG_*DID_SID_Program_Host_PID_XYZ*

Processes that add the *SID* are BMA/RMA, xBDA/xRDA, and other processes started by the session, but not by the BSM/RSM itself.

> **NOTE:**
> The session ID helps you identify sets of debug files. Other debug files may belong to the same session and you may need to provide them as well.

A `ctrace.log` file is generated on the Cell Manager, containing information where (on which clients) debug files are generated and which debug prefixes are used. Note that this file does not contain a complete list of all generated files.

To change the default location of debug files on a per-system basis, use the omnirc option `OB2DBGDIR`.

Debugging Inet

> **NOTE:**
> `Inet` is a service on windows platform and needs to be restarted for `omnirc` entry to take affect:
>
> (sc stop OmniInet && sc start OmniInet).

To enable only inet debugs, modify .omnirc file on the inet client:

a) To enable only `inet` debugs: `OB2DBG=1-200 inet.txt INET,INET-THREAD`

b) To enable all debugs: `OB2DBG=1-200 all.txt`

Debugging the CRS

Windows systems:

<Data Protector bin>\crs -redebug <range> <postfix> <select>

UNIX systems:

<Data Protector lbin>/crs -redebug <range> <postfix> <select>

> **CAUTION:**
> Do not stop the CRS from Windows Service Control Manager, as this will cause the Data Protector cluster group to failover.

HPE Serviceguard/Symantec Veritas Cluster Server Environment:

1. To start the debugging: `crs -debug <ranges> <postfix> [<select>]`, or put `OB2DBG` to the omnirc file before starting the CRS.

2. To stop the debugging: `/opt/omni/lbin/crs -redebug`

3. To restart the debugging: `crs -redebug <ranges> <postfix> [<select>]`

Debugging the AppServer

Viewing detailed AppServer logs

By default, the AppServer logs show the messages for `warn` level. To view detailed AppServer logs, modify the `level name` parameter in the `standalone.xml` file as shown in the following code:

```
<size-rotating-file-handler name="DP_LOGGER" autoflush="true">

    <level name="ALL"/>

        <formatter>

        <pattern-formatter pattern="%d{HH:mm:ss,SSS} %-5p [%C{1}:%L:%t]
        %s%E%n"/>

        </formatter>

        <file relative-to="jboss.server.log.dir" path="DPServer.log"/>

        <rotate-size value="10M"/>

        <max-backup-index value="5"/>

        <append value="true"/>

        </size-rotating-file-handler>
```

Restart the AppServer after you make any changes in the `standalone.xml` file.

Viewing detailed WildFly logs

To view detailed WildFly logs, add the `<level name>` parameter to the `standalone.xml` file, before the `<root logger>` tag. After you add the parameter, the code in the `standalone.xml` must appear as following:

```
<logger category="org.jboss.as">

    <level name="ALL" />

</logger>

<root-logger>

    <handlers>

    <handler name="CONSOLE"/>

    <handler name="FILE"/>

    </handlers>

</root-logger>
```

Restart the AppServer after you make any changes in the `standalone.xml` file.

Enable statistics on WildFly datasource

Open the `standalone.xml` file, and add the attribute `statistics-enabled="true"` to the datasource definition, as shown below:

```
<datasource jta="true" jndi-name="java:jboss/datasources/HPJobControlEngineDS"
pool-name="HPJobControlEngineDS" use-ccm="true" statistics-enabled="true">
```

```
<datasource jta="true" jndi-name="java:jboss/IDBPostgreSQLDS" pool-
name="IDBPostgreSQLDS_Pool" use-java-context="true" use-ccm="true" statistics-
enabled="true">
```

```
<datasource jta="false" jndi-
name="java:jboss/datasources/HPJobControlEngineQuartzDS" pool-
name="HPJobControlEngineQuartzDS" use-ccm="true" statistics-enabled="true">
```

Restart the AppServer after you make any changes in the `standalone.xml` file.

You can view the statistics in the Microsoft Management Console (MMC). Select Server: Standalone Server > Monitor: Subsystems > Subsystem: Datasources to view the data.

Debugging Scheduler and Missed Job Executions

To debug Scheduler and Missed Job Executions, view the Application Server Logs.

Open `server.log` and review the output for more information, error codes and error messages.

For more information, see Location of log files.

Preparing the Generated Data to Be Sent to the HPE Customer Support Service

The HPE Customer Support Service might ask you to gather and send them data they need to resolve a technical issue. Since Data Protector operates in large network environments, the data might sometimes be difficult to gather. The Data Protector `omnidlc` command is a tool for collecting and packing log, debug, and getinfo files. Use this command if this is requested by the HPE Customer Support Service.

The `omnidlc` command can be run from the Data Protector CLI or from the Data Protector GUI. Both methods are described in this section.

> **NOTE:**
> The `omnidlc` command cannot be used to collect the Data Protector installation execution traces. For details of how to create and collect these, see the *HPE Data Protector Installation Guide*.

About the omnidlc command

After Data Protector debug data has been generated, the `omnidlc` command can be used to collect Data Protector debug, log, and getinfo files from the Data Protector cell (by default, from every client). The command transfers the data from selected clients to the Cell Manager where it is then packed.

The command can also selectively collect the data, for example, only log files from a certain client, or only debug files that were created during a particular Data Protector session.

> **NOTE:**
> When object consolidation is scheduled as part of a post-backup session, backup and

> consolidation sessions get different session IDs. However, the debug ID is the same for both backup and consolidation. In this case, if you run the `omnidlc` command and specify the consolidation session ID using the `-session` parameter, debugs will be collected for both backup and consolidation.

Limitations

- The command can only be run on Cell Managers.

- In a MoM environment, you can only collect data for each Data Protector cell separately by running the command from the respective Cell Manager.

- If you moved debug files from the default directory, specify the new location using the `-debug_loc Directory1` option. Otherwise, debug files will not be collected.

- When a debug and log file collector is used on HP OpenVMS, the following applies:

  - The OpenVMS ODS-2 disk structure file name can contain the maximum of 39 characters.

  - As OpenVMS systems do not have the `get_info` utility, the `get_info.out` file is blank and is not collected.

  - The `omnidlc` command run with the `-session` option 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.

Using the omnidlc command from the CLI to process debug files

Limiting the scope of collected data

To limit the scope of collected data, use the following `omnidlc` command options:

```
{-session SessionID | -did DebugID | -postfix String | -no_filter} [-hosts List] [-
no_getinfo] [-no_config] [-no_logs] [-no_debugs] [-debug_loc Directory1
[Directory2]...]
```

You can combine the following features:

- To collect data only from the selected clients, use the `-hosts List` option. Specify the names of the clients, separated by spaces.

  In a cluster environment, use the `-hosts` option, specifying the cluster nodes. If this option is not used, the data is collected from the active node only.

- To exclude the getinfo, the configuration information, log, or debug log files from the collected data, use the `-no_getinfo, -no_config, -no_logs`, or `-no_debugs` option, respectively. Note that `-no_getinfo` is not applicable for HP OpenVMS systems.

- To collect the debug files only from a specific session, use the `-session SessionID` option. Note that on OpenVMS, all available logs are collected.

- To collect the debug files matching a specific debug ID, use the `-did DebugID` option.

- To collect the debug files matching a specific postfix, use the `-postfix String` option.

- To collect all debug files, use the `-no_filter` option.
- To collect debug files not only from the default debug files directory but also from other directories, use the `-debug_loc Directory1[Directory2]...` option. Note that the subdirectories are excluded from the search. If a specified directory does not exist on a particular client, the directory is ignored.

Segmentation of data

If a file to be sent to the Cell Manager is larger than 2 GB, the file is split into 2 GB-sized chunks. An extension ranging from `s001` to `s999` is appended to each chunk. A second extension (`.gz`) is added if the files are compressed.

On the Cell Manager side, if the size of all collected compressed or uncompressed files exceeds 2 GB, the collected files are packed in 2 GB-sized packages with an extension ranging from `s001` to `s999`.

Disabling compression of the collected data

By default, the collected data is compressed before it is sent to the Cell Manager. To disable the compression, use the `-no_compress` option.

Saving packed data

By default, the data is sent over the network to the Cell Manager, where it is packed and saved in the current directory as the file `dlc.pck`.

The packed file includes a generated directory structure that includes the hostnames, paths, and the collected files of the clients involved.

Limitations

- The size of the resulting packed file cannot exceed 2 GB. In such a case, do not pack the data.

Use the `-pack Filename` option to pack and save the data:

- With a different file name. Specify the `Filename` as a file name.
- In a different directory and with a different file name. Specify the `Filename` as a full pathname.

Saving unpacked data

To leave the data unpacked and save it, use the `-depot [Directory]` option. The files are collected within the `dlc` subdirectory. If the `Directory` is not specified, the files are saved on the Cell Manager within the `dlc` directory in the default Data Protector temporary files directory.

The directories for the packed or unpacked files are generated as follows:

`./dlc/client_1/tmp/debug_files`

`./dlc/client_1/log/log_files`

`./dlc/client_1/getinfo/get_info.txt`

`./dlc/client_2/tmp/debug_files`

`./dlc/client_2/log/log_files`

```
./dlc/client_2/getinfo/get_info.txt
```

```
...
```

Estimating the required space

To display the amount of disk space required on the Cell Manager to gather the data, use the `-space` option.

Deleting debug files on clients

To delete the collected data on the clients, use the `-delete_dbg` option. Note that only debug files are deleted; getinfo and log files are not deleted. On HP OpenVMS, if run together with the `-session` option, the `omnidlc` command does not delete any debugs from the debug files directory.

Deleting information about debug files

To delete `ctrace.log` files containing the information where (on which clients) debug logs are generated and which debug prefixes are used, use the `-del_ctracelog` option. Note that if used together with the `-hosts List` option, the command deletes `ctrace.log` files on specified clients only. Otherwise, `ctrace.log` files on all clients in a cell are deleted.

> **NOTE:**
> Use this option for `ctrace.log` files cleanup. Note that if this file is deleted, the debug log collector will only get debugs from the default `dlc` residing in the default Data Protectortemporary files directory and not from other debug directories you specified.

Problems and workarounds

Debug log collection fails

Problem
During the debug log collection operation, `omnidlc` is unable to connect to a client. The following error is displayed:

```
Collection from client1.company.com started.

Error: Data retrieval from client1.company.com failed.

Warning: Collection from client1.company.com incomplete.
```

The problem occurs when a Cell Manager name specified in the configuration file on a client does not match the name of the Cell Manager that requested the debug log collection.
Action
Add the Cell Manager hostname to the `omnidlc_hosts` file located in the default Data Protector client configuration directory.

Additional operations

- To pack unpacked data, compressed or uncompressed, that was sent to the Cell Manager (using the `-depot` option), use the `-localpack [`*`Filename`*`]` option.

  This option packs the directory structure of the current directory (must be the directory containing the `dlc` directory generated by the `-depot` option). If the *`Filename`* argument is not specified, the file `dlc.pck` is created in the current directory.

  This option is equivalent to the `-pack` option, but should be used only if the data was collected using the `-depot` option.

- To get the additional information (for example, screenshots, pictures and the like) from a specified directory on client, use the `-add_info [-any |` *`Host`*`]` *`Path`* option.

  The `-any` option is used when the directory path is the same for all clients.

- To unpack data, use the `-unpack [`*`Filename`*`]` option.

  If the *`Filename`* argument is not specified, the `dlc.pck` file from the current directory is unpacked. The data is always unpacked to the `dlc` directory in the current directory.

  Use this option when the collected data was packed on the Cell Manager either using the `-pack` or `-localpack` option.

- To uncompress a compressed single file, use the `-uncompress` *`Filename`* option. Packed data must be unpacked first.

- To enable verbose output, use the `-verbose` option.

Using the Data Protector GUI to process debug files

During debug sessions, the following types of files can be generated: debug, log, and getinfo

The following debug file operations can be performed in the Data Protector GUI:

- Invoking debug file operations, on the next page

  Debug file operations can be started from different locations within the Data Protector GUI.

- Collecting debug files, on the next page

  Debug files are collected from client systems and stored on the Cell Manager.

- Calculating debug files space, on page 98

  The space required on the Cell Manager for the collected files is calculated.

- Deleting debug files, on page 99

  Debug files are deleted from the client systems.

They can be invoked from the **Internal Database** context or the **Clients** context.

The GUI operations use various options of the `omnidlc` command. Additional operations can be performed on collected files by using the `omnidlc` command directly in the command line interface. For further information, see Using the omnidlc command from the CLI to process debug files, on page 93 or the *HPE Data Protector Command Line Interface Reference*.

When performing any of the operations in the following sections, the `omnidlc` syntax used can be seen in a **Results** window.

Invoking debug file operations

To access debug file operations from the **Clients** context:

1. In the Scoping Pane, expand the **Clients** folder and select the client for which debug file operations are required.

2. Select the operation to perform:

   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space** or **Delete Debug Files.**

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space** or **Delete**

To access debug file operations from the **Internal Database** context:

1. In the Scoping Pane, expand the **Sessions** folder and select the session for which debug file operations are required.

2. Select the operation to perform:

   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space**, or **Delete Debug Files**.

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space**, or **Delete**.

In each case, selecting an operation starts a wizard that guides you through the required steps.

Start/Stop MMD debugging without restarting services

1. To start MMD debugging, while MMD is running, run the following command:

   `mmd.exe -redebug [ranges] [postfix] [select]`

2. To stop MMD debugging, while MMD is running, run the following command:

   `mmd.exe -stopdebug`

Collecting debug files

To collect debug files:

1. Start the Debug File Collector wizard as described in .

   If you started from the Internal Database context by selecting a session, the session will be pre-selected in the Filter section of the wizard Clients page and the clients involved in the session will be selected.

   If you started from the Client context, the clients that you selected there will be pre-selected in the wizard Clients page.

2. In the Clients page, to limit the clients involved:

   a. Select only the client(s) from which you want to collect files. If clients were pre-selected, you can de-select any of them.

   b. Click **Next**.

3. In the Directories page:

   a. Enter any other directories that should be checked for debug files in addition to the default debug files directory and click **Add**.

   b. In the directory tree, select any other directories whose contents you want collected (the contents of sub-directories are not collected).

   c. Click **Next**.

4. In the Options and Operation page:

   a. De-select any debug collection options you don't want to use. For information on the `omnidlc` options, see the *HPE Data Protector Command Line Interface Reference*.

   b. You can specify multiple filter options for collecting the debug logs. The following filter options are available:

      - Session ID: The backup session for which the debug files were produced.
      - Debug ID: The debug session for which debug files were produced.
      - Postfix: The debug filename.
      - Module/s: The modules for which you need the debug logs. You can enter multiple modules, each separated by a comma. Example: BSM,BDSM,VBDA.

   c. Select the operation to be used for storing the debug files on the Cell Manager:

      - **Create Depot** stores the files (not packed) in the default Data Protector temporary files directory, within a `dlc` subdirectory.

        To specify an alternative location, enter an existing directory in **Target Path**. If you want to use the default location, make sure that the text box is clear.

        Using this option allows you to review the collected files and remove any of them before sending the information to support. You can subsequently create a pack file using the CLI command `omnidlc -localpack [Filename]` (for more information, see the *HPE Data Protector Command Line Interface Reference*.

      - **Create Pack File** creates a pack file containing the collected files.

        Specify the full path for the file in **Target Path**.

   d. Click **Finish**.

Calculating debug files space

You can calculate the total space required on the Cell Manager for a debug file collection before actually performing the collection, by entering all the required collection information in the Debug File Space Calculation wizard. After the calculation has been performed, you have the option to start the collection using the specified criteria.

To calculate the total space required on the Cell Manager for a debug files collection:

1. Start the Debug File Space Calculation wizard as described in Invoking debug file operations, on the previous page.

2. In the Clients page, to limit the clients involved:

   a. Select only the client(s) from which you want to collect files. If clients were pre-selected, you can de-select any of them.

   b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix**, or **No filter**, and enter the

required identifier. If **No filter** is selected, all debug files on the selected client(s) will be collected. If a session was pre-selected for you, you cannot change this.

    c. Click **Next**.

3. In the Directories page:

    a. Enter any other directories that should be checked for debug files in addition to the default debug files directory and click **Add**.

    b. In the directory tree, select any other directories whose contents you want collected (the contents of sub-directories are not collected).

    c. Click **Next**.

4. In the Options page:

    a. De-select any debug collection options you don't want to use. For information on the `omnidlc` options, see the *HPE Data Protector Command Line Interface Reference*.

    b. Click **Next**.

The results of the check are displayed in the **Results** tab.

After the calculation, a dialog box appears asking if you want to start the debug file collection.

To start debug file collection using the options selected for the space calculation:

- Click **Yes**.

  The default operation behavior (Create Pack file) will be used on the Cell Manager. See Collecting debug files, on page 97.

Deleting debug files

To delete debug files from clients:

1. Start the Delete Debug Files wizard as described in Invoking debug file operations, on page 97.

2. In the Clients page, to limit which files are deleted:

    a. Select only the client(s) from which to delete files.

    b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier.

    If **No filter** is selected, all debug files on the selected client(s) will be deleted.

    c. Click **Next**.

3. In the Directories page:

    a. Enter any other directories from which debug files should be deleted, in addition to the default debug files directory, and click **Add**.

    b. Click **Finish**.

Examples of Using the omnidlc Command

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 the Cell Manager, using verbose output, run:

```
omnidlc -no_filter -verbose
```

2. To collect only log and debug 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 file `c:\pack\pack.pck` 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 debug files 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 files for the session with the ID `2012/02/16-11`, run:

   ```
   omnidlc -session 2012/02/16-11 -delete_dbg
   ```

6. To display disk space needed on the Cell Manager for the uncompressed debug files with the debug ID `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 `C:\debug` directory on the client `client1.company.com` together with debug log files for the session with the ID `2012/02/12-24`, run:

   ```
   omnidlc -session 2012/02/12-24 -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
   ```

Processing Debug Files using the Data Protector GUI

During debug sessions, the following types of files can be generated: debug, log, and getinfo.

The following debug file operations can be performed in the Data Protector GUI:

- Invoking debug file operations, on the next page

  Debug file operations can be started from different locations within the Data Protector GUI.

- Collecting debug files, on the next page

  Debug files are collected from client systems and stored on the Cell Manager.

- Calculating debug files space, on page 102

  The space required on the Cell Manager for the collected files is calculated.

- Deleting debug files, on page 103

  Debug files are deleted from the client systems.

They can be invoked from the **Internal Database** context or the **Clients** context.

The GUI operations use various options of the omnidlc command. Additional operations can be performed on collected files by using the omnidlc command directly in the command line interface. For further information, see Using the omnidlc command from the CLI to process debug files, on page 93 or the *HPE Data Protector Command Line Interface Reference*.

When performing any of the operations in the following sections, the omnidlc syntax used can be seen in a **Results** window.

Invoking debug file operations

To access debug file operations from the **Internal Database** context:

1. In the Scoping Pane, expand the **Sessions** folder and select the session for which debug file operations are required.

2. Select the operation to perform:

   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space** or **Delete Debug Files.**

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space** or **Delete.**

To access debug file operations from the Clients context:

1. In the Scoping Pane, expand the **Clients** folder and select the client for which debug file operations are required.

2. Select the operation to perform:

   - Right-click on the selection and select the required operation: **Collect Debug Files**, **Calculate Debug Files Space** or **Delete Debug Files.**

     or

   - From the menu bar, select **Actions -> Debug Files** and then **Collect**, **Check Space** or **Delete.**

In each case, selecting an operation starts a Wizard that guides you through the required steps.

Collecting debug files

1. Start the Debug File Collector wizard as described in Invoking debug file operations, above.

   If you started from the Internal Database context by selecting a session, the session will be pre-selected in the Filter section of the wizard Clients page and the clients involved in the session will be selected.

   If you started from the Client context, the clients that you selected there will be pre-selected in the wizard Clients panel.

2. In the Clients page, to limit the clients involved:

   a. Select only the client(s) from which you want to collect files. If clients were pre-selected, you can de-select any of them.

   b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier. If **No filter** is selected, all debug files on the selected client(s) will be

collected. If a session ID was pre-selected for you, you cannot change this.

    c. Click **Next**.

3. In the Directories page:

    a. Enter any other directories that should be checked for debug files in addition to the default debug files directory and click **Add**.

    b. In the directory tree, select any other directories whose contents you want collected (the contents of sub-directories are not collected).

    c. Click **Next**.

4. In the Options and Operation page:

    a. De-select any debug collection options you don't want to use. When first opened, the selections match the standard defaults used by the `omnidlc` command. For information on these, see the *HPE Data Protector Command Line Interface Reference*.

    b. Select the operation to be used for storing the debug files on the Cell Manager:

- **Create Depot** stores files (not packed) in the default Data Protector temporary files directory within a `dlc` subdirectory.

  To specify an alternative location, enter an existing directory in **Target Path**. If you want to use the default location, make sure that the text box is clear.

  Using this option allows you to review the collected files and remove any of them before sending the information to support. You can subsequently create a pack file using the CLI command `omnidlc -localpack [`*`filename`*`]` (for more information on this, see the *HPE Data Protector Command Line Interface Reference*.

- **Create Pack File** creates a pack file containing the collected files.

  Specify the full path for the file in **Target Path**.

    c. Click **Finish**.

Calculating debug files space

You can calculate the total space required on the Cell Manager for a debug file collection before actually performing the collection, by entering all the required collection information in the Debug File Space Calculation wizard. After the calculation has been performed, you have the option to start the collection using the specified criteria.

To calculate the total space required on the Cell Manager for a debug files collection:

1. Start the Debug File Space Calculation wizard as described in .

2. In the Clients page, to limit the clients involved:

    a. Select only the client(s) from which you want to collect files. If clients were pre-selected, you can de-select any of them.

    b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier. If **No filter** is selected, all debug files on the selected client(s) will be collected. If a session was pre-selected for you, you cannot change this.

    c. Click **Next**.

3. In the Directories page:

a. Enter any other directories that should be checked for debug files in addition to the default debug files directory and click **Add**.

b. In the directory tree, select any other directories whose contents you want collected (the contents of sub-directories are not collected).

c. Click **Next**.

4. In the Options page:

a. De-select any debug collection options you don't want to use. When first opened, the selections match the standard defaults used by the `omnidlc` command. For information on these, see the *HPE Data Protector Command Line Interface Reference*.

b. Click **Next**.

The results of the check are displayed in the **Results** tab.

After the calculation, a dialog box appears asking if you want to start the debug file collection.

To start debug file collection using the options selected for the space calculation:

- Click **Yes**.

  The default operation behavior (Create Pack file) will be used on the Cell Manager. See .

Deleting debug files

To delete debug files from clients:

1. Start the Delete Debug Files wizard as described in .

2. In the Clients page, to limit which files are deleted:

a. Select only the client(s) from which to delete files.

b. In **Filters**, select the filter criteria: **SessionID**, **DebugID**, **Postfix** or **No filter** and enter the required identifier.

If **No filter** is selected, all debug files on the selected client(s) will be deleted.

c. Click **Next**.

3. In the Directories page:

a. Enter any other directories from which debug files should be deleted, in addition to the default debug files directory, and click **Add**.

b. Click **Finish**.

Example of Collecting Data to Be Sent to the HPE Customer Support Service

To collect debug, log, and getinfo files for problems occurring during backup sessions involving one client and the Cell Manager:

1. Reduce the error environment as much as possible:
   - Create a backup specification that contains just one or a few files or directories.
   - Include only one failing client in the debug run.

2. Create an `info` text file that contains the following:
   - Hardware identification of the Cell Manager, Media Agent, and Disk Agent clients. For example, `HPE-9000 T-600 Series`; Vectra XA.
   - The SCSI controller's name, for example, `onboard_type/Adaptec xxx/...` for Windows Media Agent clients.
   - Topology information obtained from the `omnicellinfo -cell` command output.
   - The output of the `devbra -dev` command if you have issues with backup devices.

3. Discuss the technical issue with the support organization and request the following information:
   - Debug level (For example, `1-200`. This is a command option needed later.).
   - Debug scope (For example, client only, Cell Manager only, every system.).

4. Exit all user interfaces and stop all other backup activities in the cell.

5. To collect Inet or CRS debugs as well, restart the Inet or CRS service on the Cell Manager in the debug mode.

6. On the Cell Manager, start the GUI in the debug mode:

   `manager -debug 1-200 error_run.txt`

   You can define the postfix of the debug file names created by substituting the `error_run` text with your preference.

7. Reproduce the problem using Data Protector.

8. Exit all user interfaces to quit the debug mode.

   If you collected Inet and CRS debugs as well, restart the Data Protector services on the Cell Manager without the debug option.

9. On the Cell Manager, run:

   `omnidlc -postfix error_run.txt`

   The command compresses the log, getinfo, and debug files with the `error_run.txt` postfix on the client and sends them over the network to the Cell Manager, where they are packed and saved in the `dlc.pck` file in the current directory.

10. E-mail the packed files (`dlc.pck`) to the support organization.

11. Delete the created debug files (with the `error_run.txt` postfix) on the client by running the following command on the Cell Manager:

    `omnidlc -postfix error_run.txt -delete_dbg`

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Troubleshooting Guide (HPE Data Protector 10.02)

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to sw-doc@hpe.com.

We appreciate your feedback!