Hewlett Packard
Enterprise

Data Protector

Software Version: 10.02

Product Announcements, Software Notes, and References

Document Release Date: December 2017

Software Release Date: December 2017

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: Announcements

HPE Data Protector automates high performance backup and recovery, from disk or tape, over unlimited distances, to ensure 24x7 business continuity, and seamless integration with HPE storage hardware solutions. Data Protector delivers innovation and performance at a much lower cost than competitive solutions, while offering flexibility, scalability, and performance. Data Protector is an important member of the fast-growing HPE Software portfolio and offers the unique advantage of being able to source hardware, software, and award winning service offerings from a single, trusted source. Data Protector is both easy to deploy and use. It has a simple installation, automated routine tasks, and centralized licensing facility that reduces costs and data center complexity.

Now announcing its latest version: Data Protector 10.02.

What is supported?

Detailed information about supported platforms, devices, and integrations is available in the support matrices, which can be found on any Data Protector installation package (zip/tar) in the `\DOCS\support_matrices` directory. The following support matrices are available in Portable Document Format (PDF):

- *HPE Data Protector 10.02 3PAR Support Matrix*
- *HPE Data Protector 10.02 Device Support Matrix*
- *HPE Data Protector 10.02 Disaster Recovery Support Matrix*
- *HPE Data Protector 10.02 Network Attached Storage (NAS) Support Matrix*
- *HPE Data Protector 10.02 Platform and Integration Support Matrix*
- *HPE Data Protector 10.02 Virtualization Support Matrix*
- *HPE Data Protector 10.02 VSS Integration Support Matrix*
- *HPE Data Protector 10.02 Zero Downtime Backup and Instant Recovery Support Matrix for HPE P6000 EVA Disk Array Family Using SMI-S Agent*
- *HPE Data Protector 10.02 Zero Downtime Backup and Instant Recovery Support Matrix for HPE P9000 XP Disk Array Family*
- *HPE Data Protector 10.02 Zero Downtime (Split-Mirror) Backup Support Matrix for EMC Arrays*
- *HPE Data Protector 10.02 Zero Downtime Backup Support Matrix for Non-HPE Storage Arrays*

For the latest version of support matrices on the Web, see https://softwaresupport.hpe.com/.

In the event of hardware or software failures on third-party products, please contact the respective vendor directly.

Commands of the Data Protector command-line interface (CLI) are documented in the *HPE Data Protector Command Line Interface Reference*.

Support for earlier agent versions

Wherever possible, Data Protector components on all clients in a Data Protector cell should be upgraded to version 10.02 during the regular upgrade process. This ensures that customers can benefit from the full

feature set of Data Protector 10.02 on all systems in a cell.

Nevertheless, Disk Agent and Media Agent components of an earlier Data Protector version (7.00, or 8.00) are supported in a 10.02 cell with the following constraints:

- The earlier product version is still supported by HPE as an independent product. To check the announced end-of-support dates for HPE products, see the webpage https://softwaresupport.hpe.com/.

- Support is limited to the feature set of the earlier Data Protector version.

- If you are performing operations involving clients on different systems, all agents of the same type (for example Media Agents) must be of the same version.

- Earlier Media Agent component versions are not supported in combination with NDMP servers.

- If one Data Protector component on a client is upgraded to 10.02, all other components have to be upgraded to 10.02 as well.

If you encounter problems establishing a connection with agents of an earlier product version, consider upgrading to 10.02 as the first resolution step.

Updated information

For the latest information about the product, see the Data Protector website http://www.hpe.com/software/dataprotector.

> **IMPORTANT:**
> For the latest version of the Data Protector documentation set, including corrections and last-minute updates due to known issues, see https://softwaresupport.hpe.com/.

Chapter 2: Product features and benefits

The section lists all the new features and benefits added in Data Protector 10.02.

New features in Data Protector 10.02

- Scheduler Enhancements
- Recovery Manager Central (RMC) support
- Support for GRE with Microsoft Exchange 2016

This section provides a brief description of the key Data Protector features that are introduced in the 10.02 release.

Scheduler Enhancements

With Data Protector 10.02, the following scheduler enhancements are added:

- **Minutes and Hours**: You can now schedule the jobs to recursively in minutes or hours frequency pattern.
- **Debug**: A new debug option is added that enables creation of debug logs for a particular schedule.

> **NOTE:**
> To ensure that the Scheduler works correctly after upgrading, make sure that you clear the IE cache immediately after upgrading to Data Protector 10.02.

Recovery Manager Central (RMC) support

With Data Protector 10.02, Recovery Manager Central (RMC) 4.0 and 4.1 are supported.

Support for GRE with Microsoft Exchange 2016

With Data Protector 10.02, Microsoft Exchange 2016 is now supported along with Granular Recovery Extension (GRE).

Features added in previous releases

The following key features were introduced in Data Protector 10.01:

- Network multihoming support
- NetApp Cluster Support
- Scheduler improvements
- MS SharePoint 2013 GRE support with SQL Availability Groups
- Auto removal of failed objects
- Direct I/O support on Linux and AIX operating systems

- VMware 6.5 Update 1 and VMFS 6 support
- Oracle 12c SYSBACKUP compatibility
- SAP archive backup sessions successful
- DD OS 6.1 and DDboost 3.4 support

This section provides a brief description of the key Data Protector features that are introduced in the 10.01 release.

Data Protector 10.01

Network multihoming support

In Data Protector, multihoming environment refers to a system that is connected to multiple networks. If a client has multiple network interfaces (hostnames) then Data Protector transfers data using the hostname that has been imported to the cell.

NetApp Cluster Support

NetApp Storage residing in cluster environment is supported.

Scheduler improvements

With Data Protector 10.01, following new features are added to the Scheduler:

- Monthly view: Shows calendar view for the current month, where the number of schedules for each day are listed against each date.

  > **NOTE:**
  > To ensure that the latest monthly view appears correctly after upgrading, ensure that you clear the IE cache immediately after upgrading to Data Protector 10.01.

- Filtering options: Enables you to filter schedules based on the specification type.
- Search: Enables you to run a free text search in Daily view.
- Performance improvements: The following table shows the schedule rendering time for 1300 schedules per day:

	Data Protector 10.00	Data Protector 10.01
Daily view	12 seconds	0.5 seconds
Monthly view	21 seconds	2.7 seconds

MS SharePoint 2013 GRE support with SQL Availability Groups

In Data Protector versions prior to 10.01, SharePoint 2013 Granular Recovery Extension (GRE) did not support SQL Availability Groups in combination with Availability Group listener. Importing database operation was not possible and database restore operation failed. With Data Protector 10.01, SharePoint 2013 Granular Recovery Extension (GRE) supports SQL Availability Groups, which is able

to import databases and perform item recovery in case SharePoint farm uses Availability Group Listener configuration.

Auto removal of failed objects

With Data Protector 10.01, daily maintenance tasks are introduced that delete failed session objects, if these failed sessions were successfully resumed. As a result, the report now does not show an incorrect count of failed objects. A new command `omnidbutil -delete_obsolete_resumed_versions` is also introduced that enables users to manually delete the failed objects.

Direct I/O support on Linux and AIX operating systems

New `omnirc` variables `OB2ODIRECT_BACKUP`, `OB2ODIRECT_RESTORE`, and `OB2ODIRECT_RESTORE_MINIMUM_SIZE` are introduced to enable direct I/O on Linux and AIX operating systems by the Data Protector Disk Agent. However, if the underlying file system does not support direct I/O operations, the old behavior is applied.

VMware 6.5 Update 1 and VMFS 6 support

Data Protector 10.01 provides support for new backup proxies, Virtual Disk Development Kit (VDDK) 6.5 Update 1, and full support for VMFS 6. For more information on the supported backup proxies, see *HPE Data Protector 10.01 Virtualization Support Matrix*.

Oracle 12c SYSBACKUP compatibility

Currently, Data Protector Oracle integration uses SYSDBA as requested user privileges to connect to the database. With the new Oracle 12c version, a new SYSBACKUP user privilege with all required privileges for backup, restore and recover functionalities are provided. This enhancement enables SYSBACKUP user privileges to connect to the Oracle database for 12c Oracle version. The older Oracle versions will continue with the SYSDBA user privileges as before.

SAP archive backup sessions successful

In versions prior to 10.01, SAP Archive log backup status was marked as Failed, if no archive logs were to be backed up. With version 10.01, a new global option `SessSuccessfulWhenSAPNoArchiveLogsBackedUp` is introduced, which if enabled, marks the SAP backup session as successful, even if 0 archive logs were backed up.

DD OS 6.1 and DDboost 3.4 support

Data Protector is now compatible with Data Domain OS 6.1 and DDBoost 3.4 libraries.

Chapter 3: Limitations and recommendations

Limitations

Scalability limitations

Backup infrastructure scalability

Backup infrastructure metric	Limit
Clients in a Data Protector cell	5000
Cell Managers (cells) in a Data Protector Manager-of-Managers (MoM) cell	50
Total number of clients in a MoM environment	50 000 [1]

Internal Database scalability

Specific limits, which are marked as such in the following tables, can be reconfigured by adjusting the Data Protector global options. For details, see the *HPE Data Protector Troubleshooting Guide* and the *HPE Data Protector Help*.

Basic Internal Database capacity	Limit
Data Protector sessions stored in the Internal Database (IDB)	100 million (100 000 000)
Filenames with metadata referenced in the IDB	1 trillion (1012)
Backup objects referenced in the IDB	1 million (1 000 000)
Backup object versions referenced in the IDB	50 million (50 000 000)

Detail Catalog Binary Files capacity	Maximum configurable limit (Predefined default limit)
Detail Catalog (DC) directories	100 (50)

[1] In MoM environments, the total number of clients does not scale linearly.

Detail Catalog Binary Files capacity	Maximum configurable limit (Predefined default limit)
Size per DC directory	2047 TB [1] [2] (200 GB)
Files per DC directory	500 000 (100 000)
DC binary file size	n/a [3]
DC directory low space (minimum difference to the effective limit on the directory size)	n/a [4] (2 GB)

Media Management Database capacity	Limit
Backup media in the Media Management Database (MMDB)	50 million (50 000 000)
Total number of backup media in all MMDBs (or in the CMMDB [5]) in a MoM environment	2.5 billion (2 500 000 000)
Backup media in a media pool	200 000

Concurrency limitations

Backup session concurrency metric	Maximum configurable limit (Predefined default limit)
Concurrent [6] backup sessions	1000 (100)
Total number of concurrent backup sessions in a MoM environment	50 000 [7]
Backup sessions in a day	99 999 [8]

[1]The underlying file system limitations or settings may prevail over this limit.
[2]In the Data Protector GUI, you are only allowed to set amounts up to 10 240 GB (10 TB). You can use the Data Protector omnidbutil command for setting bigger amounts.
[3]The effective limit depends on the underlying file system limitations or settings.
[4]The effective limit for a particular DC directory depends on the configured Data Protector limit for its maximum size.
[5]Centralized Media Management Database.
[6] In this context, "concurrent" means "running concurrently in a Data Protector cell".
[7]This limit cannot be changed.
[8]This limit cannot be changed.

Backup device concurrency metric	Limit
Disk Agent concurrency (device concurrency)	32 [1]
Backup devices (drives) used in a backup, object copy, object consolidation, or restore session	128 [2]
Concurrent [3] physical drives (DLT7000 and lower performing models)	1000
Concurrent physical drives (DLT8000, SDLT, LTO)	500
Concurrent virtual drives (LTO—where drive concurrency is set to 1)	1000

Intrasession concurrency metric	Limit
Backup objects processed concurrently in a session	4096 [4]
Backup media imported at the same time	100

Prerequisites for increasing the limit on concurrent backup sessions

If you increase the value of the `MaxBSessions` global option to a certain amount (for example, near 1000), you may have to modify specific system parameters on the Cell Manager that limit the number of concurrent sessions in general. After such modifications, restart the local Data Protector services with the Data Protector `omnisv` command. The modifications are as follows, and depend on the Cell Manager's operating system.

Windows systems:

The default non-interactive desktop heap size is sufficient for approximately 100 parallel sessions. Therefore, you need to increase the size of the non-interactive desktop heap.

Update the `Windows` value in the Windows Registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\SubSystems` by changing the third numerical value in the parameter `SharedSection=1024,20480,768` from `768` to `10240`.

For example:

```
Windows="%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,10240 Windows=On SubSystemType=Windows ServerDll=basesrv,1
 ServerDll=winsrv:UserServerDllInitialization,3
```

[1] This is the maximum configurable limit. The effective limit for a particular device depends on the configured concurrency for that device in the device configuration or session specification.
[2] This is the maximum configurable limit.
[3] In this context, "concurrent" means "used concurrently in a Data Protector cell".
[4] This is the maximum configurable limit. It depends on the effective limits for the Disk Agent concurrency and the number of backup devices that can be used in a session.

```
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16"
```

HP-UX systems:

You need to adjust the operating system kernel parameters `nproc` and `nkthread`, and possibly other dependent parameters as well. You can perform the adjustments using the `kmtune` command or the System Administration Manager (SAM) application. For instructions, see the HP-UX operating system documentation.

Linux systems:

You need to add the following line into the preconfigured `service omni` parameter group in the file `/etc/xinetd.d/omni`:

```
cps = 1100 10
```

Enhanced incremental backup

- Each new enhanced incremental database can support a maximum of 40 billion files per mount point and a maximum of 40 million files per directory.

- The maximum memory consumption is determined by the largest number of files within one single directory. The approximate maximum memory consumption is 130 MB per 1 million files within one directory.

- Data Protector supports enhanced incremental backup of the following number of files per directory:

    Windows systems (32-bit):

    10 million files

    HP-UX systems:

    5 million files

    Linux systems (32-bit):

    5 million files

Size of file depots used for file library

On Windows, the maximum recommended file depot or slot size is 50 GB, although the standalone file device has been tested on Windows with file depots of up to 600 GB.

On HP-UX, the maximum allowed file depot size is 2 TB. However, for best performance a 50–100-GB depot size is recommended. In Windows environments, configure smaller file depot sizes for better performance. Creating larger files requires more CPU and memory resources. For similar environments, the recommended maximum file depot size is 10–50 GB.

Installation limitations

Data Protector cannot be installed if the installation path:

- Contains non-ASCII characters
- Contains the characters "@" or "#" or "&"

- Contains a directory that ends with the character "!"
- Is longer than 80 characters

Spaces are not supported in the Omniback data directory during an upgrade procedure.

If you are upgrading from a path that has any of the above characteristics, you must migrate the installation to a different directory. See the troubleshooting chapter of the *HPE Data Protector Installation Guide*.

Upgrade limitations

- A backup of the Internal Database, created with previous versions of Data Protector, cannot be restored. After upgrading the Cell Manager, back up the Internal Database before you continue using Data Protector.
- If the stores created using an older Data Protector version are not visible after upgrading, then you should restart the client (where stores reside).

Migration limitations

- Cell Manager can only be migrated to the same Data Protector version.

  To use a new Data Protector version on the system you want to migrate to, upgrade the existing Cell Manager installation to the new version before you start migration.
- Cross-platform migration, for example from a Windows system to an HP-UX system, is not supported.
- Migrating the Data Protector Cell Manager from a clustered environment to a single server environment is not supported.

Platform limitations

UNIX and Linux limitations

- LOFS filesystems are fully supported. However, Data Protector does not recognize directories that are lofs-mounted if they are mounted within the same filesystem. This will result in additional data being backed up.
- Cross-filesystem restore of ACLs (file permission attributes) is not supported. For example, ACLs backed up from the VxFS filesystem cannot be restored to a UFS filesystem and the other way round. File objects however, can be restored to a different filesystem without ACLs.
- Cross-platform restore of ACLs is not supported. This limitation is due to different internal ACL data structures on different operating systems.
- Modification of ACL entries does not affect the modification time of the file object, so the file object (and the modified ACL) is not backed up during an incremental backup.
- The GUI can display a maximum 64 000 items (files in one directory, slots in a library, and so on) in a tree view.
- File names containing quotation marks are not supported.

HP-UX limitations

- Restore of a single file from a disk image is not supported.

- On HP-UX 11.31 that uses new persistent multi-pathing and path-independent Device Special Files (DSFs), backup specifications referring to the old DSF may not work if the old DSF is disabled on the system. In this case, reconfigure the devices and update backup specifications to use the new-style DSF.

Solaris limitations

- If a `csh` script is used for `pre-` or `post-exec`, the `-b` option must be specified in the interpreter specification line: `#!/bin/csh -b`

- On Solaris, `/tmp` is a virtual filesystem in the swap area. If the `/tmp` directory is included in a backup specification, it is backed up as an empty directory. If restoring such backup, a swap area must be configured on the client prior the restore, otherwise the `/tmp` directory cannot be re-created.

- Backup and restore of access control lists (ACLs) on Veritas Cluster File System (CFS) is not supported.

- On Solaris, detection of media types other than Data Protector media is not reliable, due to the use of a number of different block sizes. Do not rely on Data Protector to recognize foreign media.

  Workaround: To prevent Data Protector from automatically initializing a medium it does not recognize correctly, set `InitOnLoosePolicy` global option to `0`. All media then have to be initialized manually.

- Cleaning tape recognition in DDS libraries does not function.

Linux limitations

- After the transition from the ext2 to the ext3 filesystem on Linux systems, the journal will be visible as the `.journal` file in the `root` directory of the filesystem. If the filesystem is not mounted, the journal will be hidden and will not appear in the filesystem.

  Due to the Linux operating system limitations, do not delete this `.journal` file, do not back it up, and do not restore it from backup.

- If you use access control lists (ACLs) and perform backup and restore between 32-bit and 64-bit Linux systems (for example, you perform a backup on a 32-bit Linux system and restore this backup to a 64-bit Linux system), the ACL entries are not restored.

- Cross-platform restore of ACLs between 32-bit and 64-bit Linux operating systems is not supported.

- On Linux systems, before you restore a symbolic link whose owner is not the `root` user, ensure that all directories in the path where the link will be restored have execute permission set for the link owner. Otherwise, the restore session will fail.

- Disaster recovery (Enhanced Automated Disaster Recovery or One Button Disaster Recovery) is not supported if SELinux is enabled.

Mac OS X limitations

- The Internet Protocol version 6 (IPv6) is not supported on Mac OS X operating system.

- Cross file system restore of ACL (Access Control List), extended ACLs, and file attributes is not supported (for example, ACL's backed up from the HFS+ file system cannot be restored to the UFS file system and the other way round).

- Encrypted control communication is not supported on Mac OS X operating system.

Windows limitations

- Windows directory share information can only be restored to a Windows system with the Data Protector Disk Agent. If this requirement is not met, the directory will still be restored, but the Disk Agent will ignore the directory share information.

- Only one CONFIGURATION backup can run on a Windows client at a time.

- Data Protector requires the same name for both, the computer name and the resolving hostname.

- Remote installation using secure shell (SSH) is not supported on Windows platforms.

- Local secure shell installation supports key-based authentication. It does not support other authentication modes.

- Backing up network shared volumes using the VSS functionality is not supported.

- The GUI on Windows systems can display a maximum 64000 items (files in one directory, slots in a library, and so on) in a tree view.

- The name of the file cluster resource used during the installation of the Data Protector Cluster Integration on Windows must not be `omniback`. For details, see the *HPE Data Protector Installation Guide*.

- When browsing with the backup specification editor a Windows client, the Windows user interface lists both online and offline Informix Server dbspaces. To check for databases, use the `onstat -d` command. Available databases are marked with the PO flag.

- On Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 systems, the user performing a network share backup must be a member of the operating system Backup Operators user group and must be added to the Inet configuration on the system where Disk Agent is running (using `omniinetpasswd -add`). In a cluster environment, users must be configured on both nodes.

- On Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, the broadcast message send method is not supported.

- Backed up directory share information of directories which were located on a 32-bit Windows system cannot be restored to a 64-bit Windows system and the other way round. In such restore scenarios, the selected directories and their contents will be restored as expected, but without their share information.

- VSS disk image backup of the logical volumes can be used for disaster recovery only on Windows Sever 2008 systems.

- You can boot the target system over the network only on Windows 2008 Server systems.

- The HPE Data Protector Disaster Recovery GUI is available only on Windows 2008 Server systems. On other Windows systems, a console interface is available.

- IPv6 addresses cannot be used in share names when backing up network share volumes.

- Data Protector Inet service cannot be started if the Windows system is started in Safe Mode with Networking.

Windows 32-bit limitations

- On Windows systems, the native robotics driver (Removable Storage Manager) is automatically loaded to enable tape libraries. To use the library robotics with Data Protector on 32-bit Windows systems, disable the Windows medium changer (robotics) driver before you configure the system with the Data Protector Media Agent.

Windows 64-bit limitations

- The original Microsoft Windows installation CD-ROM is supported for Automated System Recovery (ASR).
- It is not possible to integrate the Data Protector GUI with the Microsoft Management Console (MMC) using the Data Protector OB2_Snap snap-in.
- Data Protector does not support Java web reporting on Windows systems based on the Itanium 2 processor architecture, since Java runtime environment is not supported on this platform.
- On AMD64/Intel EM64T systems, sending notifications and reports by e-mail using MAPI is supported only with Microsoft Outlook Express, and not Microsoft Outlook.

Windows Server 2012 limitations

- Filesystem backup of volumes formatted with the Resilient File System (ReFS) is not supported. Use disk image backup instead.
- Backup of network shared disks is supported without using the VSS for SMB File Shares functionality.

Novell Open Enterprise Server (OES) limitations

- Back up or restore of any GroupWise system files is not supported.
- The Internet Protocol version 6 (IPv6) is not supported for OES cluster configurations.

HP OpenVMS limitations

- The OpenVMS client must be installed locally on the OpenVMS system. There is no support for remote installation from an Installation Server.
- The product can only be installed on the system disk in `SYS$COMMON:[OMNI]`.
- Any file specifications that are passed to the CLI must conform to a UNIX-style syntax:

  `/disk/directory1/directory2/filename.ext.n`

  - The string should begin with a slash, followed by the disk, directories, and file name, separated by slashes.

  - Do not place a colon after the disk name.

- A period should be used before the version number instead of a semi-colon.

- File specifications for OpenVMS files are case insensitive, except for the files that reside on ODS-5 disks.

For example:

An OpenVMS file specification of:

`$1$DGA100:[USERS.DOE]LOGIN.COM;1`

must be specified in the form:

`/$1$DGA100/USERS/DOE/LOGIN.COM.1`

- Patch level display is not available on OpenVMS.

- There is no implicit version number. You always have to specify a version number. Only file versions selected for the backup will be backed up. If you wish to include all versions of the file, select them all in the GUI window, or, using the CLI, include the file specifications under the `Only (-only)` option, including wildcards for the version number, as follows

  `/DKA1/dir1/filename.txt.*`

- If the `Do not preserve access time attributes` option is enabled during a backup, the last accessed date will be updated with the current date and time on ODS-5 disks. On ODS-2 disks, this option has no effect, and all the dates remain unchanged.

- Disk backup is not available on OpenVMS. There is no equivalent to "BACKUP/IMAGE" or "BACKUP/PHYSICAL".

- When the data backed up from an OpenVMS Alpha system is restored or migrated to an OpenVMS Integrity system using Data Protector, some of the default file attributes (such as creation time, last revised time, version limit and some of the file record attributes) may get lost. This also applies to the data restore or migration from Itanium to Alpha.

  Workaround: Manually reset the attributes using the DCL command line.

- The `Backup POSIX hard links as files (-hlink)` option is not available on OpenVMS.

  Files with multiple directory entries are only backed up once using the primary path name. The secondary path entries are saved as soft links. During a restore, these extra path entries will also be restored.

  For example, system specific roots on an OpenVMS system disk will have the `SYSCOMMON.DIR;1` path stored as a soft link. The data for this path will be saved under `[VMS$COMMON...]`.

- Files being backed up or restored are always locked regardless of whether the `Lock files during backup (-lock)` option is enabled or disabled. With the `-lock` option enabled any file opened for write is not backed up. With the `-lock` option disabled any open file is backed up as well. No message is issued when an open file is saved.

- The default device and directory for pre- and post-exec command procedures is `/omni$root/bin`. To place the command procedure anywhere else the file specification must contain the device and directory path in UNIX-style format. `/SYS$MANAGER/DP_SAVE1.COM` is an example of a valid specification.

- If you restore to a location other than the original location, only the disk device and starting directory are changed. The original directory path is added to the destination path to form the new restore location.

- To successfully back up write-protected and shadow disks, enable the `Do not preserve access`

`time attributes` option in the backup specification.

- If the `Do not preserve access time attributes` option is disabled during a backup and if the `Restore Time Attributes` option is disabled during a restore, the last accessed date will be updated with the current date and time on ODS-5 disks. On ODS-2 disks, the original dates will be set on the files.

- The `Move Busy Files (-move)` and `Restore Sparse Files (-sparse)` options are not available on OpenVMS.

- Files backed up from an ODS-5 disk on an OpenVMS system that have extended filesystem names (for example upper and lower case letters, Unicode characters, etc.) may not be restored to an ODS-2 disk.

- If the `Restore Protection Attributes (-no_protection)` option is disabled, the files are created with the default owner, protection and ACL.

- There is no support for a BACKUP/IMAGE equivalence. To make a restored copy of an OpenVMS system disk bootable, the OpenVMS WRITEBOOT utility has to be used to write a boot block onto the restored disk.

- The `omnicheck -patches -host` command is not supported on OpenVMS.

- The `omnirpt -email` command is not supported on OpenVMS. You can use the `-log` option to create a local dump of a report file and use the native OpenVMS mail utility to send an e-mail with this file as an attachment.

- 16-bit Unicode filenames on an ODS-5 disk volume will be displayed in VTF7 (OpenVMS specific) notation on the Cell Manager in the form of `^Uxxyy` for a Unicode character where `xx` and `yy` are the Unicode hex codes for this character. Other valid characters for files on ODS-5 volumes can be specified using the OpenVMS guidelines for extended file specification syntax.

- If an OpenVMS file is restored to a non-OpenVMS platform, file attributes specific to OpenVMS may not be retained (for example record format, backup date, ACL).

- Files that have been saved on non-OpenVMS platforms and are to be restored to an OpenVMS system may lose some file attributes. No ACL will be restored in this case.

- No qualification is done for tape drives which are not supported by OpenVMS. For a complete list of tape drives, see the OpenVMS Software Product Description (SPD).

- HSJ connected tape libraries cannot be autoconfigured. Use manual configuration methods to add these devices to Data Protector.

- Data Protector file library is not supported on OpenVMS ODS-2 disks.

- Restore file to original location with the `-no_overwrite` option will not restore any files.

- Incremental backup will work at the directory level only, because OpenVMS creates a new file with a new version number upon modification of an existing file. Data Protector on OpenVMS allows to create incremental backup at file level only if the filename is exactly the same as the previous, including the version number.

- On the OpenVMS client with the Oracle integration installed, you have to configure a Data Protector `admin` user with the username `<Any>` and the group name `<Any>`. This limitation is due to the lack of the user group name concept on OpenVMS.

- If you run the Media Agent and the Data Protector Oracle integration agent on the same OpenVMS client, modify the group ID of the `omniadmin` user as `DBA` using the `MCR AUTHORIZE` utility.

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

- The OpenVMS ODS-2 disk structure file name can contain a 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 executed with the `-session` parameter does not collect the debug files produced during specified session, because session names are not part of the OpenVMS debug filename. All available logs are collected instead.

- The Oracle environmental variables and `omnirc` options `OB2_RMAN_COMMAND_TIMEOUT` and `OB2_SQLP_SCRIPT_TIMEOUT`, which help improving Oracle Server backup session handling, are not supported on OpenVMS systems.

- The Internet Protocol version 6 (IPv6) is not supported on HP OpenVMS.

- Encrypted control communication is not supported on HP OpenVMS.

- Enhanced incremental backup is not supported.

Limitations on clusters

HPE Serviceguard limitations

- When adding components on HPE Serviceguard, add the components on the active node. Then start the package on the other node, and add the components on this node too.

Limitations on licensing

General licensing limitations

- Both licensing models, the capacity based and traditional cannot coexist in the same Data Protector cell.

- In a MoM environment, you cannot mix both licensing models --- all Cell Managers must use the same licensing method.

License upgrading limitations

- Limitations on advanced backup to disk licensing:

- The library capacity (`VTLCAPACITY`) of a virtual tape library, which was created with a previous version of Data Protector, is by default set to 1 TB after the upgrade to the latest version. You must enter the estimated library capacity value manually through the graphical user interface (GUI) or via the command-line interface (CLI). See the advanced backup to disk example in the *Data Protector licensing* chapter of the *HPE Data Protector Installation Guide*, and the `omniupload` man page or the *HPE Data Protector Command Line Interface Reference*.

Internet Protocol version 6 (IPv6) networking limitations

- Licenses acquired with versions earlier than Data Protector9.00 only support IPv4 and dual IP stack environments and require the Cell Manager to have an IPv4 address. In order to use Data Protector in an IPv6 only environment, the licenses acquired with versions earlier than Data Protector 10.02 should be converted to the Data Protector licensing technology. To convert the keys, follow the procedures provided by the password delivery center.

  This limitation does not apply to licenses acquired with or after Data Protector 9.00 or later.

Limitations on license reporting in a traditional licensing model

- In a cell if the Data Protector Cell Manager and a client is not upgraded , Media Agent on a client cannot send the information about the used disk capacity to the Cell Manager. Consequently, the license checker does not receive the needed information about disk space that is used and cannot report the actual license capacity in use. Therefore, the license checker reports an additional Advanced backup to disk for 1 TB license-to-use is required for such file library.

- Due to the migration of multi-drive server licenses to single-drive licenses, the license enforcement is stronger than the license checking. If a multi-drive server license is installed on a system that is not a drive server, the multi-drive license is not used and the backup may not be possible, although the license checker reports enough appropriate licenses installed.

- Due to the platform independent licenses for slot libraries, the license enforcement is stronger than the license checking. During the backup, Data Protector is checking the licenses for different platforms and the backup may not be possible because of the missing licenses for a specific platform, although the license checker reports enough appropriate licenses installed.

- Since the legacy ZDB and the IR licenses respectively are grouped into one generic license, the license enforcement is stronger than the license checking. During the ZDB backup, Data Protector is checking licenses for different storage arrays and the backup may not be possible due to the missing licenses for a specific storage array, although the license checker reports enough of the zero downtime backup extension and instant recovery extension licenses-to-use (LTU) installed.

Limitations on accessing Home context web pages

- Browser limitation: For the Home context web pages to work correctly, the computer must have Microsoft Internet Explorer v10 or v11 installed.

Limitations with new web-based Scheduler

- The Data Protector Scheduler only supports the 12-hour time format.

- For all type of specifications in the **Scoping pane**, the values for **Scheduled** and **Backup Type** column appear as `n/a` in the **Results Area**, even if the specification is scheduled.

- With the new Scheduler, you cannot schedule a backup specification of the type `disk+tape` as `disk only`. The Scheduler uses the backup type option that was specified during backup specification creation. Also, you cannot reconfigure the backup type during the schedule creation or schedule migration.

However, during migration, the old schedules created using basic scheduler are migrated as-is. For example, in Data Protector 9.0x, if a backup specification was created as `disk+tape` backup, and scheduled as `disk` only; post-migration, the schedule runs as `disk only`, the way it was configured in the basic schedule file.

Limitations on encryption

Limitations on data encryption

- Consolidation of objects backed up with software encryption is not supported.

Limitations on Data Protector MoM environments

- Debug log collection is not supported in MoM environments.

Device and media limitations

- Device filtering during a backup session is supported for Data Protector File System, Data Protector Oracle Server integration, Data Protector Microsoft Exchange Server 2010 integration, and Data Protector Microsoft SQL Server integration.

  Device filtering can be enabled by setting the `global` option `EnableDeviceFilters` to `1`.

  For details on setting the `global` options, see the *HPE Data Protector Help*.

  If you are an existing customer using the `omnirc` variable `OB2DEVICEFILTER` for the device filter feature, you need to migrate the filter tags using the `omnicc -migrate_devfilter [HostName] [-delete_old_devfilter]` command.

  For information on migrating the existing `omnirc` variable based `OB2DEVICEFILTER` tags, see the *HPE Data Protector Command Line Interface Reference*.

- Source-side deduplication backup to StoreOnce Backup system devices configured with Fiber Channel (FC) can be performed on only those systems that are connected to FC. Therefore, before performing this backup, you must ensure that the systems meet the following requirements:

  - Data Protector Disk Agent is installed.

  - Data Protector Media Agent is installed.

  - Fiber Channel connection is configured.

  During backup, you can use the **Systems ready for source-side deduplication** option to filter out systems that do not support the source-side deduplication. However, this option does not filter out systems that do not have the FC connection, which is one of requirements for performing the source-side deduplication backup to StoreOnce Backup system devices configured with FC.

  To verify whether systems have the FC connection, click **Check** to validate the Gateways, while adding the StoreOnce Backup system device.

- Replication between Backup to Disk (B2D) is not supported if the source and target store does not have the appropriate credentials. The replication session fails with the following error message:

```
Permission Denied
```

If the original client with the source store does not have access rights on the target store, the client information is written in the source store which cannot be changed when imported to other clients. This problem cannot be resolved even if the new client has access to the target store. The original information on the source host is written on the store which is a crucial one.

- Reconstruction of broken media soon after a failed backup fails with the following error message: `The media cannot be loaded or open`. This problem occurs on StoreOnce or EMC Data Domain Boost Backup system devices. Therefore, you must wait for some time before triggering the reconstruction.

  The wait time for StoreOnce software deduplication is 2 hours, and the wait time for EMC Data Domain Boost device is 3 hours.

- StoreOnce catalyst does not support reconnect to Data Protector Media Agent when the connection is lost.

NDMP limitations

- Only filesystem backup and restore are available.

- Only `Full` and `Incr1` backup types are supported.

- Maximum device concurrency is 1.

- Device selection as well as filesystem browsing is not possible.

- NDMP devices must use dedicated media pools.

- Localization for the NetApp-specific messages is not possible.

- It is not possible to deselect a subtree of the selected tree to be restored.

- It is not possible to perform a restore of the selected fileset as a tree with a different path name.

- Copying of NDMP backup objects and object mirroring in NDMP backup sessions are not supported.

- NDMP object copy to more than one target device is not supported.

- Medium header sanity check is not supported on NDMP clients.

- The data that was backed up from an NDMP Server of a particular type (for example, NDMP-NetApp) cannot be restored to an NDMP Server of another type (for example, NDMP-Celerra).

- When restoring to another NDMP Server, the device to restore from must be connected directly to the target NDMP Server, must be of the same type, and selected or specified as the restore device in the Data Protector GUI or CLI.

- Restore preview is not supported.

- Restoring data using the Data Protector `Restore by Query` functionality is not supported.

- Direct restore (`DIRECT=Y`) for NDMP backup is not supported in case of `log file` logging level. To restore NDMP backup with `log file` logging level, manually set the NDMP environment variable `DIRECT=N` from the Data Protector GUI (**Restore** context > **Options** tab > **Advanced**).

- Data Protector does not support IPv6 for NDMP backup sessions, therefore the NDMP servers should have IPv4 protocol enabled.

- On 64-bit Linux systems, the Data Protector NDMP Media Agent does not support ADIC/GRAU DAS library devices.

- Three-way backup or restore is only supported in filers with the same major version of firmware (For eg. ONTAP 8.x).
- Three-way backup does not offer remote copy facility wherein the data from NDMP filer is sent to the Media Agent client independently, which then backups the data to the target.
- Cluster Aware Backup (CAB) or restore is supported only on the same cluster filer. Data Protector supports only backup and restore of volumes and files; which are on the same cluster filer as the devices used for backup or restore operation.
- In a non Cluster Aware Backup (CAB) environment, you cannot combine the three-way objects with the local objects during backup specification.

NetApp filer

- On NetApp filers running Data ONTAP version prior to 6.4, direct access restore (DAR) is not supported for directories; a standard restore will be performed instead. This has performance implications only.
- On NetApp filers, running Data ONTAP version 8.0 or newer, direct access restore (DAR) is not possible for backups made before Data Protector 9.05 when DAR support was introduced.
- With the `SMTape` backup type, a backup image of a volume in a particular aggregate type cannot be used for restore to a volume in a different aggregate type.
- With the `SMTape` backup type, a backup image of a volume in a regular aggregate cannot be used for restore to a volume in a larger aggregate, and the other way round.
- The `SMTape` backup type offers only full backup (level-0 backup).
- The `SMTape` backup type enables you to only back up entire file systems. For example, you can back up `/ufs1`, but not `/ufs1/dir1`.

Celerra

- Media copying is not supported for NDMP-Celerra backup sessions.
- If you select both a directory and individual files from another directory and start the restore, only the selected files are restored. To restore both, use standard restore (set the NDMP environment variable `DIRECT` to N).
- Directory direct access restore (DDAR) cannot be used with backup images created with the NDMP volume backup (NVB) option selected.
- The `NVB` backup type enables you to only back up entire file systems. For example, you can back up `/ufs1`, but not `/ufs1/dir1`.
- The `NVB` backup type and file or directory filtering cannot be used together. If both are used, `NVB` takes precedence and the filters have no effect.

Limitations on enhanced incremental backups

- · Limitations on the enhanced incremental database:
  - Hard link detection is not supported with enhanced incremental backups. Hard links for selected object will be backed up as files.

○ To maintain the optimal size of a new enhanced incremental database, Data Protector by default performs a regular check every 30 days. The objects that were deleted from the source volume or were not backed up for a period of 30 days are removed from the database. Thus, the objects that were not backed up for 30 days will be backed up in the Full mode. This is applicable only to HP-UX, Windows, and Linux systems.

- Limitations on incremental backups using Windows NTFS Change Log Provider:

  ○ Hard link detection is not supported with Windows NTFS Change Log Provider incremental backups. Hard links for selected object will be backed up as files.

  ○ Backup of **FAT16** and **FAT32** filesystems is not supported.

  ○ Data Protector does not have private access to the Windows Change Journal which means that other applications might turn it off while Data Protector is using it.

Limitations on virtual full backups

- Virtual full backup is only supported for filesystem data. Data Protector integrations do not support the functionality.

  As the distributed file media format is optimized for virtual full backups, do not use it when performing, for example, an Oracle or Microsoft SQL Server database integration backup. It will only reduce backup performance, without providing any beneficial results.

Limitations on object copy and consolidation

Due to dynamic expansion of gateways and gateway or store or device connection limitations, object copy and consolidation must ensure the following:

- When B2D devices are used as sources, at least one connection should be available for object copy and at least N for object consolidation, where N is the number of source media used for consolidation.

- When B2D devices are used as targets, at least M connections should be available – M being the MIN device setting in the copy or consolidation specification, if only B2D devices are used as targets. If other types of devices are used in parallel, CSM will balance them so that MIN setting is reached, or abort the session otherwise.

Limitations on object verification

General functionality limitations

- Object verification is applicable to backups stored in Data Protector tape format that can be restored using standard Data Protector network restore. It is not applicable to ZDB-to-disk, or the disk part of ZDB-to-disk+tape, which use instant recovery for restore.

- While the source media are being read for object verification, they are unavailable for restore.

- The use of Web Reporting with object verification is not supported.

Application integration limitations

- Object verification only verifies application integration objects from the Data Protector point of view: It can verify object data and delivery of that data to the required destination host. The object verification process does not communicate in any way with integrated applications and so cannot verify restore capability by the applications concerned.

Limitations on application integrations

For integration-specific limitations, see the *HPE Data Protector Integration Guide* and *HPE Data Protector Zero Downtime Backup Integration Guide*.

General limitations

- With database integrations that support restore by starting the integration agent via the CLI, starting such a restore is not supported if you access the client through Remote Desktop Connection and the Media Agent to be used is on the same client.

Oracle limitations

- When using RMAN scripts in Oracle backup specifications, double quotes (") must not be used, single quotes (') must be used instead.
- Data Protector does not check whether database objects to be restored were backed up and exist in the Data Protector Internal Database. The restore procedure simply starts.
- When restoring tablespaces to point in time the RMAN interface has to be used.
- Only the Oracle Restore GUI and Oracle RMAN can be used to recover the Oracle recovery catalog database.
- When restoring a database using the Data Protector GUI to a client system other than the one where the database originally resided, the instance name chosen on the new client system must be the same as that of the original instance name.
- On Windows platforms, a proxy copy backup of an Oracle database is not possible if the database is on raw disks even if the backup seems to complete without any problems reported.
- If an object is deleted from the RMAN Recovery Catalog database, these changes will not be propagated automatically to the IDB and the other way round.
- The Oracle backup set ZDB method is not supported if the database is installed on raw disks.
- Configuration of multiple Oracle databases using user created XLS (Microsoft Office Excel) and CSV (comma separated values) files is not supported on HP OpenVMS clients. Also, this feature cannot be used to configure standby databases and Oracle databases in ZDB environment. The Microsoft Office Excel 2007 Open XML Format is also not supported.
- Backing up Oracle control files with Oracle backup set ZDB method on IPv6-only clients is not supported.
- You cannot use the Data Protector GUI to configure an Oracle database whose files are managed by Automatic Storage Management (ASM) and for which any of the following ASM properties differs

from their default values: home directory of the ASM instance, the authentication mode used by the Data Protector Oracle integration agent to connect to the ASM instance.

MySQL limitations

- MySQL configurations with circular binary log implementation cannot be backed up with Data Protector.
- The incremental backup type is only available for InnoDB database tables. When tables using other MySQL storage engines, are included in an incremental backup session, full backup will be performed for such tables.
- MySQL data can only be restored to a system that hosts the same MySQL version as the system from where the data was backed up.
- Import (restore with the **Import tables to target instance** option) of the database or database tables that use the InnoDB storage engine can be only performed if the MySQL file-per-table setting was enabled for the backup.

SAP R/3 limitations

- If ZDB to tape is used to back up a tablespace in a ZDB environment on Windows systems, and the `ZDB_ORA_INCLUDE_CF_OLFomnirc` option is not set to 1, the backup will fail if the control file is not on the mirrored disk or in the snapshot that will be backed up.
- A split-mirror restore of the SAP R/3 data using the Data Protector GUI on the backup system is executed as a regular filesystem restore, during which ZDB agents (SYMA, SSEA) mount disks on `/var/opt/omni/tmp` (the default mount point). Since this is a restore of application data, VRDA restores files to the original mount points. Therefore, the data is not restored to EMC Symmetrix or P9000 XP Array disks, but to the root partition instead.

Informix Server limitations

- On Windows systems, cold restore of non-critical dbspaces is not possible.

Microsoft SQL Server limitations

- Backup preview is not supported.
- Backup compression is supported only by SQL Server 2008 Enterprise and later.
- A data file belonging to a database which was backed up with the option **Concurrent streams** set to more than 1 cannot be restored. You can only restore the entire database.

Microsoft Exchange Server limitations

- Backup preview is not supported.

Microsoft Volume Shadow Copy Service limitations

Common VSS limitations

- Preview is not supported for any type of VSS sessions: backup, restore, zero downtime backup, and instant recovery.
- The **Restore files to temporary location** mode is not available for the DPM *Database* writer components. Because the files were backed up by another writer (MSDE Writer in this case), they are not shown in the restore page. Only the **Restore components** mode is available in such cases.

Microsoft Exchange Server 2003

- Due to a Microsoft Exchange Server 2003 writer issue, non-Latin characters (for example, Japanese characters) for Exchange store or storage group names are not supported.

Microsoft Virtual Server 2005

- Cluster backup of Microsoft Virtual Server 2005 is not supported. You can back up only individual nodes.

Microsoft SQL Writer

- Microsoft SQL Writer does not support Microsoft SQL database restore to another system. If you try to perform a restore, only files are restored.

Data Protector Virtual Environment Integration limitations

VMware limitations

- After you upgrade to Data Protector 9.05 or later, you cannot restart the failed VMware backup sessions from earlier Data Protector versions.
- After you upgrade from 7.03 or earlier versions to , you cannot run incremental or differential backups without running a full backup.
- Power On and Live Migrate operations from StoreOnce catalyst are supported only with Linux backup hosts.
- The SAN transport mode falls back to NBDSSL on the vSphere 5.5 environment, after an upgrade to VDDK 6.0 Update 1.
- For Changed Block Tracking requirements, see the following URL:
  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128
- 3PAR Zero Downtime Backup (ZDB) and Instant Recovery of virtual machines on vSphere VVol (Virtual Volume) datastore are not supported. So, it is recommended to ensure that VMs are not hosted on VVol datastores before starting a ZDB backup. In case, VMs are hosted on VVols in the Datacenter, which is selected for backup, the following Warning message is displayed:

```
[Warning] From: VEPALIB_VMWARE@hostname "/Datacenter" Time: <Date> <Time>
ZDB backups are not supported with vSphere Virtual Volumes. Skipping Virtual
Machine 'vm_name'...
```

Lotus limitations

- On Solaris and AIX systems, offline restore is not available for Lotus Notes/Domino Server 7.0 and later versions.
- On Solaris systems, restore with recovery is not available for Lotus Notes/Domino Server 7.0 and later versions.

Limitations on disk array integrations

For additional integration-specific limitations not included in this section, see the *HPE Data Protector Zero Downtime Backup Administrator's Guide*.

HPE P4000 SAN Solutions limitations

- In a Microsoft server cluster environment, all volumes which are selected for zero downtime backup session must belong to the same cluster.
- Backup preview is not supported.
- Object copying and object mirroring are not supported for ZDB to disk.
- Although you can create replica sets, replica set rotation is not supported.
- A replica cannot be used for instant recovery under any of the following conditions:
  - A target volume of the replica has been automatically removed during an instant recovery session based on another ZDB backup specification.
  - Other entities exist on the disk array which depend on the source volume that was used to create a target volume of the replica:
    - A newer target volume exists, and a smartclone is attached to it.
    - A newer snapshot exists, and the snapshot was not created by Data Protector.
- The Data Protector `omnidbp4000` command that you should use for configuring access to the CIMOM provider of the HPE P4000 SAN Solutions is available only on Windows systems.

HPE P6000 EVA Disk Array Family limitations

- The single-host (BC1) configuration based on Linux platform is not supported. In such a configuration, a single Linux system acts as the application system and the backup system.

  For a list of supported configurations, see the latest support matrices at
  https://softwaresupport.hpe.com/.
- Dynamic disks are not supported.
- Only one type of target volume per source volume can exist on a disk array at the same time. For example, a snapclone of a source volume cannot be created if a vsnap or a standard snapshot of the

same source volume already exists.

- A replica cannot be reused if any snapclone from this replica has a snapshot attached or if a target volume from this replica is presented to a system other than backup system.

- Data Protector does not allow ZDB to use an instant recovery object as a source volume.

- When cloning of a source volume is in progress, another snapclone of that source volume cannot be created.

- Backup preview is not supported.

- Object copying and object mirroring are not supported for ZDB to disk.

- When using the "switch of disks" instant recovery method with HPE P6000 EVA Disk Array Family, care must be taken when instant recovery is performed on objects located on lower performance disks, as this may result in undesired performance penalties. In such cases, a ZDB to the high performance disks and subsequent instant recovery will reverse the situation.

- During instant recovery, CRC check is not performed.

- Instant recovery from a ZDB-to-disk+tape session cannot be performed using the Data Protector GUI after exporting or overwriting the media used in the backup session. The backup media must not be exported or overwritten even after an object copy session. If the backup media have been exported or overwritten, perform instant recovery using the Data Protector CLI. For information, see the *HPE Data Protector Zero Downtime Backup Administrator's Guide*.

- Routine maintenance tasks, including (but not limited to) hot-swapping HBAs/SCSI controllers, disk array controllers, FC switches, and online firmware upgrade during backup are not supported. Backup is a high-IO activity and should not be done at the same time as routine maintenance.

- The number of standard snapshots or vsnaps that can be created for a specific source volume is limited by the HPE P6000 EVA Disk Array Family storage system. The actual limitation is determined by the storage system's firmware revision. For details, see the HPE P6000 EVA Disk Array Family documentation. Consider the limitation when specifying a value for the option **Number of replicas rotated** of a zero downtime backup specification. Note that the limitation does not apply to snapclones.

- In zero downtime backup sessions using multisnapping, only two snapshot types are supported by default: standard snapshot and snapclone. For information on whether your HPE P6000 EVA Disk Array Family environment supports multisnapping using vsnaps, see your HPE Command View (CV) EVA documentation. For instructions on how to enable support for the vsnap snapshot type in multisnapping ZDB sessions in Data Protector, contact HPE technical support.

- The Data Protector`omnicreatedl` command cannot be used for creating Microsoft Exchange Server ZDB backup specifications for ZDB sessions involving P6000 EVA Array or P9000 XP Array.

HPE P9000 XP Disk Array Family limitations

- Asynchronous HPE Continuous Access P9000 XP configuration is not supported.

- The single-host (BC1) configuration based on Linux platform is not supported. In such a configuration, a single Linux system acts as the application system and the backup system.

  For a list of supported configurations, see the latest support matrices at
  https://softwaresupport.hpe.com/.

- With the single-host (BC1) configuration, only filesystem and disk image backup are supported.

- Split-mirror restore (restore of data from the backup medium to a secondary volume and restore of

data from the secondary volume to a primary volume afterwards) is supported for the filesystems and disk images in the HPE Business Copy P9000 XP configuration. Database (application) split-mirror restore is not supported.

- Instant recovery is only available in HPE Business Copy P9000 XP configurations.

- In case Microsoft Exchange Server is installed on the backup system, its Information Store (MDB) and Directory Store have to be installed on the HPE P9000 XP Disk Array Family LDEVs that are different than the mirrored LDEVs used for the integration. The drive letters assigned to these LDEVs have to be different from those assigned to the LDEVs that are used for the integration.

- Backup preview is not supported.

- Object copying and object mirroring are not supported for ZDB to disk.

- Instant recovery from a ZDB-to-disk+tape session cannot be performed using the Data Protector GUI after exporting or overwriting the media used in the backup session. The backup media must not be exported or overwritten even after an object copy session. If the backup media have been exported or overwritten, perform instant recovery using the Data Protector CLI. For information, see the *HPE Data Protector Zero Downtime Backup Administrator's Guide*.

- When restoring filesystems in an instant recovery session, no object other than those selected for instant recovery should share the disks that are used by objects selected for the session.

- Routine maintenance tasks, including (but not limited to) hot-swapping any field replaceable components like, disk array controllers, FC switches, and online firmware upgrade during backup are not supported. Backup is a high-IO activity and should not be done at the same time as routine maintenance.

- The maximum number of secondary volumes (mirrors, volumes to be used for snapshot storage) that can be created for a specific primary volume is limited by the HPE P9000 XP Disk Array Family model used and its installed firmware revision. Note that the limitation for mirrors and the limitation for volumes to be used for snapshot storage differ. For details, see the HPE P9000 XP Disk Array Family documentation.

HPE 3PAR StoreServ Storage limitations

- Snapshot of snapshot is not supported.

- On Windows, only MBR formatted volumes are supported.

- On Linux, only two-host configurations are supported. The application system and the backup system must not be the same client.

- During instant recovery, the target volumes from which the replica data copy is to happen, should not be presented to any client.

- Data Protector does not support the HPE 3PAR StoreServ Storage iSCSI host interface.

- In a Microsoft server cluster environment, all volumes which are selected for zero downtime backup session must belong to the same cluster.

- Backup preview is not supported.

- Object copying and object mirroring are not supported for ZDB to disk.

- A replica cannot be used for instant recovery if it was created with a Data Protector version earlier than 7.00 or with Data Protector 7.00 without the patch bundle set installed.

- Oracle ASM is supported with firmware 3.1.2 MU2 or later.

- During Instant Recovery, all volumes that are part of the volume set are accessible until the restore is completed.

EMC Symmetrix disk array limitations

- Only ZDB to tape is supported which means that instant recovery is not.
- Backup preview is not supported.
- Routine maintenance tasks, including (but not limited to) hot-swapping any field replaceable components like, disk array controllers, FC switches, and online firmware upgrade during backup are not supported. Backup is a high-IO activity and should not be done at the same time as routine maintenance.

NetApp Storage limitations

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- Instant recovery is not supported.
- Oracle ASM is not supported.
- Oracle RAC is not supported.

EMC VNX limitations

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- Instant recovery is not supported.
- SnapView Snapshot is not supported.
- Oracle ASM is not supported.
- Oracle RAC is not supported.

EMC VMAX limitations

- In cluster environments, the backup system must not be in the same cluster with the application system. Additionally, the backup system cannot be the cluster virtual server, it can only be a cluster node.
- Instant recovery is not supported.
- TimeFinder/Snap snapshot type is not supported.
- TimeFinder/Consistency Groups are not supported.
- Oracle ASM is not supported.
- Oracle RAC is not supported.

Disaster recovery limitations

- One Button Disaster Recovery (OBDR) method is not available for Data Protector Cell Managers.

- The Cell Manager recovery wizard is no longer available in the Data Protector GUI. As the Internal Database can only be backed up separately from the files systems, when preparing for disaster recovery of a Cell Manager, you need to ensure the backup images are created in the correct order: the Cell Manager filesystem backup image first, the Internal Database backup image second.

- When recreating volumes during Phase 1 of an automated disaster recovery process (Enhanced Automated Disaster Recovery, One Button Disaster Recovery), the original volume-compression flag is not restored (always saved to non-compressed).

  Workaround: Restore the volume compression flag manually after restore.

- Disaster recovery functionality is supported only if the platform on which the Data Protector GUI is used and the platform of the system which will be recovered are the same.

- One Button Disaster Recovery (OBDR) functionality is available only locally on the system to which the OBDR device is connected.

- The path of DR image file is limited to 250 characters, if it is saved on the Cell Manager during backup.

- The booting of Disaster Recovery image for Linux OS in physical machines with UEFI ROM can take a long time. Usually, it takes a minute for each physical core. But this does not affect the Disaster Recovery (DR) process, as once the image is booted, the DR continues to work properly.

User interface limitations

- The Data Protector GUI can display a limited number of backup specifications. The number of backup specifications depends on the size of their parameters (name, group, ownership information and information if the backup specification is dynamic or not). This size should not exceed 80 kB.

- The Data Protector command-line interface (CLI) does not support logging of user-triggered events to the Data Protector event log.

- On Linux systems, messages and notifications of the Data Protector CLI are only available in the English language.

Reporting limitations

- Information about physical devices, which is shown in the Device Flow report if the `RptDisplayPhysicalPath` global option is set to 1, is acquired from the current device configurations and may therefore be different from information at the time when the devices were actually used.

- In the Manager-of-Managers enterprise (multicell) Device Flow Web Report, devices are not sorted separately for each Cell Manager in the MoM.

- The following reports provide information only on destination media: Configured Devices not Used by Data Protector, Extended Report on Used Media, Report on Used Media, Session Media Report, and Session Devices Report.

- The virtual machine must not contain the following special characters: & ^ $! ~ , . ' ; () {} [], otherwise

the `omnidb -session <sessionID> -detail` does not display the correct Object Name, VM Path, and VM Name, and the `omnidb -veagent <ObjectName>` report displays a syntax error or "No objects were found" error message.

> **NOTE:**
> This is applicable for VADP reporting feature.

Other limitations

- For StoreOnce federated stores, all writing operations are performed in the low bandwidth mode (Application Source or Backup Server deduplication). Even if a gateway is configured as target-side deduplication (high bandwidth mode), it automatically switches to the low bandwidth mode.

- Only local shared storage (connected to cluster nodes via SCSI) is supported in cluster environments for ASR. Shared storage on disk arrays connected to cluster nodes via Fibre Channel (for example: P6000 EVA or P9000 XP disk arrays) is not supported unless appropriate device drivers are provided during the initial phase of ASR recovery (by pressing F6). This enables Windows Server 2008 Setup to correctly detect shared storage located on disk arrays.

   It is necessary to execute a test plan. The operation is at your own risk.

- Data Protector does not support hostnames with non-ASCII characters.

- Do not export media which contain integration object copies made from platforms that support Unicode (for example, Windows) to non-Unicode platforms (for example, HP-UX) or the other way round.

- The STK - Horizon Library manager is not supported.

- The filestream database trans backups are not supported.

- You cannot select different condition factors for pools sharing the same free pool. All media pools using a free pool inherit the condition from the free pool.

- Device files for the spt driver cannot be created automatically by Data Protector. The device file needs to be created manually using the `mknod` command.

- Media pools with magazine support cannot use free pools.

- Data and catalog protection can only be set until the year 2037.

   Workaround: Set protection period to 2037 or less and extend it with one of the future Data Protector releases that will support time settings past the year 2037.

- The network connections from the Cell Manager to Disk Agent clients must respond within 10 seconds or the session will be marked as failed.

- The name of a backup specification should not exceed 64 characters.

- The maximum length of text strings to identify or describe the properties of media and devices (for example, the media label applied to a medium when being initialized) is 80 characters.

- Session level restore is not available for the online database integrations.

- Automatic device selection during restore and/or object copy is limited to libraries. Only a device in a library can be automatically replaced with another device from the same library and of the same media type (for example, LTO).

- Automatic device selection during restore cannot be disabled for the Data Protector integrations that cannot be restored using the Data Protector GUI or CLI (for example, Sybase integration).

- The minus symbol (–) must not be used as the first character in any Data Protector labels or descriptions.

- The word `DEFAULT` is a reserved keyword and must not be used in device names, backup specification names, and pool names.

- All media with barcode labels starting with the CLN prefix are treated as cleaning tapes. Labels with this prefix should only be used on cleaning tapes.

- Software data compression for online database backups, such as Oracle, Sybase, SAP R/3, Informix Server, and Microsoft SQL Server, is not supported.

- The eject/enter functionality for ATL 2640 and ATL 6/176 devices is not supported using the fast access port.

- Media of different format types are not compatible:

  ○ Data Protector (written by devices under direct Data Protector MA control)

  ○ NDMP NetApp (written by devices connected to NetApp filers)

  ○ NDMP Celerra

  Media from these different format categories cannot reside in the same pool. Media from one format category cannot be recognized when subjected to one of the other environments using a different format category. In such a case, the media will be viewed as foreign and depending on the policy, unexpected overwrites might occur.

- From one backup object, only 1024 files and/or directories can be selected, otherwise select the entire object. For details about backup objects, see the *HPE Data Protector Help*.

- Some filesystems allow creation of deep directory structures (deeper than 100). Data Protector can only back up down to a depth of 100.

- When changing the `omnirc` file, it is required to restart the Data Protector services/daemons on the system. This is mandatory for the `crs` daemon on UNIX and recommended for `Data Protector Inet` and CRS services on Windows. On Windows systems, restarting is not required when adding or changing entries, it is required only when removing entries.

- If you use quotes ("") to specify a pathname, do not use the combination of a backslash and quotes (\"). If you need to use trailing backslash at the end of the pathname, use double backslash (\\).

- Tape quality statistics functionality is not supported if the Media Agent runs on a Linux or AIX system.

- Automatic drive cleaning for library definitions with a shared cleaning tape is not supported. Each library definition needs to have its own cleaning tape configured.

- The maximum pathname length supported by Data Protector is 1023 characters.

- Devices of file library type are not supported for filesystems that have compression turned on.

- The length of the pathnames of the directories that can be used for configuring devices of the file library type cannot exceed 46 characters.

- The length of the pathnames for jukebox slots and standalone file devices cannot exceed 77 characters.

- Data Protector does not support copying a media copy. However, such a copy can be made if the original medium is exported and thus the copy becomes the original. If you export the second level copy, you cannot import it again if the original medium is imported.

- The configuration of SNMP traps using the Data Protector Manager depends on the platform of the Cell Manager:

  ○ On HP-UX systems, the recipient system for the trap that is configured in the GUI receives the traps.

  ○ On Windows systems, the content of the recipient field in the GUI is ignored. The recipient must be configured on the Cell Manager in the Control Panel under **Network > Services > SNMP Services**.

- If Boot Configuration Data (BCD) is located on removable storage like floppy disk, USB flash drive, CD-ROM, or DVD-ROM, Data Protector cannot back up BCD registry entries.

- The Windows NTFS Change Log Provider cannot be used with Hierarchical Storage Management (HSM) solutions.

- The maximum size the Windows Change Journal is 4 GB. This space allows logging about 10,000,000 changes. After the maximum size is reached, a part of data is overwritten. In this time frame an incremental backup should be run.

- Automated System Recovery (ASR) cannot be used in IPv6-only environments. ASR can be used only in environments with a functioning DHCPv4 server.

- The Data Protector replication must always be configured in such way that we copy from one source Store on a physical Appliance to one target Store on an Appliance. The following are not supported:

  1. A replication from two or more source Stores on an Appliance to one target Store on an Appliance.

  2. A replication from two or more source Stores on an Appliance to two or more target Stores on an Appliance.

  3. A replication from one source Store on an Appliance to two or more target Stores on an Appliance.

- For Data Protector integration objects, the following actions cannot be restricted by using the `user_restrictions` file:

  ○ Start backup

  ○ Start backup specification

  ○ Start restore

- If the VADP reporting is enabled when a Virtual Machine (VM) is configured with IPv6 and DNS hostname (FQDN) is not known, reports display the VM name instead of the IP address.

- At the end of a Data Protector integration backup preview session, the backup statistics report that gets displayed contains irrelevant information. The following statistics are always zero: `Completed Media Agents`, `Failed Media Agents`, `Aborted Media Agents`, `Media Agents Total`, `Mbytes Total`, and `Used Media Total`.

- On UNIX systems, the original creation timestamp of a symbolic link is not preserved during a restore. The timestamp is set to the current system time. Due to a limitation of the system call `utime()`, the creation timestamp of a symbolic link cannot be changed after the link creation.

Recommendations

Using Data Protector with hierarchical storage management applications

If you are using an application such as file migration or hierarchical storage management that creates links, stubs, or shortcuts, it is recommended that Data Protector backup policies and file migrations do not execute against the same data set at the same time. This will avoid the situation where the backup may capture the stub and the migrated file in an inconsistent state.

Organizing Data Protector clients into cells

In small environments, the most simple approach is to manage all Data Protector clients within one Data Protector cell.

To efficiently hierarchically structure and manage large-scale environments, you can use the Data Protector Manager-of-Managers (MoM). An environment structured in such a way allows you to manage numerous clients from a central location; for MoM-related scalability limitations, see Backup infrastructure scalability, on page 14. Furthermore, multiple MoM cells can be centrally managed using the HPE System Management. Such a setup allows you to manage an unlimited number of Data Protector clients from one central location while distributing administrative and managerial rights to different Data Protector users and user groups.

Support for NIS+

NIS+ cannot be used as the primary name resolution for hosts when using Data Protector. However, you can run Data Protector on the hosts where NIS+ is configured if one of the following alternatives for name resolution with Data Protector is chosen:

- Using DNS. In this case, change the line starting with hosts in the /etc/nsswitch.conf file as follows:

  `hosts: dns [NOTFOUND=continue] nisplus`

- Using hosts file. In this case, change the line starting with hosts in the /etc/nsswitch.conf file as follows:

  `hosts: files [NOTFOUND=continue] nisplus`

In both cases, the Cell Manager must have fully qualified domain name registered in DNS or hosts file.

Large file support

- HPE recommends that the file system where DC directories reside supports files larger than 2 GB, especially if drives with large capacity, for example LTO 6, are used, and more than 10 million files are backed up on tape. In addition, on Windows systems HPE strongly recommends to use NTFS filesystem.

Encrypted control communication recommendations

- Use the generated keys and certificates instead of the default HPE Data Protector certificate `hpdpcert.pem`.
- Consider the manual distribution of keys and certificates to clients.

  For more information, see *Enabling encrypted control communication with manual distribution of certificates and keys* in *HPE Data Protector Installation Guide*.

Pre-exec and Post-exec scripts

The Pre- and post-exec commands for backup specifications must be located as follows:

- **Windows systems:** The scripts must be located in the `Data_Protector_home\bin` directory.
- **UNIX systems:** The exec commands for backup specifications must be located as follows:

  - **HP-UX, Solaris, and Linux systems:** `/opt/omni/lbin`

  - **Other UNIX systems:** `/usr/omni/bin`

  > **NOTE:**
  > For the commands located in the `/opt/omni/lbin` or in the `/usr/omni/bin` directory, specify only the filename, otherwise, specify the full pathname. For more information, see *Pre- and Post-Exec Commands for a Backup Specification* in *HPE Data Protector Online Help*.

With the enhancements in Data Protector 9.05 , if the Pre- and Post-exec scripts are not located in the specified directories, you will encounter an error message and the backup specification will fail.

Hence, it is highly recommended that you run `omnicellinfo -prepostinfocheck` to identify the locations that are not valid before performing backup. If the scripts are located in folders different than the ones specified, move the scripts to the specified locations and then continue.

Enhanced incremental backup

- To enable Data Protector Disk Agent to access more memory if needed for enhanced incremental backup on HP-UX systems, 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
  ```

Object consolidation

- When consolidating a large number of objects from synthetic backup with very long restore chains, an error might occur. To prevent this, run object consolidation regularly, for example, when you would normally run a full backup, to keep the restore chain manageable.

- Before starting an object consolidation session, ensure that the order of the objects is kept the same. Changing the order of the backed up objects may result in object consolidation failure.

Microsoft Exchange Single Mailbox integration

- Microsoft Exchange Server single mailbox backup is not as space- and CPU-efficient as backup of the whole Microsoft Exchange Server. HPE recommends to use the Microsoft Exchange Single Mailbox integration only for backup of a small number of mailboxes. If you are backing up large numbers of mailboxes, use the Microsoft Exchange Server integration instead.

Microsoft Volume Shadow Copy Service integration

Shadow copy storage area and disk space recommendations

- When backing up volumes using VSS (either using the Disk Agent or the VSS integration), ensure that there is enough free space available for the shadow copy storage area.

  By default, the initial size for the shadow copy storage area is set to 300 MB on Windows Server 2008 systems and 320 MB on Windows Server 2008 R2 systems. This means that for example on Windows Server 2008 R2 systems with the default settings there must be at least 320 MB of free space available on the volume that you are backing up.

  If you encounter timeout errors during the shadow copy creation, you may also want to increase the initial size for the shadow copy storage area. For details, see the Microsoft Knowledge Base article at http://support.microsoft.com/kb/826936.

Regular maintenance of the VSS part of the registry

- Microsoft Windows operating systems maintain a record of mount operations in the registry. This process results in registry growth over time and eventually leads to volume shadow copy import problems. For details, see the *HPE Data Protector Zero Downtime Backup Integration Guide*, chapter *Integrating the Data Protector ZDB integrations and Microsoft Volume Shadow Copy Service*, section *Troubleshooting*.

  To prevent the registry from growing excessively, HPE recommends that you periodically perform registry management tasks with Microsoft Registry Management Tool.

Network Data Management Protocol Server integration

- The maximum number of files and directories per NDMP backup specification should not exceed 20 million. The recommended number of files and directories per NDMP backup specification is 10 million.

Windows Server 2008 clients

- **Server roles and services on Windows Server 2008**

  Similarly to previous Windows Server operating system releases, Microsoft extended the concept of server roles and services in Windows Server 2008. To enable backup of data belonging to the server roles and services introduced with Windows Server 2008, Data Protector provides extended filesystem backup functionality for this platform. Among others, the following roles can be backed up using filesystem backup:

  - Active Directory Certificate Services (AD CS)

  - Active Directory Domain Services (AD DS)

  - Application Server (requires IIS 6 compatibility)

  - Dynamic Host Configuration Protocol (DHCP) Server

  - DNS Server

  - Network Policy and Access Services

  - Terminal Services

  - Web Services (IIS) (requires IIS 6 compatibility)

  When configuring a backup specification for data belonging to a particular server role or service, you should select either the entire volume on which the data resides or the entire client system that hosts the server role or service. Moreover, you should select the **Use Shadow Copy** option on the **WinFS options** property page of the **Filesystem Options** window. When selected, this option provides a consolidated, consistent state of the backed up data.

  > **CAUTION:**
  > Additionally, if configuring a backup specification for disaster recovery purposes, clear the option **Allow Fallback**. Failing to do so may result in backup data unusable for disaster recovery.

- **System State backup and the CONFIGURATION object**

  To perform a System State backup on Windows Server 2008, you should follow the above instructions for filesystem backup of the relevant volumes or the entire client system, instead of backing up the `CONFIGURATION` object.

- **Active Directory Domain Services restore**

  On Windows Server 2008, only offline restore of Active Directory Domain Services is supported, which must be performed in Directory Services Restore Mode. Since the Active Directory Domain Services restore is a complete overwrite of the existing database, it does not preserve any new users which are created after the backup operation.

Windows Server 2012 clients

- When performing a filesystem backup or restore of a deduplicated volume, data is backed up and restored rehydrated (nonoptimized backup or restore). Therefore, consider the following:

  - Make sure that the target media and the restore target have enough storage space available:

    - Plan the storage space needs based on the original (logical) size of data, *not* the space occupied by deduplicated data on the volume. For example, if 100 GB of data occupies 40 GB of space on the volume, plan for 100 GB.

      If you do not have enough free capacity, and you do not need to restore individual files, you can perform a disk image backup instead (optimized backup).

    - Data is always restored to the original (non-deduplicated) size, in the above example, it occupies 100 GB space after restore.

      Schedule a periodic deduplication process at the restore target system to deduplicate the restored data again.

  - In case of a backup to a Backup to Disk device, HPE recommends to use the Data Protector deduplication functionality (either StoreOnce software deduplication or the method provided by the device) to reduce the amount of space consumed by the backed up data. To reduce the network load, use source-side deduplication.

  - If you back up data with a high deduplication ratio, an optimized disk image backup is faster because less data needs to be transferred over the network.

UNIX system clients

- When performing a disk image backup, HPE recommends to dismount disk partitions before the backup and mount them back later.

Chapter 4: Recognized issues and workarounds

This section lists known Data Protector and non-Data Protector issues and workarounds.

Known Data Protector issues and workarounds

Installation and upgrade related issues

During upgrade, the VEAgent backup fails with error message

Problem

After upgrading to Data Protector9.00 or later, if the backup specification is created using Data Protector 7.0 , 7.01, or earlier versions, the VEAgent backup fails with the following error:
 	
 `[Critical] From: VEPALIB_VMWARE@hostname; "<Datacenter>" Time: <Date Time>;`
 	
 `No Objects found for backup`

Workaround
After upgrading, re-create the backup specification with the same VM selection and options as earlier, and run the backup again.

Installation Server patches list does not display the patches for the newly installed Installation Server

Problem
If you install the Installation Server directly from another installation server (where GR, and MMR patches have been applied), these patches will not be shown in the list of Installation Server patches for the newly installed Installation Server. However, patches are only not shown but the new Installation Server depot contains the same patches as the one from where it was installed.
Workaround
Hence if you need to see the installed patches, then copy the patch_* files from the original Installation Server system `<DP_DATA_DIR>\Config\Server\install\patch_*` to the newly installed Installation Server system: `<DP_DATA_DIR>\Config\Server\install`

Restore of encrypted backups fails after the migration

Problem
Encryption keys are not migrated correctly when migrating the Cell Manager from 32-bit to 64-bit Windows systems. As a result, restore of encrypted backups fails after the migration.

Workaround

To ensure that encryption keys are correctly migrated, perform the following:

1. Export all keys from the Key Management Server (KMS) on the 32-bit system using the `omnikeytool` command.

2. After you perform the migration, *delete* all data (`DAT`) files from all key store folders from the directory `Data_Protector_program_data\server\db80\keystore` on the 64-bit system, except from the `catalog` folder. Do not delete the index files.

3. Import all previously exported keys to the KMS on the 64-bit system. After the import, encrypted backup can again be restored.

During upgrade, the Cell Manager fails to update configuration information

Problem

HP-UX and Linux systems: For Data Protector cluster-aware clients, the Data ProtectorCell Manager will only update configuration information for their cluster virtual system during the upgrade process, but not for the corresponding cluster nodes (physical systems).

Workaround

The issue has no effect on the actual state of such clients, only their configuration data is not upgraded. After the upgrade, to update the configuration data and complete the upgrade process, execute the command `omnicc -update_host` *ClientName* for each cluster-aware client, where *ClientName* is the name of a particular cluster node.

Data Protector GUI allows to remotely install the components to a virtual host

Problem

HP-UX and Linux systems: The Data Protector GUI enables you to remotely install the components to a virtual host, even though the components must not be added to the virtual host.

Workaround

None. Do not remotely install the components to the virtual host, but install the clients locally as described in the *HPE Data Protector Installation Guide*.

Import of the cluster virtual host with Data Protector installed is unsuccessfull

Problem

Import of the cluster virtual host with Data Protector installed will not finish successfully (cluster will be imported but offline virtual servers will not be imported) during the installation of cluster-aware Cell Manager if there is another cluster virtual server configured on Microsoft Cluster Server in any cluster group and is offline. If this virtual server is online during the Data Protector installation, the import of the Data Protector cluster virtual server will be successful.

Workaround

Put all virtual servers in your cluster online and import the Data Protector cluster virtual server

manually after the installation.

Binaries of the Data Protector components are not supported

Problem
If you upgrade a Data Protector client on an HP-UX 11.23 or HP-UX 11.31 system, the binaries of the Data Protector components that are not supported on HP-UX 11.23 or HP-UX 11.31 (for example, EMC Symmetrix Agent, DB2 Integration) are not removed. If you later uninstall Data Protector, the binaries are left on the system.
Workaround
Uninstall the earlier version of Data Protector. Install Data Protector9.00, and then install the Data Protector9.05 patch.

Desktop shortcuts fails to function after an upgrade

Problem
On Windows systems, desktop shortcuts for starting Data Protector that were created by the user, for example by dragging the menu item to the desktop, do not function after an upgrade.
Workaround
Recreate the desktop shortcuts after upgrading.

Installation check fails on the non-active node

Problem
In a cluster-aware Cell Manager configurations running on an HPE Serviceguard cluster or Veritas Cluster Server, the installation check fails on the non-active node although Data Protector is correctly installed, because only the active node can access the Cell Manager configuration.
Workaround
If the cluster fails over, the check on the now active node succeeds.

Installation fails when the Restart failed clients option is used

Problem
If a remote UNIX or Linux client installation fails, and you restart the installation using the **Restart failed clients** option, the installation is either skipped or fails again, although the issue that caused failure of the first installation session is resolved.
Workaround
Locally uninstall the client and repeat the remote installation. For uninstallation details, see the *HPE Data Protector Installation Guide*.

Windows Installer service fails to start

Problem
On Windows systems, the Data Protector installation might fail with the following error: `Error 1601. The Windows Installer Service could not be accessed. This can occur if the Windows Installer is not correctly installed. Contact your support personnel for assistance.` The root cause of the problem is the Windows Installer service that could not be started at the beginning of the installation. If the service cannot be started, the installation fails.
Workaround
In the **Control Panel > Administrative Tools > Services**, change the startup type for the Windows Installer service from Manual to Automatic, start the service, and restart the Data Protector installation.

After upgrading, passwords of all virtual environment hosts will no longer work

Problem
After upgrading the Data Protector Virtual Environment integration component without the installed patch bundle set 6.21 to the latest release version, passwords of all virtual environment hosts will no longer work. To solve this, execute the following command: `vepa_util.exe --upgrade -cell_info`
Workaround
This is needed due to a change in password encoding in the `cell_info` file. It will re-encode the passwords of all virtual environment hosts, first creating a `cell_info.bak` file.

During installation, a message is displayed

Problem

On HP-UX systems, the following message may be reported during installation of the Data ProtectorCell Manager, but the installation succeeds nevertheless:
 	
`* "Hostname:/cdrom/hpux/DP_DEPOT": Cannot open the logfile on`
 	
`this target or source. Possibly the media is read-only or`
 	
`there is a permission problem. Check the daemon logfile and`
 	
`"/var/tmp/swagent.log" on this host for more information`

Workaround
None. You can safely ignore the message.

Communication between Data Protector components in the cell may not work properly

Problem
During the installation, Data Protector setup will update only `Private` and `Domain` Windows Firewall profiles. The `Public` profile is not updated. As a result, communication between Data Protector components in the cell may not work properly, resulting in various issues.

Workaround
If you are using the `Public` profile, update the firewall rules manually. For more information about Data Protector and firewalls, see the *Data Protector Help index: "firewall support"*.

After installing General Release Patches, the error message appears

Problem
On HP-UX systems, the HPE Software Assistant (SWA) may report errors after installing General Release Patches: `ERROR: Patch PHSS_xxxxx is not recognized.` This occurs in cases where General Release Patches have been correctly installed on top of a Data Protector patch bundle, and the patches contained inside the bundle are not present in the catalog referenced by SWA.

Workaround
None. You can safely ignore the messages.

Problem

On HP-UX systems, after you install a patch on the Cell Manager system, the GUI connection to the proxy service fails with an exception:
 	
`16:38:04,534 SEVERE [org.jboss.resteasy.core.SynchronousDispatcher] (http--0.0.0.0-7116-4)`
 	
`Failed executing GET /backupspec: org.jboss.resteasy.spi.WriterException:`
 	
`java.lang.IllegalStateException: Invalid JSON namespace:`
 	
`http://www.hp.com/2011/software/im/dp/data_model at`
 	
`org.jboss.resteasy.core.ServerResponse.writeTo(ServerResponse.java:262)`
 	
`[resteasy-jaxrs-2.3.2.Final.jar:]`

Workaround
After installing a patch, restart the Cell Manager

During installation, an error message is reported

Problem
On Windows systems, the following message may be reported during installation of Data Protector, but the installation succeeds nevertheless:

```
{A37E26EF-E4F1-432B-ABA4-02268BC99B80}: related product unexpectedly found on the
system. or/and "{30692C3E-7A60-4BD4-B021-213055B1810F}: related product
unexpectedly found on the system."
```

The root cause of the problem are previously uninstalled Data Protector components `VMware Granular Extension Web Plug-In` and `VMware Granular Recovery Extension Agent`, which the uninstallation process did not remove.

Workaround

You can safely ignore the message. To properly uninstall the Data Protector Granular Recovery Extension for VMware vSphere, manually remove entire Data Protector (all installation components) from your system. For details on removing Data Protector, see the *HPE Data Protector Help* index: "uninstalling, Data Protector software".

During upgrade, the installation displays a warning message

Problem

While upgrading to the latest Data Protector General Release patch bundle, the installation displays the following warning:

```
Timeout reached before Data Protector Application Server stopped.
```

Workaround

You can safely ignore the message

Clean up the older FUSE mount points and 3PAR replica presentations to the mount proxy

Problem

Prior to an upgrade to Data Protector 9.04 and above, if you have used FUSE in Data Protector 9.02 and 9.03, and 3PAR VMware GRE, the older FUSE mount points and 3PAR replica presentations to the mount proxy must be cleaned up.

Workaround

To clean up the older FUSE mount points and 3PAR replica presentations to the mount proxy, proceed as follows:

- Delete the request files from the Cell Server. The request files are available in the following location:

  Windows Cell Manager:

  `C:\ProgramData\OmniBack\Config\Server\Integ\Config\Vmware\<vCenterHost>\`

  Linux Cell Manager:

  `/etc/opt/omni/server/integ/config/Vmware/<vCenterHost>/`

- Unmount the vmfs fuse mount point (Specific to Linux only) #unmount <MountPoint>

  #unmount <MountPoint>

  The <MountPoint> format is as follows:

```
/var/opt/omni/tmp/VMWareGRE/<vCenterName>/<reqID>
```

- Unpresent replica from the 3PAR Array console, if requests are created using the ZDB backups.
- Remove the nfs share from the Media Agent, if requests are created using the Smart Cache backups.

User interface related issues

During the user account settings, the configuration fails with an error message

Problem
When you are setting up a user account for the Data Protector Inet Service user impersonation using the Data Protector GUI, the configuration may fail with an error message similar to the following: `Failed to modify config information for user myuser@hostname.`
Workaround

1. Connect to the client where the issue appears.
 	
 2. Delete the user impersonation configuration for the specified client using the `omniinetpasswd` command:
 	
    `omniinetpasswd -delete myuser@hostname`
 	
 3. Reconfigure the user impersonation for the specified client using the `omniinetpasswd` command:
 	
    `omniinetpasswd -add myuser@hostname`
 	
 For details of the `omniinetpasswd` command, see the *HPE Data Protector Command Line Interface Reference*

Characters from other code pages will appear corrupted

Problem
When using the Data Protector CLI on a Windows system to manage backups of data residing on clients running on other platforms, the filenames will only be displayed correctly for code page 1252. Characters from other code pages will appear corrupted. Even though a filename appears corrupted in the CLI, it will be backed up or restored properly. Data Protector CLI expects such "corrupted" filenames as input parameters. You can use copy and paste functionality to input filenames as they appear in code page 1252.   For internationalization limitations tables, see the *HPE Data Protector Help* index: "internationalization".
Workaround
None

Paused backup session reports an error message

Problem

The session messages for a paused backup session display an error from the Disk Agent when the backup session is scheduled from the Scheduler and has the ability to pause lower priority sessions.

```
[Normal] From: BSM@hostname "Bkp_Low" Time: <Date> <Time>
Session pause request received by user ADMINISTRATOR.123@hostname. Pausing the
session.
[Normal] From: VBDA@hostname "C:" Time: <Date> <Time>
Received ABORT request from SM => aborting.
```

Workaround

None. This is the expected behavior when a backup session is being paused on a busy backup device. The warning can be safely ignored.

Schedule migration fails

Problem

Schedule migration fails after you upgrade to Data Protector 10.00.

Workaround

If schedule migration fails during the upgrade process, you can manually run the following command to successfully migrate the existing schedules to the new Scheduler:

```
omnidbutil -migrate_schedules
```

Paused backup session contain failure messages

Problem

The session messages for a paused backup session may contain some failure messages for a session that succeeds.

In certain scenarios where multiple backup sessions are scheduled for the same device, a lower priority session is waiting for a device to start before it receives a session pause request due to a higher priority session. The session logs contain all of the success messages, warning and pause messages.

```
[Warning] From: BSM@hostname "Bkp_Low_FL1"  Time: <Date> <Time>
[61:2013] Some of the backup devices are occupied. Session is waiting for all the
devices to get free.
[Normal]  From: BSM@hostname "Bkp_Low_FL1"  Time: <Date> <Time>
Session pause request received by user@hostname. Pausing the session.
```

Workaround

None. This is the expected behavior when a backup session is being paused on a busy backup device. The warning can be safely ignored.

Disk Agent related issues

During a parallel restore, the Disk Agents fails with the error message

Problem
When attempting a parallel restore which uses more Disk Agents than the current Media Agent concurrency setting, some Disk Agents may fail with the following error: `Cannot handshake with Media Agent (Details unknown.) => aborting.`
Workaround
Restart the restore objects of the failed Disk Agents.

During restore, the actual restore target mount point is not displayed

Problem
During restore, the volume restore Disk Agent (VRDA) displays the mount points of the application system in the monitor. For example, instead of the restore target mount point `/var/opt/omni/tmp/`*hostname*`/BC/fs/LVM/VXFS` it actually displays the corresponding application source mount point `/BC/fs/LVM/VXFS`.
Workaround
None

Restore fails with the message in the session log

Problem

When restoring files to a different system via a UNC share, the restore fails with the following message in the session log:
 	
 `Can not open: ([112] There is not enough space on the disk. ) => not restored.`
 	
 `[Warning] From: VRDA@hostname "host2.test.com [/H]" Time: <Date> <Time> Nothing restored`

Workaround
The Data Protector `Inet` logon user account must have the access to log on to the remote system, which is specified in the UNC path. You should also be the owner or have permission to write to the files you want to restore via UNC share.

During the directory structure backup, the same message is displayed twice

Problem
When trying to back up directory structure with more than 100 directories (on HP-UX systems, this number is equal to the maximum number of allowed open file descriptors), the following message is

displayed twice instead of once:

```
[Major] From: VBDA@hostname "C:" Time: <Date> <Time>
```

```
[81:74] File system too deep: (100) levels.
```

Workaround

None.

Backing up a mount point

Problem
When backing up a mount point that resides on a Windows system, if a subdirectory is deselected and therefore excluded from backup, the whole mount point might be backed up nevertheless.
Workaround
None.

Expanding the empty mount point fails with an error message

Problem
When trying to expand the empty Windows mount point in tree view, the following error is reported: `Cannot read directory contents.`
Workaround
None.

Only account user can remove the encrypted attribute

Problem
On Windows, the encrypt attribute of encrypted folders will be restored. However, only a user who logs on using the account under which the Inet service runs on the client or an Administrator will be able to remove the attribute.
Workaround
None.

During Macintosh files backup, certain characters in file names may cause problem

Problem
On Windows systems, when backing up Macintosh files, certain characters in file names may cause problems. If file names contain characters considered invalid on a Windows filesystem (typically '*' and '?'), or contain characters mapped to such invalid characters (for example, the Macintosh bullet character), it is possible that individual files are not backed up or that the Disk Agent terminates abnormally.

Workaround
Rename the problematic files.

Backed up data cannot be restored to its original location

Problem
Data backed up from a shared network folder using Data Protector Disk Agent installed on a Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012 system cannot be restored to its original location, even though the user account which was used during the backup session is granted write permissions for the folder.
The problem occurs because Data Protector does not have impersonation capability for filesystem restore sessions.

Workaround
Using the `runas.exe` command, start the Data Protector GUI as the user whose account was used during the backup session, and only then start the restore session.

During a disk image backup, a warning message is displayed

Problem
On HP-UX systems, when performing a disk image backup, a warning message is displayed although the backup session succeeds:
`Object is a mounted filesystem.`

Workaround
None. Check if the disk or volume is mounted. If it is not mounted, you can ignore the warning message.

During replication sessions, the sessions fails with an error message

Problem
If you schedule several replication sessions to run in parallel and the replication source are also replication sessions, the sessions may fail with an error similar to the following:
`[Major] From: CSM@hostname "QCTP2A53730" Time: <Date> <Time>`
`[65:99] Import failed with possible cause:`
` this media already has valid copy in DB.`
The issue is caused by objects with identical labels that appear in multiple backup specifications, for example, if you create multiple backup specifications for different directories of the same filesystem on the same client.

Workaround
Using the Data Protector GUI, provide different descriptions for the conflicting objects in the backup

specifications that were the initial source for the replication specifications or make sure that replication sessions containing these objects are not started in parallel.

Data Protector GUI unable to distinguish between active source devices

Problem
It is possible to start a replication when the source and target of the replication is the same B2D device because the Data Protector GUI is not able to distinguish between active source devices. If the user attempts to create an object copy specification using the **Capable of Replication** option, it is possible to select the same source and target B2D devices in the Data Protector GUI.
Workaround
Ensure that the replication source and targets are different B2D devices.

During the backup on resume, unable to analyze what files have already been backed up

Problem
When resuming a backup on a filesystem where too many changes took place from the time the session was aborted, Data Protector might not be able to use the Windows native change journal to analyze what files have already been backed up. In this case, a filesystem scan will disregard all resume related information upon resume. The backup session will be displayed as resumed, however, all the files will be backed up again, which might result in a larger size of the resumed backup than expected.
Workaround
None.

Backup fails with an error message

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. ).` • `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.
Workaround
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

Enhanced incremental backup option will result in 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.
Workaround
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.

Disk Agent unable to backup files from sub volume

Problem
Disk Agent does not backup all the sub volumes directly, if accessed using its parent sub volume. Therefore, the sub volumes must be mounted and backed up separately. BTRFS (a new file system for Linux) as a feature enables creating sub volumes from one folder tree. So, you can have many sub volumes on one file system. Once such a sub volume is created, the Disk Agent will not able to backup files from that sub volume.
Workaround
You can mount that volume as a new mount point and configure that in the backup specification to backup the mount point.

Media Agent related issues

During a backup session, the Utility Media Agent (UMA) may stop responding

Problem
If during a backup session a shared StorageTek ACS tape library is used as a backup device, and intercommunication between a Disk Agent and a Media Agent is interrupted, the Utility Media Agent (UMA) may stop responding. Consequently, subsequent sessions that use the involved tape drive may fail.
Workaround
Use the `omnirc` option `OB2ACSUMATIMEOUT` to specify how long Data Protector should wait for the connection between the Disk Agent and the Media Agent to be restored before it terminates the UMA.

Intercommunication problems

Problem
If during a backup, copy, or restore session, SCSI read or SCSI write errors are intermittently reported, there may be intercommunication problems between a Media Agent and a SCSI device connected to SAN.

Workaround
The problem may be solved by configuring the following `omnirc` options on the affected Media Agent system: `OB2MAREADRETRY`, `OB2MAXREADRETRIES`, `OB2MAREADRETRYDELAY`, `OB2MAWRITERETRY`, `OB2MAXWRITERETRIES`, and `OB2MAWRITERETRYDELAY`.

Failover during the backup

Problem
In a cell where the Cell Manager is not installed on the cluster, the devices are connected to cluster nodes, and a failover during backup activity occurs, the Media Agent may not be able to properly abort the session, which results in the medium no longer being appendable.

Workaround
None.

Mount request for the cleaning tape fails to function properly

Problem
Cleaning tape drive functionality functions correctly only when there is a cleaning tape present either in the library slot or in the repository slot. If the cleaning tape is not present, the mount request for the cleaning tape will not function properly.

Workaround
None.

During import, the Data Protector reports a major error and ends abnormally.

Problem
When importing a range of tapes, Data Protector normally skips all invalid tapes (such as tar tapes, blank tapes, and so on) and continues with the next slot. When importing a range of tapes on NetApp Filer (Celerra) and when a NetApp tape is detected, Data Protector reports a major error and ends abnormally.

Workaround
None.

ACSLS library mount request occurs during the backup or restore session

Problem

If ACSLS library mount request occurs during backup or restore session (in case that library ran out of usable media), do not format or scan additional tapes with the tape device currently being used by the session. Use a different tape device in the library to perform this operation and confirm the mount request.

Workaround

None.

Unable to restore any backup data from the corrupted medium

Problem

During a backup session, if you restart the system that hosts a Data Protector Media Agent, the medium to which data is backed up with this Media Agent becomes corrupted, although Data Protector does not report any errors. Consequently, you may not be able to restore any backup data from this medium. Subsequent backup sessions to the corrupted medium will fail, too.

Workaround

None.

Media pre-allocation list is ignored

Problem

Backup sessions for backing up to a file library device ignore the media pre-allocation list.

Workaround

None

Restore fails with the error message

Problem

If the media of a file library device are unprotected, they are deleted at the beginning of the next backup session that is using this device. However, the session which was using the first medium of the file library device is still stored in the database. If you attempt to restore data by specifying this session, the restore fails and the following message is issued:

```
Object not found.
```

Workaround

None

During the backup session, the unprotected media will be marked as empty

Problem

If a disk becomes full during a backup session using a jukebox (with media of type file) as destination device, all slots configured on this disk which contain unprotected media will be marked as empty.

Workaround

1. Rescan the slots which are marked as empty.

   After the rescan, the media will be visible again in the slot.

2. Free up space on the disk to avoid this problem from recurring.

After performing both steps, you can continue to work with the jukebox device.

Object copy session become unresponsive

Problem

An object copy session containing numerous objects (more than 200) or complex object media relations (see below) may become unresponsive.

Workaround

- Change the device mapping so that only one device is used to read the copy source media per media type (DLT or LTO) and restart the session.

- Split the original object copy session into multiple sessions and restrict each session to copy objects from one backup session only.

- Split the original object copy session into multiple sessions and restrict the session to copy as few media as possible in a single session.

Unresponsiveness is commonly caused by copying objects from source media which were created by different backup sessions using different (logical) devices.

NDMP object copy session become unresponsive

Problem

An NDMP object copy session with more than one source device used for the object copy may become unresponsive.

Workaround

Limit the number of objects to be copied. Additionally, limit the number of source devices to 1.

Failure to read the tape medium header

Problem

When an external encryption controller is controlling encryption on a tape device, a failure to read the tape medium header of a previously encrypted medium can occur. This happens if the connection to the external encryption controller is not available or a decryption key is deleted from the external encryption controller.

Workaround

Set the `OB2_ENCRYPT_FORCE_FORMAT` environment variable to force a format operation on the tape.

The following options are available:

- If the variable value is set to 0 then a format operation will be aborted.
- If the variable value is set to 1 then Data Protector Media Agent will force a format operation.

  The default value is 0 (not set).

Incorrect handling of the ownership of backup objects

Problem
When importing legacy NDMP media populated in a Data Protector version earlier than 7.x and 8.x, there is a problem with imported UNIX file system backup objects: ownership flags (owner, group) of such objects are set to 0 0. The root cause of the problem is incorrect handling of the ownership of such objects in earlier Data Protector versions, where the ownership fields stored alongside the object data were misused for purposes other than object ownership.
Workaround
None.

Device for restore is unavailable

Problem
When a device required for restore is unavailable or disabled, the restore session fails.
Workaround
Restore your data with an alternative device. For instructions, see the *HPE Data Protector Help* index: "selecting, devices for restore".

Capacity and usage are incorrectly recorded

Problem
When more than 4 TB of backup data is stored to a single medium, its capacity and usage are incorrectly recorded in the IDB. Consequently, invalid figures are presented.
Workaround
None. Nevertheless, all the Data Protector operations such as backup and restore, function properly.

Incorrect calculation of the space used by file libraries

Problem
In previous releases, Data Protector incorrectly calculated the space used by file libraries. As a result, the TB based licensing database tracked file library usage as being many times lower than actual.
Workaround
None. In this release, customers may see a sudden increase in reported file library usage when file library usage is checked with omnicc.

Unable to distinguish between media agent versions of Data Protector10.02 and subsequent General Release patches

Problem
The gateway filter cannot distinguish between media agent versions of Data Protector10.02 and subsequent General Release patches. When attempting to create a Cloud device with a gateway on a media agent, the GUI reports an error of `unsupported`. Install the latest 9.05 patch.
Workaround
Update all clients with media agents to the latest General Release patch bundle.

Number of initiators on the Media Agent

Problem
General Data Protector backups use upto 64 connections but backups over Fiber Channel (FC) use only 16 connections, which is four times less.
Workaround
Increase the number of initiators on the Media Agent to 64.

NDMP path-based file history does not work

Problem
Cannot browse the files for restore in Restore context, if NDMP path-based file history (HIST=F) is set during backup.
Workaround
Switch the file history to `dir/node`. Set default on filer or through NDMP environment variable in backup specification.

Integration related issues

Microsoft Exchange Server

Tape device for a Microsoft Exchange Server restore cannot be changed

Problem
In the Data Protector GUI, the tape device you want to use for a Microsoft Exchange Server restore cannot be changed from the device originally used by backup.
Workaround
To change the device for restore, in the Data Protector GUI, click the **Change** button. You cannot change the device by just deselecting the default device and selecting the desired device.

Microsoft Exchange Single Mailbox

During the Microsoft Exchange Single Mailbox integration configuration, some issues may occur

Problem
When configuring the Microsoft Exchange Single Mailbox integration, the following issues may occur: • The CLI configuration session finishes without errors, but the configuration actually fails. When creating a backup specification, the configuration dialog displays. If the backup is started from the CLI or from the GUI where the configuration was not performed in GUI, the session finishes immediately without backing up any data.   • If the integration was configured using the GUI, and you run the configuration check from the CLI, the check will fail with `*RETVAL *8561`.
Workaround
• Use the GUI to configure the integration and to check the configuration.   • Set or export the environment variable `OB2BARHOSTNAME` on the client system with the command `set OB2BARHOSTNAME=`*client_name* (on Windows systems) or `export OB2BARHOSTNAME=`*client_name* (on UNIX systems) and repeat the configuration from the CLI.

Microsoft SQL Server

Tape device for a Microsoft Exchange Server restore cannot be changed

Problem
In the Data Protector GUI, the tape device you want to use for a Microsoft SQL Server restore cannot be changed from the device originally used by backup.
Workaround
To change the device for restore, in the Data Protector GUI, click the **Change** button. You cannot change the device by just unselecting the default device and selecting the desired device.

Data Protector does not enforce the requirement that different source media are copied to different target media

Problem
When performing an object copy session where B2D devices are the source devices, Data Protector may not enforce the requirement that different source media are copied to different target media.
Workaround
To make sure that several data streams are not multiplexed to the same medium, configure a separate object copy specification for each database and set the following:

- the number of devices must be the same as the number of streams of an object in the selected session
- the minimum value for Load balancing must equal the number of the devices
- target device concurrency to 1.

To calculate the number of devices you need, multiply the maximum number of streams for any database in a session with the number of parallel object copy sessions from these specifications. For example, if there are a maximum of five data streams in a session and two parallel object copy sessions based on this session, you need 10 devices.

Microsoft Volume Shadow Copy Service

Backup fails if a transportable backup is performed in parallel

Problem
When backing up many writer components at once, the backup fails if a transportable backup is performed in parallel.
The issue appears if you select many writer components (for example SQL databases for SqlServerWriter or Hyper-V virtual machines for the Hyper-V writer) directly instead of their container (for example, the whole writer) and, at the same time, a transportable backup is performed.

Workaround
- Perform a local backup instead of a transportable backup. You can still use the VSS hardware provider if necessary. The writer components (databases, virtual machines, and so on) can be selected directly one by one.
- Select the whole container (for example an SQL instance for the SqlServerWriter or the entire Hyper-V writer) instead of individual components (for example SQL databases or virtual machines). In this case, you can use VSS transportable backup.

Incorrect processing of the restore chains

Problem
Data Protector might incorrectly process restore chains of two backup objects (volumes, folders, or files) during the restore sessions. For example, if both full and incremental backup images exist for objects A and B, and you select a full backup image of A and an incremental backup image of B for restore, Data Protector overrides your selection for A by also including its incremental backup image in the restore chain.

Workaround
To make Data Protector correctly process different restore chains for multiple objects backed up in the same sessions, restore the objects separately in several restore sessions.

SAP R/3

Backup of SAP R/3 data fails

Problem
Backup of SAP R/3 data fails when the `-u` option is specified in the command line for the `brbackup` or `brarchive` command.

Workaround
If you specified `-u` in the command line of `brbackup` or `brarchive`, it should be followed by *username*/*password*.

Oracle Server

Waiting time occurs for a backups session

Problem
On Windows system, Oracle backup sessions wait for 20 seconds before they end. This waiting time occurs because Oracle does not notify that the API session is complete. If you run a backup from RMAN and use the Data Protector library (`orasbt.dll`) to perform that task, you must wait at least 20 seconds between two backup sessions using the same backup specification. In the opposite case, all the backup objects will be backed up within the same backup session.

Workaround
None

Database recovery after instant recovery fails with the error message

Problem
The `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` omnirc options are set and database recovery after instant recovery fails with the following error: `ORA-00338: log `*Name*` of thread `*Num*` is more recent than control file` The above message indicates that the control file was overwritten during instant recovery. This happens if the Oracle control file location was specified for the *control_file_location* parameter which should define the location of the control file copy.

Workaround
Perform recovery using a backup of the control file. Ensure that *control_file_location* does not point to the location where the Oracle control file is located.

Recovery fails during the backup data restore

Problem
If you restore backup data created using the proxy-copy method and perform a database recovery, RMAN may try to use the channel allocated for restoring proxy-copy backups to recover the database. As a result, the recovery fails.

Workaround

Start a database recovery-only session from the Restore context or using RMAN scripts.

Data Protector managed control file backup ends unexpectedly with the error message

Problem

In an Oracle Real Application Clusters (RAC) environment with Oracle version 11.2.0.2 or later, a Data Protector managed control file backup ends unexpectedly with the following message:

```
The database reported error while performing requested operation.
```

```
ALTER DATABASE BACKUP CONTROLFILE TO '/var/opt/omni/tmp/ctrl_dbpp.dbf' REUSE
sqlcode 245 error occurred at line 1.
```

```
ORA-00245: control file backup operation failed
```

By default, Data Protector backs up the Data Protector managed control file from the default Data Protector temporary files directory .

Workaround

The directory to back up the control file from must be located on a shared disk and be accessible from all RAC nodes. Define an appropriate directory by setting the OB2_DPMCTL_SHRLOC environment variable for the control file copy, and restart the session.

Configuration of the ZDB Backup specification fails

Problem

If you are configuring a backup set ZDB backup specification that involves a disk array of the HPE 3PAR StoreServ Storage family, Data Protector may incorrectly detect that the chosen database files are managed by an Oracle ASM instance, in case it is running on the same Oracle Server system. Since the atomic snapshot feature is a prerequisite for backing up Oracle ASM-managed data with Data Protector, but the HPE 3PAR StoreServ Storage disk arrays do not support it, sessions based on such a backup specification fail.

Workaround

Before you start configuring a Data Protector ZDB backup specification for Oracle Server backup, shut down the running Oracle ASM instance and start it up again after you have saved the backup specification. Data Protector will successfully back up correct data that you have selected for backup.

Configuration of the VMware (Legacy) integration fails with the error message

Problem

In a VirtualCenter environment with VirtualCenter Server 4.0, configuration of the VMware (Legacy) integration using any of the four methods (Suspend, Snapshot, VCBFile, VCBImage) may fail with the following error:

```
The database reported error while performing requested operation.
```

Workaround

On the VirtualCenter client, perform the following steps to add Data Protector to the VirtualCenter client list.

1. On the VirtualCenter client, go to the folder `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter`.

2. Edit the file `vpxd.cfg` and add the variables `maxBufferedResponseBytes` and `agentsNeedingContentLength`:

```
<config>...
  <vmacore>
    <threadPool>
        <TaskMax>30</TaskMax>
    </threadPool>
<http>
      <maxBufferedResponseBytes>104857600</maxBufferedResponseBytes>
       <agentsNeedingContentLength>VMware-client|DataProtector/6.1
       </agentsNeedingContentLength>
    </http>
  </vmacore>...
</config>
```

3. Save the changes.

4. Right-click **My Computer** and choose **Manage**.

5. Double-click **Services and Applications** in the **Name** column on the right.

6. Double-click **Services** in the **Name** column on the right.

7. Right-click **VMware VirtualCenter Server** in the **Name** column on the right, and choose **Restart**.

8. After restarting verify that the change has taken effect by verifying the VirtualCenter log as follows:

   a. Go to the folder `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\Logs`

   b. Find the log file `vpxd-NN.log` (where *NN* is the latest number).

   c. Open the log file and look for the following two lines:

      `Loaded agentsNeedingContentLength: 'VMware-client|DataProtector/6.1'`

      `"Max buffered response size is 104857600bytes"`

VMware vSphere

During restore, the virtual machine fails to start

Problem

When restoring a virtual machine with a virtual Raw Device Mapping (vRDM) disk to a directory using the option **Restore to Directory**, the restore succeeds and you can import or upload the files

to a vCenter. However, starting such a virtual machine fails.
Workaround
None. Do not use the Restore to Directory option when restoring a virtual machine with a vRDM disk.

Storage policy for VVol datastores is not considered

Problem
Storage policy for VVol datastores not considered during the restore.
Workaround
You can edit the storage policy of the virtual machine after a restore. For more details, see the following URL: http://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.storage.doc/GUID-D6A099C5-8F80-474C-A79A-64F5EC4455DA.html

Backing up VMs from a vCenter fails with an error message

Problem

On Windows systems, when backing up VMs from a vCenter installed on a French-language version of the operating system, the backup fails with the following error:
 	
`[Major] From: VEPALIB_VMWARE@hostname "/Datacenter"`
 	
` Time: <Date> <Time>`
 	
` Virtual Machine 'vm_2': Could not backup disk scsi0:0 ...`
 	
`[Major] From: VEPALIB_VMWARE@hostname "/Datacenter"`
 	
` Time: <Date> <Time>`
 	
` Virtual Machine 'vm_2': No disk backed up ...`
 	
If you back up the same VM from a vCenter installed on an English-language version of the operating system, the backup finishes successfully. After that, a backup from a French-language operating system host is also successful. The issue is caused by UTF-16 characters in the VDDK temporary directory path, which is by default set to %TEMP%\vmware-%USERNAME%.

Workaround
Set a different temporary directory in the file *Data_Protector_Program_ data*\Config\client\vepa_vddk.config, for example: tmpDirectory=c:\tmp.

Creating a virtual machine snapshot fails with the error message

Problem
Creating a virtual machine snapshot, either when the virtual machine is being migrated using VMotion migration or when such migration is not taking place, may fail with one of the following

errors:

[Major] From: BSM@hostname "Barlist-BackupRestore-1054"

 Time: <Date> <Time>

[61:3003] Lost connection to OB2BAR Backup DA named "ERROR" on host hostname

 Ipc subsystem reports: "IPC Read Error System error: [10054] Connection reset by peer"

[Normal] From: VEPALIB_VMWARE@hostname ""

 Time: <Date> <Time>

Creating Virtual Machine 'jeos-e10x-001' ...

 Datacenter: /ESX5.0_Name

 Host/Cluster: cluster.company.com

 Datastore: VMData_env39 name

2013-04-12T17:30:35.651+02:00 [04048 trivia 'ThreadPool'] PrepareToWait: Starting new thread

2013-04g45280-12T17:30:35.806+02:00 [02928 trivia 'ThreadPool'] PrepareToWait: Starting new thread

2013-04-12T17:30:35.899+02:00 [02928 trivia 'ThreadPool'] PrepareToWait: Starting new thread

2013-04-12T17:30:35.902+02:00 [03184 trivia 'ThreadPool'] PrepareToWait: Starting new thread

2013-04-12T17:30:35.902+02:00 [02852 trivia 'ThreadPool'] PrepareToWait: Starting new thread

2013-04-12T17:30:35.902+02:00 [03184 trivia 'ThreadPool'] PrepareToWait: Starting new thread

[Major] From: RSM@hostname ""

 Time: <Date> <Time>

[61:3003] Lost connection to OB2BAR restore DA named "" on host hostname.

 Ipc subsystem reports: "IPC Read Error System error: [10054] Connection reset by peer"

Workaround

Restart the backup session.

Lotus Notes

Backup fails with the error message

Problem
In case the Data Protector application specific pre-exec script is specified for the Lotus integration backup on Solaris, the backup may fail with the following error: `Data Protector Lotus Agent cannot back up object objectname.`
Workaround
Disable the Data Protector application specific pre-exec script and restart the backup.

During a point-in-time restore an error message is displayed

Problem
During a point-in-time restore of the Lotus Notes database, the following error may occur: `Lotus Notes C API 'NSFRecoverDatabases' returned error 5099: Recovery Manager: Backup was later than recovery point in time.` The problem occurs if the specified point in time is earlier than the time when the source backup was performed.
Workaround
Specify a different point in time or a different source backup, so that the point in time is later than the time when the source backup was performed.

Disk array integrations

Change in the configuration requirements for ZDB

Problem
The configuration requirements for ZDB of Oracle or SAP R/3 databases have changed in the following cases: • if Oracle is used as a part of Oracle ZDB integration and you intend to perform instant recovery sessions, • if Oracle is used as a part of SAP R/3 ZDB integration and you intend to perform instant recovery sessions. In these cases, the Oracle database needs to be reconfigured. For more information on configuration requirements, see description of the `ZDB_ORA_INCLUDE_CF_OLF` omnirc option in the *HPE Data Protector Zero Downtime Backup Administrator's Guide*.
Workaround
None

Database recovery cannot be performed from the CLI

Problem

Database recovery after instant recovery for the Microsoft Exchange Server and Microsoft SQL Server integrations cannot be performed from the Command Line Interface (CLI).
Workaround
Perform the recovery using the GUI.

Data Protector session fails with an error message

Problem

The Data Protector session in the NetApp storage environment fails with an error similar to the following:
 	
`[Major] From: SMISA@hostname "SMISA" Time: <Date> <Time>`
`The presentations have not been created for this storage volume:`
`Storage volume:`

Workaround
Workaround: Delete the LUNs left after the backup session and restart the Data Protector ZDB session for the NetApp storage. The name of such LUN has the following syntax: *LUN_name.ID* (ID is generated by the NetApp storage), for example, `LUN_2_4.DP-2014.11.14-10-05465F54A`.

Granular Recovery Extension issues

VMware vSphere

Performance slows down during the restore process

Problem
When performing a partial restore using the VMware Granular Recovery Extension for cached recovery, Data Protector reads all disks from tape device instead of only the selected ones, which can significantly slow down the restore process.
Workaround
Backup to either the Smart Cache device or 3PAR replica to take advantage of cached recovery.

Swap partitions reports an error message

Problem

The granular recovery or browsing of swap partitions in Linux systems may result in the following error message:
 	
`Exception: The virtual disk does not have any partitions that the host system`
`knows how to mount.`

Workaround

Navigate to other partitions or volumes.

Microsoft SharePoint Server

Granular Recovery link does not work if MDS is enabled

Problem
Microsoft SharePoint Server 2013: When you select Site Settings > HPE Data Protector Granular Recovery Extension > Granular Recovery, the Granular Recovery link does not work if Minimal Download Strategy (MDS) is enabled. If MDS is disabled, the link properly opens the Granular Recovery Extension page.
Workaround
- Open the link in a new tab or window.   - Alternatively, disable Minimal Download Strategy.

Disaster recovery issues

Encrypted backup of the Internal Database fails

Problem
An encrypted backup of the Internal Database (a prerequisite for Cell Manager disaster recovery) fails unless an active encryption key was created prior to the backup.
Workaround
Create an active encryption key prior to invoking an encrypted backup of the Internal Database. For details, see the `omnikeytool` man page or the *HPE Data Protector Command Line Interface Reference*.

Incorrect message is displayed when command starts with invalid parameters

Problem
If the `omnidr` command is started with invalid parameters, a message to press the F8 key in the next 10 seconds is displayed instead of the command synopsis. After pressing any key, the command properly displays the command synopsis.
Workaround
None

During disaster recovery process, the data and mounting is skipped

Problem
When hidden dynamic volume is mounted to an empty NTFS folder and backed up, the disaster

recovery process creates the volume but skips mounting it to the folder and restoring the actual data.
Workaround
Once the disaster recovery completes, you can restore the data using the following procedure: • Mount the volume to the same NTFS folder. • From the Restore context of the Data Protector GUI, execute data restore.

Cluster related issues

Common issues

Instant recovery fails

Problem
When backup system is in a cluster environment and the backup session is performed using the name of the cluster node, instant recovery fails if you try to perform recovery using the other cluster node.
Workaround
To avoid this problem, use the name of the virtual host for configuration of the backup specification.

Backup session not responding

Problem
If a backup session stops responding during a cluster failover, and all Backup Agents fail, a timeout will be reported but the session itself will not abort. The default session timeout occurs after 7200 seconds (two hours). As long as the session is not responding, another session using the same backup specification cannot be started.
Workaround
Manually abort the backup session and restart the session.

Cluster failover occurs during a Data Protector backup session

Problem
If a cluster failover occurs during a Data Protector backup session in which an application database that resides on the cluster is being backed up with the appropriate application integration agent, particular problem may occur after the failover which prevents the session from succeeding. Under such circumstances, in Monitoring context of the Data Protector GUI, two backup sessions are displayed: the backup session that was restarted after the failover, and another, unknown session. Output of the unknown session contains messages similar to the following: [Critical] From: BSM@*ClusterNode01Name* "*BackupSpecificationName*" Time: <Date>

```
<Time>

[12:1243] Device not found.

[Critical] From: OB2BAR_VSSBAR@ClusterNode02Name "MSVSSW" Time: <Date> <Time>

 Failed VSSBAR agent.

[Major] From: OB2BAR_VSSBAR@ClusterNode02Name "MSVSSW" Time: <Date> <Time>

 Aborting connection to BSM. Abort code -1.

[Critical] From: BSM@ClusterNode01Name "BackupSpecificationName" Time: <Date>
<Time>

 None of the Disk Agents completed successfully.

 Session has failed.
```

The root cause of the problem is unsuccessful identification of the restarted backup session after the failover. The involved integration agent is not notified about the backup session restart. Depending on the particular situation, the integration agent either starts a new backup session or connects to the restarted backup session manager (BSM) process. In both cases, such behavior of the integration agent is wrong.

Workaround

None.

Issues in HPE Serviceguard

Instant recovery fails with the error message

Problem

After failover on the secondary application system (application runs on the HPE Serviceguard cluster) instant recovery may fail with the following error message, if the **Check data configuration consistency** option is selected:

```
[Critical] From: SSEA@hostname"" Time: <Date> <Time>

Data consistency check failed!

Configuration of volume group /dev/vg_sap has changed since the last backup
session!
```

Workaround

- Make sure that the vg configuration on the system is not changed, deselect the **Check data configuration consistency** option, and restart the instant recovery.
- When setting up the cluster, use the ioinit command to ensure that all disk device files are identical.

Unable to import the physical node

Problem
If you export a physical node from an HPE Serviceguard cluster, you cannot import it back as the `cell_server` file is deleted. This file is shared among all nodes of a cluster, so you need to recreate it.
Workaround
Execute the command `/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade`.

Issues in Microsoft Cluster Server

Restore API fails

Problem
When restoring the Cluster Database of Microsoft Cluster Server, you should stop the cluster service on all inactive nodes before starting the restore. If cluster service is active on any other node at the time of the restore, the restore API will fail and eventually cause a failover.
Workaround
None

Restore session stops to respond

Problem
When the Cell Manager is installed on Microsoft Cluster Server and you start a restore of the Cluster Database, the restore session will stop responding. This is because the cluster service is stopped by the restore API causing the Restore Session Manager to lose the connections to the IDB and the MMD.
Workaround
Wait for the VRDA to complete and then abort the session. You then need to restart the GUI (or reconnect to the Cell Manager). Additionally, when starting a Cluster Database restore, make sure that this is the only item you are restoring and that no other sessions are running.

Reporting related issues

Email does not have a subject when report is sent using e-mail send method

Problem
On Linux systems, when sending a report using the e-mail send method, the e-mail does not have a subject and contains `root` in the **From** field. The correct **From** and **Subject** entries are inside the e-mail body.
Workaround

Use sendmail to send reports using the e-mail send method. For example, to use `sendmail` instead of `/usr/bin/mail`, create the following link:

```
ln -s /usr/sbin/sendmail /usr/bin/mail
```

Note that on some Linux distributions `/usr/bin/mail` already exists. HPE dissuades you from removing this existing path since some applications may rely on it.

Other known issues

Data Protector is unable to detect duplicate IP addresses

Problem
Data Protector is unable to detect duplicate IP addresses within a cell or MoM environment and cannot report them as such. If a duplicate IP address is assigned to a system with the Data Protector software installed, Data Protector reports such network misconfiguration with the message `Cell Manager host IP is not in IP range` in the GUI and CLI as follows: - In the About Data Protector Manager or About Data Protector MOM dialog box in the GUI, in the Remark column of the Passwords info property page   - In the `Remark` lines of the Data Protector`omnicc -password_info` command output   Under these circumstances, Data Protector licensing is no longer covered. Until you resolve the problem, you can expect session and operation failures in the affected Data Protector cells.
Workaround
Reconfigure your network by assigning a unique IP address to the problematic system.

Clocks between the Cell Manager and the client are not synchronized

Problem
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.
Workaround
None. Make sure the clocks between the Cell Manager and the client are synchronized.

Restore Session Manager creates link to the shared configuration folder between the cluster nodes

Problem

The IDB restore session report displays the following message:
`The OS reported error while accessing <new restore directory>:`
`[2] No such file or directory`

Workaround
No action is required. In cluster Cell Manager Unix environment, `<DP_CONFIG_DIR>/server` is a link to the shared configuration folder between the cluster nodes. During restore, the Restore Session Manager tries to create `<DP_CONFIG_DIR>/server` as a link to the shared configuration folder between two nodes, which is not required.

Session treated as a copy cannot be selected for restore

Problem
If you consolidate object versions that have already been consolidated, selecting the session in the **Restore** context results in a message that the session contains no valid restore objects. This is because the session is treated as a copy and consequently cannot be selected for restore.

Workaround
Either select the session in which the objects were originally consolidated, or select the objects under **Restore Objects**.

Session aborts, if more object versions match the selection criteria

Problem
To prevent object consolidation sessions from using too much system resources, the number of object versions that can be consolidated in one session is limited to 500 by default. If more object versions match the selection criteria, the session is aborted.

Workaround
Either tighten the selection criteria, for example, by limiting the time frame, the number of backup specifications, and so on, or increase the value of the global option `ConsolidationAutomatedMaxObjects`.

Object consolidation session become unresponsive

Problem
If you perform interactive object consolidation of objects that span more than one medium and the number of consolidation devices used is smaller than the number of objects being consolidated, the object consolidation session may become unresponsive.

Workaround
Either increase the number of consolidation devices, or select the object versions for consolidation in the order in which their full backups were performed.

File writers (file library drives) needed for consolidation session gets aborted

Problem
If full backups for multiple objects reside multiplexed on a device which is different than the file

library hosting the corresponding incremental backups for these objects (for example, on a tape library), it may happen that some of the file writers (file library drives) needed as targets for the consolidation session get aborted because of a failure on the source Media Agent side (for example, in case of a media error, an incorrect block size, a canceled mount request, and similar). This may result in a hanging object consolidation session, in case there are not enough file writers remaining to complete the consolidation for other objects. Once all remaining objects are consolidated, all file writers will be freed up again at the end of the session.

Workaround

Ensure that the number of file library drives used as consolidation devices is equal or higher than the number of objects being consolidated. If the number of configured file library drives is smaller than the number of objects to be consolidated, HPE suggests to split the consolidation of multiple objects into more than one session.

Session fails during replication of several backup sessions

Problem

When replicating several backup sessions which backed up the same objects at the same time, for example, folders that reside on the same mountpoint on the same host, the session might fail with the following error:

```
[Major] From: CSM@hostname "new_0" <Date> <Time>

[65:99] Import failed with possible cause:

this media already has valid copy in DB.
```

Workaround

Group such objects into one session or explicitly use different labels for each object.

During restore, the Vapp is not deleted

Problem

When trying to restore to another organization, the original Vapp does not get deleted.

Workaround

You must manually delete the Vapp before performing a restore.

(Or)

As soon as the restore completes in the Data Protector GUI, the Administrator must manually delete the original Vapp and start the restored Vapp. If required, you must configure the network as well.

Restore session fails with an error message

Problem

When restoring to a new location from a medium that contains a consolidated object on HPUX 11.31 Itanium, the restore session fails with errors. For example:

> [Minor] From: VRDA@hostname CONSO2 Time: <Date> <Time> /tmp

Workaround

If the buffer size is less than 8, set it to 8 (the default value) and restart the restore session. For instructions, see the *Data Protector Help*, index: "setting, advanced options for devices and media".

Backup session fails with the error message

Problem

When performing a backup from HP-UX or AIX or Solaris system (Disk Agent) with deduplication functionality, the backup session fails with the following error, if the two omnirc variables (OB2ALIGN and/or OB2SAPALIGN) are set:

[Major] From: BMA@computer.com "D2D_NS_Baze_gw5 [GW 4560:4:1766155810]" Time: 7/15/2015 2:39:25 PM

[90:51] \\COFC-D2DNS\D2D_NS_Baze\df2ebb9f_55a6547a_2014_0233

Cannot write to device (JSONizer error: Invalid inputs)

Workaround

Ensure that the two omnirc variables (OB2ALIGN and/or OB2SAPALIGN) are not set. For more information, see the omnirc reference page in the HPE Data Protector Command Line Interface Reference Guide or the omnirc man page.

Collision between different logical devices for the same physical device

Problem

If you have different logical devices for the same physical device and you use a different logical device for backup every day, the lock name concept prevents collisions between different logical devices assigned to the same physical device.

When trying to perform a restore, where several logical devices but only one physical device was used for different backups (Full, Incr1, Incr2, Incr3, ...), Data Protector does not check the lock name, and therefore does not recognize that the same physical device was used for all backups. An error message that the restore session is waiting for the next device to get free is displayed.

Workaround

Remap all logical devices to the same physical device by following the steps below:

1. In the Context List, click **Restore**.
2. In the Scoping Pane, expand the appropriate data type and desired client system and object for restore.
3. When the Restore Properties window opens, select the files that you would like to restore.
4. In the Devices tab, select the original device and click **Change**.
5. When the Select New Device window opens, select the physical device name and click **OK**.

Instant recovery fails

Problem
Data Protector instant recovery fails when the filesystem is busy.
Workaround
List processes which occupy filesystem by using the `fuser` command. For example, if the filesystem `/oracle/P01` is busy, execute the command `fuser -kc /oracle/P01`.

Difference in LUN configuration on clients

Problem
If a backup is performed on one node and then instant recovery attempted on another node with the **Check data configuration consistency** option selected, the following error message is displayed:
`Volume group configuration has changed.`
The message is displayed because the `vgdisplay` command detects that the LUN configuration on one client is different than that of the other client.
Workaround
If the `ext_bus` instance is the same, this message is not displayed. Alternatively, it is not displayed if the **Check data configuration consistency** option is not enabled.

Services fail to run after EADR or OBDR.

Problem
Data Protector services may not be running after EADR or OBDR.
Workaround
In the **Control Panel > Administrative Tools > Services**, change the startup type for Data Protector services from Manual to Automatic. Start the services after you have changed the startup type.

Backup fails due to invalid object

Problem
A backup may fail if the snapshot backup specification contains an invalid `rdsk` object in the first place.
Workaround
Change the order of the `rdsk` objects so that a valid `rdsk` is in the first place.

Unusual delay in unloading a tape drive

Problem
On HP OpenVMS systems, a restore session may become unresponsive and report errors due to an

unusual delay while unloading a tape drive.
Workaround
Set the Cell Manager global parameter `SmPeerID` to 10 and restart all Data Protector services on your Cell Manager.

Data Protector uses the default community name `public`.

Problem
When using SNMP traps on a Windows Cell Manager, Data Protector uses the default community name `public`. This applies to both the SNMP send method with Data Protector notifications or reporting and the SNMP traps for system and application management applications.
Workaround
In the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\SNMPTrap` create a value named `Community` and set it to the community name you want to use. Note that all SNMP traps will be sent with the same community name and to the destinations associated with it in the Control Panel.

Disabling of Name Server Caching affects the RHEL

Problem
Data Protector performance on Red Hat Enterprise Linux (RHEL) is negatively affected if the Name Server Caching (`nscd`) daemon is disabled.
Workaround
Enable Name Server Caching on RHEL, or switch to a local DNS, and then execute the `omnisv -start` command.

B2D copy session may allocate more source gateways

Problem
The B2D copy session may allocate more source gateways than needed.
Workaround
You can control the gateway expansion with global variable **LimitInitGatewayExpansion** as described in global file.

Command `omnistat -session [session ID] -detail` incorrectly display a message

Problem
The command `omnistat -session [session ID] -detail` may incorrectly display a message `Restore started` or `Backup started`. This may result in both parameters appearing to be identical.

Workaround
None.

Using the Data Protector GUI or CLI, the debug logs are not collected

Problem
When you collect the debug files matching a specific debug ID, using the Data Protector GUI or CLI, the relevant debug logs may not be collected.

Workaround

When you are collecting and saving the debug files, make sure you also specify all known source debug directory paths.
 	
• If you use the Data Protector CLI, execute:
 	
  `omnidlc -did debugID -debug_loc Dir1`
 	
• If you use the Data Protector GUI:
 	
  1. In the Context List, click **Clients**.
  2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**.
  3. Right-click the client and click **Collect debug files**.
  4. In the Debug File Collector – Directories page, enter the paths for all known non-default debug directories and click **Add**.
  5. Click **Next** as many times as needed to reach the last page of the wizard.
  6. Click **Finish** to exit the wizard.

Restore from a client system fails

Problem
When performing a point-in-time restore from a client system which is in a different time zone than the Cell Manager, the restore fails. If started from the Cell Manager, the restore succeeds. The issue arises because the Cell Manager does not store the time zone of the client system during the backup.

Workaround
If you are performing a restore from a client system, account for the time zone difference when selecting the point in time to which to restore. For example, if the Cell Manager is in the time zone UTC+1 and the client is in UTC+5, and you performed the backup at 5:00 as seen on the client system, enter the time as it was on the Cell Manager at the time of the backup, that is 1:00.

Object version is not encrypted

Problem
The object version properties in the GUI and CLI only display information about the Data Protector software encryption. In case that only drive-based encryption was used, the object version is

displayed as not encrypted.

Workaround
Drive-based encryption is not related to object version. To check for the object's drive-based encryption, use the `omnimm -media_info` *Medium* `-encryptioninfo` command.

Running a restore to another location reports an error message

Problem
When you run a restore to another location (using the `Restore into` option) of the multiple filesystem objects that are located in different subdirectories of the same top level directory, the following error may occur:
`[Minor] From: VRDA@hostname "OBJECTNo1" Time: <Date> <Time> /tmp/RestoreDir Cannot create: ([17] File exists).`
The restore finishes successfully.

Workaround
None. You can safely ignore the message.

Backup session hangs

Problem
Backup session hangs if the original and mirror device have their Max concurrency set to 32.

Workaround
Lower the concurrency on both the original and mirror device to 30.

CA certificate unavailable in the filesystem

Problem
When starting the Data Protector GUI, it will attempt to connect to the Cell server. The Cell server is identified by either its `short hostname` or `hostname.domain`. Just before authenticating, the certificate of the Certificate Authority (CA) is transferred from the Cell server and stored in the filesystem using the FQDN of the Cell in the path. When connecting to the Cell server for the second time, the already stored CA certificate is compared with the newly received one from the Cell server. When identifying the Cell server by the hostname only, the CA certificate is not found in the filesystem and an `accept certificate` dialog pops-up.

Workaround
The folder that stores the `cacert.pem` file on the client is located at the following location: `\users\<user>\AppData\Local\Hewlett-Packard\Data Protector\ca\<FQDN>\cacert.pem`. If you copy this folder to the following location then the issue does not occur again: `\users\<user>\AppData\Local\Hewlett-Packard\Data Protector\ca\<hostname-without-domain-name>\cacert.pem`.

Restore session is incomplete

Problem
A resumed session contains more than one object version per backed up object. But the `omnir` command expects each session to have one object version per object and does not restore the session completely with default parameters.

Workaround
Restore the resumed session by following the steps below: 1. Obtain the copy IDs of the session using the `omnidb –session <sessionId>` command. 2. Run `omnir` multiple times and add the `–copyid "UUID/seqnr"` one after the other in the `omnir` command line. **NOTE:** The restore sequence has to be performed in a chronological order for a successful and complete restore.

During restore, a resumed session appears repeatedly for the same object

Problem
In the restore context of Data Protector GUI, when you restore by session, a resumed session appears in the left pane repeatedly for the same object, given the number of object versions per object in the resumed session.

Workaround
For restore, select only the object coinciding with the last successful object version and one of the identical objects at the time.

Faulty Time-To-Live value of the SSL certificate is generated

Problem
When connecting the Data ProtectorCell Manager on HP-UX or Linux using the Windows Data Protector Client GUI, the following error is displayed: `A server error has occurred. Reported error message: Unknown SSL protocol error in connection to <cell manager>: 7116.` The error occurs when a faulty Time-To-Live value of the SSL certificate is generated on the Cell Manager.

Workaround

Manually generate a new SSL certificate with the `omnigencert.pl` script from the command line. To do so, perform the following:
 	
1. Get the store password by performing the following:
 	
    • Navigate to the `webservice.properties` file from the following location:
 	
      `/etc/opt/omni/client/components`

- Search for the `keystorePassword` value, for instance, consider that the `keystorePassword` = `<store_password>`.

2. Generate a new SSL certificate by executing the following command:

   `/opt/omni/bin/perl /opt/omni/sbin/omnigencert.pl -server_id <CellManagerHostname.domain.com> -user_id hpdp -store_password <store_ password>`

3. Restart the Data Protector services using the following commands:

   `omnisv stop`

   `omnisv start`

   (Or)

   Reload the jboss configuration using the following command:

   `/opt/omni/AppServer/bin/jboss-cli.sh -c --command="/:reload`

Deactivating the password key affects backup

Problem
Password encryption is done by AES keys with the entity name "Data Protector Passwords". Do not delete or deactivate this key, as Data Protector will not be able to decrypt encrypted strings. Deactivating the password key affects backup only; it does not affect restore, nor does it disable the key or act as a key revocation. For Cloud devices, deactivating or deleting the key renders the Cloud device unusable. For details, see the `omnikeytool` man page or the *HPE Data Protector Command Line Interface Reference*.
Workaround
Do not delete or deactivate this password key.

Error in communication with the Cloud object store

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`
Workaround
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.

Cloud Azure device configuration fails

Problem
The Cloud Azure device encounters problems during configuration when attempting to configure with Data Protector 9.08 or earlier.

Workaround
Cloud (Azure) devices are not supported by earlier versions of Data Protector. Ensure that all Cell Managers, GUI servers, Installation Servers, and Media Agents are updated to the General Release Patch or later.

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

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.

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

PDB dropped from CBD

Problem
In case where PDB has been dropped from CDB following error displays: ORA-65011: Pluggable database does not exist.

Workaround
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`

Known non-Data Protector issues and workarounds

Non-Data Protector issues related to installation or upgrade

Installation fails on the NFTS filesystem

Problem
On Windows systems, the operating system might incorrectly report free disk space for an NTFS

volume that is mounted to a directory on an NTFS filesystem: instead of the NTFS volume free space the amount of free space on the NTFS filesystem is reported. In such cases, the Data Protector Setup Wizard will not start the installation to the mounted NTFS volume if the amount of free space on the NTFS filesystem is smaller than the minimum disk space installation requirement.

Workaround

Free disk space on the NTFS filesystem by removing unnecessary files until the installation requirement is met.

Verification fails on the windows systems during the absence of G5 root certificate

Problem

On Windows systems which do not have the G5 root certificate issued by the VeriSign Class 3 Public Primary Certification Authority installed, verification of the binaries signed with the new Authenticode signing certificate may fail.

For more information on the root cause of this problem, see the related Verisign Knowledge Center article published on the web at
https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1747&actp=search&viewlocale=en_US.

Workaround

None.

Installation from a mapped drive fails with the error message

Problem

On Windows systems, if you start local installation from a mapped drive through Remote Desktop Client, the installation may fail with the following error message:

Error 2755. Server returned unexpected error 3 attempting to install package *MappedDrive*:\i386\DataProtector.msi.

The Windows Installer service is running under a different user account than the user account under which the mappings were created, and therefore has different drive mappings. As a result, the installation fails.

Workaround

- Do not start the installation from a mapped drive. Use the UNC path specification instead (for example \\hostname*shared_folder*).
- For installation, use VNC instead of Remote Desktop Client.
- Start the installation on the console.

The `rpm` utility does not remove theData Protector

Problem

On Linux systems, the `rpm` utility does not correctly remove Data Protector components if you specify several installation packages in the same command line. For example, if you use `rpm -qa | grep OB2 | xargs rpm -e`, the `rpm` utility does not resolve dependencies in the correct order.

Workaround

Remove the Data Protector components one by one.

Non-Data Protector issues related to user interface

Using CLI on UNIX system displays incorrect characters

Problem

When using CLI on UNIX systems, the characters may be displayed incorrectly.

Different encoding systems (Latin, EUC, SJIS, Unicode) cannot be used in the desktop environment and in the terminal emulator. For example, you start the desktop environment in EUC-JP, open a terminal emulator and change the locale to SJIS. Due to an operating system limitation, if you use any CLI command, the characters can be displayed incorrectly.

Workaround

To eliminate this problem, start the desktop in your desired locale.

Non-Data Protector issues related to Disk Agent

Backed up files are restored to a wrong location with incorrect file name

Problem

On Windows systems, due to filesystem limitations, files that were backed up on UNIX systems and whose names contain the backslash ("\") character may be restored to a wrong location and with the wrong file name. Windows operating system interprets the backslash in a file name as a directory separator. For example, if a file named `back\slash` file was backed up on a UNIX system and restored to a Windows system, it will be restored into the `back` directory with the file name `slash`.

Workaround

None

Backup session fails with the error message when the option Use shadow copy is selected

Problem

On Windows systems, when backing up several objects at once and with the option **Use shadow copy** selected, backup of some objects may fail with the following error message:

`[Major] From: VBDA@ `*hostname*`"`*ObjectName*`" Time: `*SystemTime*

> It was not possible to create volume snapshot for '*Mountpoint*'. System error:
> 'VSS Snapshot creation failed'.

The issue can appear if there is not enough disk space available for storing multiple shadow copies or due to high disk I/O load. For details, see
http://www.microsoft.com/technet/support/ee/transform.aspx?ProdName=Windows%20Operating%20System&ProdVer=5.2.3790.1830&EvtID=12298&EvtSrc=VSS&LCID=1033.

Workaround

- Run the backup session again.
- Provision enough dedicated storage space on a separate volume, reserved only for shadow copy storage.

  You can allocate additional shadow storage space using the command `vssadmin add shadowstorage`.

  For details, see http://technet.microsoft.com/en-us/library/cc788051(v=ws.10).aspx.

Recommendation:

Allocate separate storage space to store shadow copies. This storage space should not be on the volumes that are backed up.

During NFS backup on HP_UX 11.31 system, the NFS mount point is inactive

Problem
On HP-UX 11.31 systems, the NFS mount points become inactive when performing an NFS backup.

Workaround
Upgrade the Open Networking Computing component (ONCplus) to B.11.31.10 or a newer version.

Non-Data Protector issues related to Media Agent

Erase operation fails on the magneto-optical drive

Problem
Erase operation on magneto-optical drive connected to an HP-UX system fails with the following error:

`[Major] From: MMA@hostname "MO-lada" Time: <Date> <Time> [90:90] /dev/rdsk/c2t0d1 Cannot erase disk surface ([22] Invalid argument) => aborting`

Workaround
None.

omnirc command options are configured to correctly function in stack mode

Problem
Breece Hill's Saguaro libraries use the stack mode for entering and ejecting cartridges. One mail slot has two SCSI addresses, one for the enter operation and the other for the eject operation. For Data Protector to function properly in this mode, the following `omnirc` command options must be configured as follows: `OB2LIB_STACKEXP` must contain the SCSI address of the export slot   `OB2LIB_STACKIMP` must contain the SCSI address of the import slot
Workaround
None.

Data loss occurs when the Media Agent coexist with CA ArcServe

Problem
Data Protector Media Agent cannot coexist with CA ArcServe installed on the same Windows client system. Such setup may lead to a data loss.
Workaround
None

Importing the media fails with the error message

Problem

When a DLT8000 library is used, media cannot be imported and the `omnimlist` command does not function properly. In this case, the following errors are reported:
 	
`[Major] From: MMA@hostname "Datacenter" Time: <Date> <Time>`
 	
`[90:182] Cannot forward segment. ([5] I/O error)`
 	
`[Major] From: MMA@hostname "Datacenter" Time: <Date> <Time>`
 	
`[90:53] /dev/rmt/1m Cannot seek to requested position ([5] I/O error)`
 	
Quantum has confirmed a problem with the controller firmware. There is a cumulative slip occurring in the tach relative to the tape. When such a slip occurs and the drive detects the BOT marker, the drive reconstructs its internal directory. The problem occurs only when tape media containing large amounts of data are used.

Workaround
Consult your HPE support representative before you proceed. You need to upgrade the DLT8000 drive firmware to version V51. More details about the firmware changes can be found in Service Note A5597A-27.

Backup session fails when the Media Agent runs on a AIX

Problem

If another medium is loaded to a tape drive during a backup session that writes backup data to this drive's tape library, the Data Protector Media Agent running on an IBM AIX system may not appropriately handle the loaded medium. In this case, the backup sessions fails.

The root cause of the problem is an AIX operating system limitation in shared memory allocation functionality. The problem occurs more frequently when a relatively high Disk Agent concurrency is used.

Workaround

Enable the IBM AIX extended shared memory model by setting the Data Protector omnirc option `EXTSHM` to the value `ON`.

Issue with SmaryArray 6i firmaware causes failure in drive based encryption

Problem

If an LTO 4 device is connected to a SmartArray 6i controller, drive based encryption may fail due to an issue with the SmartArray 6i firmware.

Workaround

Check if a newer version of the firmware resolves the issue or use a different SCSI controller.

During configuartion, a StoreOnce Backup fails with an error message

Problem

When configuring a StoreOnce Backup system device, if the Client ID field contains any of the characters "_", "-", ".", or "+", the following error is displayed:

```
Could not get information for host Hostname using gateway GatewayName…
```

Workaround

None. Do not use the above mentioned characters for client IDs.

Non-Data Protector issues related to integrations

Microsoft Exchange Server

Due to MAPI behavior, the subject line of a backed up message is wrong

Problem

Due to MAPI behavior, if the subject line of a backed up message begins with a sequence of up to 4 non-space characters followed by a space, and any of these non-space characters is a colon (":"), the message, once restored, will have a wrong subject line. For example, a message with the original subject line `ABC: hala` will get the subject line `ABC: ABC: hala.` after the restore.

This does not apply to standard prefixes for e-mail subjects, such as `Re:`, `Fwd:`, and so on, if they are

generated automatically by your e-mail client (for example, by pressing the **Reply** button in Microsoft Outlook).
Workaround
None

Microsoft SQL Server

Instant recovery of Microsoft SQL Server databases fails

Problem
Instant recovery of Microsoft SQL Server databases fails.
Workaround
Follow the instant recovery procedure in the *HPE Data Protector Zero Downtime Backup Integration Guide*. You need to restart the services of the SQL Server instance after the instant recovery completes. If this action does not automatically start a recovery of all system databases, perform the following: 1. Start the SQL Server instance in the single-user mode.   2. Manually run a recovery of the master database.   3. Run a recovery of every other system database. SQL Server instance must still be running in the single-user mode.   4. Restart the services of the SQL Server instance.

Microsoft Volume Shadow Copy Service

Restore of MSDE Writer and Microsoft SQL 2005 writer components fails

Problem
The following MSDE Writer and Microsoft SQL 2005 writer components cannot be restored while the Microsoft SQL Server is online: `master`, `model`, and `msdb`.
Workaround
None

Snapshot backup of an Exchange Server 2003 database fails

Problem
A snapshot backup of an Exchange Server 2003 database fails, and event ID 9607 is logged.
Workaround
For information on how to resolve this problem, see the Microsoft webpage http://support.microsoft.com/kb/910250.

Backup session fails during the snapshot creation

Problem
With HPE P6000 EVA Disk Array Family, a backup session may fail if there are more than 4 source volumes (original disks) in a snapshot set.

Workaround
None. Make sure that the number of source volumes in a backup specification does not exceed 4 and that the next snapshot creation starts no earlier than 30 minutes after the last snapshot was deleted.   Also ensure that you upgrade firmware and HPE Command View (CV) EVA to the latest version.

Backup session that uses software provider fails

Problem
With HPE P6000 EVA Disk Array Family, a backup session that uses software provider fails, reporting that shadow copies could not be created.

Workaround
Install the latest HBAs firmware and start a new backup session.

Client system fails abnormally for every second or third backup

Problem
With HPE P9000 XP Disk Array Family with hardware providers configured, the client system fails abnormally every second or third backup. This may be caused by particular versions of HPE MPIO DSM for HPE P9000 XP Disk Array Family.

Workaround
Ensure that you are using a supported version of HPE MPIO.

Limitation of any virtual disk in the HPE Command View (CV) EVA Virtual Disks

Problem
The full path of any virtual disk in the HPE Command View (CV) EVA Virtual Disks hierarchy should not exceed 650 characters in length.

Workaround
None. A future release of the hardware provider may remove this limitation.

During shadow copy import, a warning message is logged to the Application Event Log

Problem
With the VSS P9000 XP Array hardware provider on Windows Server 2008 systems, warning

messages are logged to the Application Event Log during each shadow copy import. The issue does not appear on Windows Server 2008 R2 systems.

Workaround
None. A future release of the VSS P9000 XP Array hardware provider may remove this issue.

During a transportable backup , an error is displayed when Data Protector tries to break the shadow copy set

Problem

When using the P6000 EVA Array hardware provider on Windows Server 2008 systems, during a transportable backup when Data Protector tries to break the shadow copy set, the following errors are reported:
 	
 `[Minor] From: OB2BAR_VSSBAR@hostname "MSVSSW" Time: <Date> <Time> Failed to break Shadow Copy Set of session '2011/01/11-4:tpc211'.`
 	
 `[Warning] From: OB2BAR_VSSBAR@hostname "MSVSSW" Time: <Date> <Time> [145:714] Rescanning system due to Break Shadow Copy Set failure.`
 	
 `[Minor] From: OB2BAR_VSSBAR@hostname "MSVSSW" Time: <Date> <Time> Failed to disable backup '2011/01/11-4:tpc211'`
 	
 The issue appears if the P4000 SAN Solutions hardware provider is also installed on the same system. The issue does not appear on Windows Server 2008 R2 systems.

Workaround
Remove the P4000 SAN Solutions hardware provider or use a different client as the backup system. A future release of the P4000 SAN Solutions hardware provider may remove this issue.

Operation fails during instant recovery with the Switch of disks method

Problem
On Windows Server 2008 R2 systems with the VDS hardware provider installed, when performing an instant recovery with the Switch of disks method and using a P6000 EVA Array with a large number of LUNs, the operation may fail.

Workaround
Use the Copy of replica data method instead of the Switch of disks method.   Recommendation: To avoid the problem, remove the VDS hardware provider. Note that there are use cases which require the VDS hardware provider to be installed. For details, see the *HPE Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Session fails when incorrect user credentials exist in the ZDB database

Problem
If two command devices are configured for a disk array of the HPE P9000 XP Disk Array Family

which supports authorization verification, one operating in the user authentication mode and the other in the conventional mode, a problem may occur when you run a ZDB or IR session if no or wrong user credentials exist in the ZDB database (XPDB). In such circumstances, the problem occurs if the HPEP9000 XP Agent first connects to the command device with enabled authentication, and after failing to start the requested operation, it connects to the command device with disabled authentication. At this point the session fails unexpectedly.

Workaround

Do one of the following and restart the session afterwards:

- Using the `omnidbxp -user` command, add correct user credentials to the XPDB or update the existing ones appropriately.

  For command syntax and usage examples, see the `omnidbxp` reference page in the *HPE Data Protector Command Line Interface Reference* or the `omnidbxp` man page.

- Disable the user authentication mode on the command device.

- Prevent the HPEP9000 XP Agent from connecting to the command device operating in the user authentication mode using either method:

  - Unpresent the command device from the application system and the backup system.

  - Follow the steps:

    1. On the application system and the backup system, set the `SSEA_QUERY_STORED_CMDDEVS` omnirc option to `1`.

    2. Remove the data belonging to the command device from the XPDB using the `omnidbxp -cm -remove` command.

Microsoft SharePoint Server

During the restore, the parameter values increases

Problem

When the number of site collections of the backed up content database equals to the value of the parameter `Site Level of Warning`, during the restore the values of the `Site Level of Warning` and the `Maximum Number of Sites` parameters increases as follows:

`Site Level of Warning` = number of site collections + 500

`Maximum Number of Sites` = number of site collections + 1000

Workaround

None.

Data inconsistency

Problem

After a restore of the configuration database, the data in the Microsoft SharePoint Server filesystem caches on front-end Web Server systems might not be consistent with the data in the newly-restored

configuration database.
Workaround
Clear the Microsoft Office SharePoint Server file system cache on all server systems in the farm and retry the restore. For details, see the Microsoft web page http://support.microsoft.com/kb/939308.

SAP MaxDB

Backup completes with an error message

Problem
Backup completes with errors if filenames contain spaces.
Workaround
Windows systems: 1. Change the RUNDIRECTORY parameter to short (8+3) path names and edit filenames in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\SAP\SAP DBTech\IndepData`. 2. Restart the database. **HP-UX and Linux systems:** 1. Create a symbolic link to the directory with a space in the name and adjust the RUNDIRECTORY parameter of the database to use the symbolic link. 2. Adjust the values of the `IndepData` parameter in the file `/var/spool/sql/ini/SAP_DBTech.ini` (on HP-UX) or `/usr/spool/sql/ini/SAP_DBTech.ini` (on Linux).

SAP HANA Appliance

SAP HANA services fails to start

Problem

After restore and recovery of an SAP HANA database using Data Protector, a problem with starting SAP HANA services occurs. The following issue is reported when the mouse pointer is paused on an instance name in the scoping pane of SAP HANA Studio:
 	
`InstanceIDSystemNameInstanceNumericalID` - Some services not started
 	
For example, the notification in a pop-up window reads:
 	
`H95 hanasys 95 - Some services not started`
 	
This symptom might indicate a failure to automatically start the SAP HANA name server. After changing the logon user account to the one that is specified in the corresponding SAP HANA backup specification (`SAPHANAUserAccount`), and attempting to manually start the name server, the system reports the following error:
 	
`su - SAPHANAUserAccount`

```
cd InstallationPath/InstanceID/HDBInstanceNumericalID

./HDB start

Start service InstallationPath/sapservices : Permission denied.
```

Workaround

Add the missing access permissions to the SAP HANA name server binary file, and manually start the name server again. Follow the steps:

1. Log on to the SAP HANA system as the `root` user and open a Terminal window.
2. Execute the commands in sequence:

   ```
   cd InstallationPath

   chmod 777 sapservices

   su - SAPHANAUserAccount

   cd InstanceID/HDBInstanceNumericalID

   ./HDB start
   ```

Oracle Server

Backup system is low on resources

Problem
In case the backup system is low on resources (CPU, memory, and so on), the following error is reported by the Oracle Server Manager in the Data Protector Monitor context for the Oracle HPE P9000 XP Disk Array Family integration: `ORA-12532: TNS: invalid argument`
Workaround
Configure the backup system so that it has sufficient resources to simultaneously run the Oracle Server instance and execute a backup session.

Displays warning during the backup set ZDB session

Problem
While performing a backup set ZDB session, the following warning is displayed for each database datafile: `RMAN-06554: WARNING: file n is in backup mode` Processing of each such message may take up to 20 seconds. It considerably slows down backups of databases with a large number of datafiles (200 or more).
Workaround
Configure the backup system so that it has sufficient resources to simultaneously run the Oracle Server instance and execute a backup session.

Manually terminate the RMAN-related Oracle Server processes

Problem
If you abort a running backup set ZDB session after the Oracle RMAN command has already been invoked by Data Protector, the ZDB session is terminated properly, but the RMAN-related Oracle Server processes continue to run on the backup system. These processes need to be manually terminated.
Workaround
To automatically terminate problematic processes properly, run another Data Protector session based on the same ZDB backup specification.

VMware vSphere

VEPA and BSM fails to respond until the time-out period

Problem

While running multiple parallel VEPA backup sessions, a small fraction (1 or 2) of the total number of sessions may stall, causing the VEPA and BSM to not respond until the time-out period. This may occur because vCenter is loaded with multiple concurrent connection requests from the VEPA agent (from parallel VM backup sessions). The stalled VEPA and BSM processes for these sessions may finally time-out with the following message:
 	
 `[Major] From: BSM@hostname "barlist7" Time: <DATE> <TIME>`
 	
 `[61:1002] The OB2BAR Backup DA named "/Datacenter" on host machineName reached its inactivity timeout of xxxx seconds. The agent on host will be shutdown.`

Workaround
After the time-out period: 1. Stop the vepa_bar processes manually and wait for the bsm process associated with it to close. The bsm closes once the vepa_bar exits.   2. Restart the backup specification that contains the failed VM objects.   **NOTE:** If the time-out period elapses before the backup starts (while resolving the objects), increase the SmWaitForFirstBackupClient parameter in Internal Database -> Global Options.

Restore is slower compared to the backup

Problem
The restore of thin disks using the SAN transportation mode is slower compared to the backup. The vCenter Server system receives a large number of requests to "Clear lazy zero" and "Allocate blocks" during the restore, which cause a slower restore and fill up the vCenter Server system database by logging the tasks.   This is caused by a known issue described at

http://kb.vmware.com/selfservice/microsites/search.do?language=en_
US&cmd=displayKC&externalId=1035096.

Workaround

Do one of the following:

- Use an ESX Server as a Data Protector client and select the target datastore for restore.
- Use a vCenter Server system as a Data Protector client and set the `OB2_VEAGENT_RESTORE_`
  `TRANSPORT_METHOD` omnirc option on the backup host to `NBD`.

SAN transport mode for backup and restore

Problem

The backup and restore of a virtual machine on VMware VVol datastores does not use the
SAN transport mode. This limitation is documented by VMWare in the VMware vSphere 6.0
Documentation Center (`Table: Summary of restore snapshot requirements`). See,

http://pubs.vmware.com/vsphere-60/topic/com.vmware.vddk.pg.doc/vddkBkupVadp.9.4.html

Workaround

None.

Fall back to NBDSSL or NBD transport mode

Problem

The backup and restore of a virtual machine with greater than 2TB disks on VMware VVol (Virtual
Volumes) datastores, fall back to NBDSSL or NBD transport mode, when the selected transport
mode is HotAdd.

This is caused by a Known Issue (VDDK cannot HotAdd a > 2TB disk on VVol datastores) described
in *VMware VDDK 6.0 Release Notes*. See,
https://www.vmware.com/support/developer/vddk/vddk-600-releasenotes.html

Workaround

None.

Fall back of SAN transport mode to NBDSSL

Problem

After an upgrade to Data Protector 9.05, the SAN transport mode falls back to NBDSSL on the
vSphere versions 5.1 and 5.5.

This is a VMware VDDK 6.0 Update1 issue. For more details, see the following URL:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_
US&cmd=displayKC&externalId=2135621.

Workaround

None

Sybase Server

Abort the Sybase backup session

Problem
On Solaris systems, aborting a Sybase backup session makes the system unresponsive.
Workaround
Abort the backup session by terminating the *$SYBASE_HOME_DIR*/bin/sybmultbuf process from the command-line interface.

Disk array integrations

Delay in snapclone creation

Problem
The Data Protector integration with HPE P6000 EVA Disk Array Family provides instant recovery by use of snapclones. The snapclone creation takes time and requires disk array resources. The actual performance impact depends on factors such as disk management, configuration, I/O load, and disk usage. Thus, HPE strongly recommends to perform performance benchmarking in sensitive environments before using snapclones. Data Protector also provides built-in performance boosting functionality. For example: • You can allocate snapclones to a different disk group than the one used for the original virtual disks, thus redirecting read and write operations on a replica from the original disk group to a replica disk group, or allocating low-performance disks for replicas. • During a ZDB-to-disk+tape or ZDB-to-tape session, you can postpone the backup to tape until the snapclones are fully created, thus preventing performance degradation of the application during this phase. For further assistance, contact HPE support.
Workaround
None.

Snapshot backup fails with the error message

Problem
On Windows systems, if performing a snapshot backup on P6000 EVA Array, the following message may occurs: [Normal]Starting drive discovery routine. [Major]Resolving of filesystem *fsname* has failed. Details unknown.

Workaround
Install Secure Path version 4.0B and patch v4.0B-3. The patch can be obtained from the HPE webpage https://softwaresupport.hpe.com/patches.

Unrecoverable error occurs on the backup system.

Problem
When using the Secure Path 4.0C driver, unrecoverable error occurs occasionally on the backup system.
Workaround
None.

During ZDB or IR session, the dismount operation fails

Problem
On Windows Server 2008 systems without the Windows Server 2008 Service Pack 2 installed, it may occur that the Data Protector ZDB agent cannot dismount a volume during an ZDB or IR session, although no processes are running which could keep the volume locked and prevent the dismount operation.
Workaround
- On the system where the problematic volume resides, perform one of the following: - Update the operating system to Windows Server 2008 Service Pack 2.   - Install a specific Windows Server 2008 hotfix. The hotfix package can be obtained from the Microsoft website http://support.microsoft.com/kb/952790.   - Set the `omnirc` option `SMISA_FORCE_DISMOUNT` (in the case of the Data ProtectorHPE P6000 / HPE 3PAR SMI-S Agent) or `SSEA_FORCE_DISMOUNT` (in the case of Data ProtectorHPEP9000 XP Agent) to `1`.   - Restart the session that failed.

Pop up window occurs with a message to format a disk

Problem

In circumstances when several ZDB sessions that involve the HPE P6000 / HPE 3PAR SMI-S Agent and a Windows Server 2008 SP2 backup system are running simultaneously, the backup administrator logged on the backup system using the system default administrative account might be occasionally presented with a pop-up window, asking them to format a disk which is presented to the backup system. A message similar to the following is displayed in the pop-up window:
 	
`You need to format the disk in drive `*`DriveLetter`*`: before you can use it.`
 	
`Do you want to format it?`

This was recognized as a known issue by Microsoft, and was addressed by the hotfix available at http://support.microsoft.com/kb/971254. When installed, the hotfix significantly reduces the frequency of such occurrences, but it does not completely eliminate them. According to Microsoft, the problem might also occur on Windows Server 2008 R2.

Workaround

Click **Cancel** to close the pop-up window. To avoid such pop-up windows from reappearing, disable the system-default administrative account and use another user account. The workaround might not be useful on Windows Server 2008 R2 systems. For further assistance, contact HPE Customer Support Service or Microsoft Support directly.

Problem occurs during the ZDB backup sessions

Problem

On Windows Server 2008 R2 systems, when using the Data Protector Microsoft Volume Shadow Copy Service integration or the Data ProtectorHPE P6000 / HPE 3PAR SMI-S Agent, you may encounter either of the following problems after several zero downtime backup sessions have been simultaneously and continuously running for several days:

- Although presented to the backup system, target volumes are not recognized by the operating system. As a result, the affected ZDB session ends abnormally. All consecutive ZDB sessions fail as well.

  Although this problem turned out not to occur under ordinary conditions, it is not possible to exclude that it will occur in your environment.

Workaround

None. HPE is collaborating with external partners to find a solution.

On the application system a Stop error message appears

Problem

A critical system error occurs on the application system, resulting in a Stop error message (displayed in white text on a blue screen).

This was recognized by Microsoft as a known issue in the Microsoft Multipath I/O (MPIO) framework driver, and was addressed by the hotfixes available at http://support.microsoft.com/kb/2511962 and http://support.microsoft.com/kb/2549567. The hotfixes resolve one aspect of the issue and significantly reduce the probability of a system failure.

Workaround

Install the hotfixes on the application system, and rerun the problematic sessions. If the problem persists, avoid running multiple ZDB sessions in parallel.

Session fails when incorrect credentials exist in the ZDB database

Problem

If two command devices are configured for a disk array of the HPE P9000 XP Disk Array Family which supports authorization verification, one operating in the user authentication mode and the other in the conventional mode, a problem may occur when you run a ZDB or IR session if no or wrong user credentials exist in the ZDB database (XPDB). In such circumstances, the problem occurs if the HPEP9000 XP Agent first connects to the command device with enabled authentication, and after failing to start the requested operation, it connects to the command device with disabled authentication. At this point the session fails unexpectedly.

Workaround

Do one of the following and restart the session afterwards:

- Using the `omnidbxp -user` command, add correct user credentials to the XPDB or update the existing ones appropriately.

  For command syntax and usage examples, see the `omnidbxp` reference page in the *HPE Data Protector Command Line Interface Reference* or the `omnidbxp` man page.

- Disable the user authentication mode on the command device.

- Prevent the HPEP9000 XP Agent from connecting to the command device operating in the user authentication mode using either method:

  - Unpresent the command device from the application system and the backup system.

  - Follow the steps:

    1. On the application system and the backup system, set the `SSEA_QUERY_STORED_ CMDDEVSomnirc` option to `1`.

    2. Remove the data belonging to the command device from the XPDB using the `omnidbxp - cm -remove` command.

Issue in handling the *Super* user account privilege level

Problem
If you remove the last HPE 3PAR StoreServ Storage snapshot presentation that belongs to a specific application system, the application system is also removed from its HPE 3PAR StoreServ Storage virtual domain. The problem is caused by a known issue in handling the *Super* user account privilege level by the HPE 3PAR StoreServ Storage firmware.
Workaround
Configure the Data ProtectorHPE 3PAR StoreServ Storage integration agent by choosing an HPE 3PAR StoreServ Storage system user account that only has the *Edit* privilege level assigned.

Non-Data Protector issues related to Granular Recovery Extensions

VMware vSphere

Windows Server 2008 in combination with Tomcat Server displays an error message.

Problem
When you select a virtual machine and navigate to the **HPE Data Protector** plugin tab, the following error message is displayed: HTTP Status 500 - Exception javax.servlet.ServletException: Unable to read shell environment variables org.apache.catalina.servlets.CGIServlet.init(CGIServlet.java:310) org.apache.catalina.valves.ErroReportValve.invoke(ErrorReportValve.java:102) ... This error appears in Windows Server 2008 environments in combination with some versions of the Tomcat Server for vCenter.
Workaround
Change the os.name property in the Tomcat configuration: 1. Run the Tomcat configuration utility: **Start** > **Vmware** > **Vmware Tomcat** > **Configure Tomcat**. 2. Click the **Java** tab and add the following line to Java options: –Dos.name="Windows 2008". 3. Restart the Tomcat Server.

Microsoft Exchange Server

Recovery of an mailbox item fails with an error message

Problem
Recovery of an entire mailbox or single mailbox items using the Data Protector Granular Recovery Extension for Microsoft Exchange Server in an Exchange Server 2013 environment with the Cumulative Update 1 for Exchange Server 2013 (Exchange 2013 CU1) installed fails with the following error message: The call to 'net.tcp://serverName/Microsoft.Exchange.MailboxReplicationService serverName (15.0.620.29 caps:3F)' failed. Error details: must be logging in with GUIDs, not legDN Parameter name: owner.

The problem is caused by a known Exchange 2013 CU1 issue, and does not appear in Exchange Server 2013 environments without the Exchange 2013 CU1 installed. For details, see http://technet.microsoft.com/en-us/library/jj150489(v=exchg.150).aspx.
Workaround
None. Installing a future Microsoft Exchange Server patch will resolve the issue.

Non-Data Protector issues related to disaster recovery

After the disaster recovery, the operating system fails to start

Problem
During an Enhanced Automated Disaster recovery of an Red Hat Enterprise Linux 5.1, the restore session completes successfully, but the operating system is left in an inconsistent state after the disaster recovery and does not start successfully.
Workaround
Update the GRUB bootloader package to `grub-0.97-13.5.src.rpm` or a later version, as described in http://rhn.redhat.com/errata/RHBA-2008-0440.html.

Non-Data Protector issues related to reporting

CRS service stops responding in the Microsoft Outlook

Problem
While using Microsoft Outlook, when you add a report to a report group specifying e-mail as the send method, and then try to start the report group, the CRS service stops responding and must be restarted. 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.
Workaround
To prevent this behavior, customize security settings so that you set the **When sending items via Simple MAPI** option to `Automatically approve`. For information on how to customize security settings for Microsoft Outlook XP, 2003, or 2007, see the respective Office Resource Kit. Additionally, Outlook Express can be used as an alternative to Outlook, as it does not require any user intervention for sending e-mails. Data Protector is able to send reports in HTML format if used in combination with Outlook Express. Otherwise an HTML report is sent as an attachment. Outlook Express is installed by default on specific Windows operating systems and is the default MAPI handler on those systems. If you plan to use Outlook Express, do not install any other e-mail software (including Outlook) since it typically replaces the default MAPI handler. If you are using Microsoft Office, ensure that you do not select Microsoft Outlook during Microsoft Office installation. Outlook Express supports only the SMTP protocol as e-mail carrier. If you plan to use Outlook Express with Microsoft Exchange Server systems, the **SMTP Mail Connector** option must be

enabled on the Microsoft Exchange Server. For details of how to configure SMTP on Microsoft Exchange Server system, see the Microsoft webpage http://support.microsoft.com/kb/265293.

E-mail reporting using MAPI fails to function

Problem
If a Data ProtectorCell Manager and Microsoft Exchange Server 2003 or 2007 coexist on the same system, e-mail reporting using MAPI does not function. This is because Microsoft does not support installing Outlook on a system with Microsoft Exchange Server 2003 or 2007 installed.
Workaround
Use the e-mail SMTP send method for reports and notifications.

International characters are incorrectly displayed

Problem
On UNIX systems, due to the operating system limitations, international characters in localized e-mail notifications and reporting may be displayed incorrectly if they are transmitted between systems using a different locale.
Workaround
None.

Inappropriate adjustment of the applet size

Problem
When viewing web reports using Netscape Navigator, after resizing the browser window the applet does not automatically adjust its size appropriately.
Workaround
Start Netscape Navigator manually, resize the window to the desired size and only then open the `WebReporting.html` file.

Characters are not displayed correctly when web reporting is used

Problem
In localized UNIX environments with SJIS or EUC Japanese locale set, the non-UTF-8 web reporting input data is converted into UTF-8 (Unicode) before it is written to the Data Protector configuration files. Such characters will not be displayed correctly when using web reporting.
Workaround
None

Creating report takes significant time

Problem
When you are backing up Data Protector clients not configured for Data Protector report, the report lists all clients from a specified network range. In case you specify a C-class network that is in another subnet, the report can take significant time to be created.
Workaround
None

Older web browsers do not support local viewing of Unicode files

Problem
If you use Data Protector reporting and the HTML output format, a Unicode file is generated. Some older web browsers do not support local viewing of Unicode files. However, the files may be displayed correctly if retrieved from a Web server.
Workaround
None.

Email notifications may not be displayed correctly for Japanese characters

Problem
If you receive localized Data Protector e-mail notifications containing Japanese characters on the host where Japanese is not the default locale, the output of the notifications may not be displayed correctly.
Workaround
1. If you have this problem with the Microsoft Outlook, save the message in the HTML format, then open it in a web browser and follow the next step. 2. If you use a web browser, select the Japanese locale, Shift-JIS, EUC, or UTF-8. For example, select **View** > **Character Encoding** > **More Encodings** > **East Asian-Japanese (Shift_JIS)**.

Limiting the maximum number of columns in a table results in some issues

Problem
Due to the Microsoft Office Word 2007 limitation which states that the maximum number of columns in a table is 63, the following issue can occur: When using Microsoft Outlook 2007 and "email SMTP" send method, HTML format, for Device Flow Report and Session Flow Report, Outlook does not display properly the tables in the reports since these reports contain more than 63 columns. The same issue occurs if you log such a report to an HTML file and then try to open it with Microsoft Office Word. Also, in both cases, the tooltips are not displayed.
Workaround
Do not use Word to display such a report. Use a web browser supported by Data Protector. You can

open the report with a web browser in one of the following ways:

- Open the mail. In the **Other Actions** menu, click **View in Browser**.

- Since the report is sent also as the HTML format attachment, you can open the attachment directly from Outlook, or you can save the attachment first and then open it with a supported browser.

Other known non-Data Protector issues

Inter-operability problem between Windows and UNIX platforms

Problem
When mounting a CIFS share on a UNIX system, the shared directory size is not calculated correctly and Data Protector backup statistics consequently report a wrong backup size at the end of the backup session. The reason are inter-operability problems between Windows and UNIX platforms.
Workaround
None

Backup fails because of the shared memory shortage

Problem
Backup on UNIX systems may fail because of the shared memory shortage with the following error:

```
Cannot allocate shared memory pool (IPC Cannot Create Shared Memory Segment
System error: [22] Invalid argument ) => aborting
```

Workaround: The actions are different for different operating systems. After you have applied the changes, you need to restart the system.

HP-UX systems:

Set the OB2SHMEM_IPCGLOBAL option to 1 in the file /opt/omni/.omnirc.

Solaris systems:

Set the kernel parameters in the /etc/system file as follows:

```
set shmsys:shminfo_shmmax=4294967295
```

```
set shmsys:shminfo_shmmin=1
```

```
set shmsys:shminfo_shmmni=100
```

```
set shmsys:shminfo_shmseg=10
```

```
set semsys:seminfo_semmni=100
```

```
set semsys:seminfo_semmsl=100
```

```
set semsys:seminfo_semmns=256
```

```
set semsys:seminfo_semopm=100

set semsys:seminfo_semvmx=32767
```

If the problem persists, the parameter value needs to be increased.

Workaround
None.

Host name resolution is used for communication between different systems

Problem
Data Protector uses host name resolution for communication between different systems. This is done either via DNS servers or via /etc/hosts or /etc/lmhosts file. On Windows clients, if the DNS service is not available or correctly configured, you can edit the hosts (lmhosts) file, which is located in the %SystemRoot%\System32\drivers\etc directory. Use the hosts file if you want to map IP addresses to host names and lmhosts file if you want to map IP addresses to computer (NetBIOS) names. Additional information on how you can edit these files can be found in the beginning of these two files. Restart Data Protector GUI for changes to take effect. You must ensure that the name resolution is consistent throughout the Data Protector cell.

Workaround
None

Raw device backup fails

Problem
Secure path on HP-UX external device filename may change after restart. This changes the mapping to volume managers. Raw device backups may fail due to a different device file being specified in the backup specification.

Workaround
None

TerminalServiceDatabase configuration objects are not backed up

Problem
When creating a file system backup for a Windows Server 2008 or Windows Server 2012 system, Data Protector GUI does not list TerminalServiceDatabase among Windows configuration objects available for backup.

Workaround
To enable backup of the TerminalServiceDatabase configuration object, install the Terminal Server Licensing service on the system which will be backed up.

RemovableStorageManagementDatabase configuration objects are not backed up

Problem
When creating a file system backup for a Windows Server 2008 or Windows Server 2012 system, Data Protector GUI does not list RemovableStorageManagementDatabase among Windows configuration objects available for backup.

Workaround
To enable backup of the RemovableStorageManagementDatabase configuration object, install Removable Storage Manager on the system to be backed up.

Clients unable to connect to IPv6

Problem
Data Protector clients without the Internet Protocol version 6 (IPv6) functionality are not able to connect to IPv6-only clients in the cell.

Workaround
For all clients running a newer version of Data Protector in such mixed environments, a dual-stack configuration (enabled both IPv4 and IPv6 protocols) is recommended.

During backup session, the performance decreases significantly

Problem
After installing the Quality Pack Patch Bundle 1103 or 1109 on HP-UX 11.31, the Data Protector backup session performance decreases significantly.

Workaround
To resolve this issue, install the kernel patch PHKL_41967.   After installing this patch and setting the parameter, the Data Protector backup performance is restored.

Chapter 5: Resolved issues and enhancements

For the complete list of enhancements and resolved issues added in Data Protector10.00, see the *HPE Data Protector 10.00 List of Implemented Enhancements and Resolved Issues* document available in one of the following directories:

- **Windows systems**: `Data_Protector_home\docs\DP10_00_ResolvedEnhancementsDefects.pdf`
- **UNIX systems**:`/opt/omni/doc/C/DP10_00_ResolvedEnhancementsDefects.pdf`

This document lists all the enhancements and defects that were added in Data Protector version 10.00, post Data Protector9.00 release.

Enhancements and resolved issues in Data Protector 10.02

This section lists the issues resolved and enhancements implemented in Data Protector 10.02.

Global ID	Summary
QCCR2A72160	IDB - omniofflr rollforward operation only works when done completely different than documented
QCCR2A73224	ARS is counting replicated data on the destination CM incorrectly
QCCR2A74036	DP 9.06: MS SQL restore does not use Trans backup but only Full
QCCR2A74244	Wrong statistics in SQL sessions
QCCR2A74460	SQL Automated restore to store LSNs in DP catalog when calculates restore chain
QCCR2A74467	SQL Automated restore to store LSNs in DP catalog when calculates restore chain.
QCCR2A74469	MS SQL restore does not take the correct parallelism for restore by time
QCCR2A74517	DP 9.08 object versions without media positions created regularly with storeonce media
QCCR2A74615	DP Check Installation over GUI fails with the "|110:1043| Hostname reported by client does not match with its name in the Cell Manager configuration files" error
QCCR2A74696	Show information about lock owner if restore is queueing on medium
QCCR2A74792	SQL restore reports problem too late
QCCR2A75059	Password characters are not supported by HP DP on MS SQL integrations
QCCR2A75100	shell-init: error retrieving current directory: getcwd: cannot access parent directories: Permission denied

QCCR2A75124	OpenSSL 0.9.8 vulnerability in DP 8.17
QCCR2A75291	DP 9.09 Data Protector Oracle Server integration - error returned while configuring if password contains special characters.
QCCR2A75514	Protection change of a mirrored VEAgent object version incorrectly propagates to all related VEAgentDisk object versions
QCCR2A75558	Negative Numbers of Media Agents in Replication statistics
QCCR2A75561	The omnidb -filesystem Client:MountPoint -file FileName return time is too long
QCCR2A75584	Barcode scan does not show serial number after reload
QCCR2A75621	IR/SQL ZDB: Query incomplete/failed (Object version backup failed or all media have been overwritten.)
QCCR2A75629	MSM abnormally terminates on MCF import
QCCR2A75630	Instant on license is still shown after installation of capacity based license
QCCR2A75633	Browsing MSSQL restore objects causes GUI to become unresponsive
QCCR2A75657	DBSM abnormally terminates if no object versions are available for restore
QCCR2A75661	Initialized free pool media are not allocated in least recently used order
QCCR2A75668	Advanced Scheduler - SQL jobs are not triggered
QCCR2A75675	"Unable to get Authentication token. Check if Appserver is running" error when refreshing GUI with delay" error
QCCR2A75713	"Tag list" column under "Catalyst item Summary" tab is shown as "unknown" in the Catalyst GUI
QCCR2A75716	DP 10.00: Schedule information is not seen in MFC GUI
QCCR2A75765	DP 10:00: The "omnirpt -rep dl_sched" return the "Error creating the report "Interactive"" error
QCCR2A75766	Windows VBDA stops unexpectedly, if filesystem Change Log Provider is used.
QCCR2A75768	Serialization of clustering calls in INET
QCCR2A75769	Query_LISTALLOVER returns no data (code 1252)
QCCR2A75770	The omniofflr fails with the "Unknown option -cleaning" error
QCCR2A75771	bma.exe of DP A.09.09_115 does not work with "NUL" Windows device / special file
QCCR2A75774	Backup size output differs depending on the used tool
QCCR2A75775	9.09_115 Power On error "Share presentation failed" with German Windows backup host
QCCR2A75776	The dbsm stops responding during the execution of omnirpt -report obj_lastbackup

QCCR2A75827	Security issue with perl provided with Data Protector
QCCR2A75837	Hostnames on 3PAR are case sensitive
QCCR2A75843	DP GUI ends abnormally
QCCR2A75889	Buffer overflow with getinfo for long patch names
QCCR2A75908	SQL integration when Windows authentication selected user rights
QCCR2A75909	MSSQL Statistic Info Issues with more than 50 backup objects
QCCR2A75917	EventLogMessages variable flag-based filtering
QCCR2A75932	DP 9.06:The best rollback procedure for a MoM in cluster
QCCR2A75943	Download of disk descriptor file ('vm_name_scsi_id.vmdk') fails
QCCR2A75972	EventLogMessages variable flag-based filtering
QCCR2A75985	Windows VBDA stops unexpectedly if CONFIGURATION object contains paths longer than supported 1023 characters.
QCCR2A75987	During Oracle backup the BSM reports the "Bar backup session was started but no client connected" error
QCCR2A76001	Restarted failed objects ignore custom protection, default protection is set
QCCR2A76024	Cleanup of unused omnirc variables
QCCR2A76057	The "StoreOnce is offline" error
QCCR2A76066	Failed sessions are not purged
QCCR2A76084	Data Protector cannot recognize added slots and tapes
QCCR2A76089	The "Cannot open device (StoreOnce error: StoreOnce device offline." backup error
QCCR2A76129	AS triggers schedules out of time
QCCR2A76139	Advanced backup to disk licenses do not count the data used
QCCR2A76149	DP 10.00 omniinetpasswd -inst_srv_user UserName@Domain requirement
QCCR2A76152	Restore from B2D backup of large (multi-segment) catalog stored with log mode LOG_FILES or LOG_DIRECTORIES
QCCR2A76162	EXEC_INTEGUTIL hardening
QCCR2A76165	Incremental backups ignore consolidated full backups in the chain
QCCR2A76168	DP 9.09_b116 - DPWIN_20240 installation does not update HPEDpHsm automatically
QCCR2A76172	VM restore fails if multiple datastores are used and restore to original name is performed
QCCR2A76176	Schedules are not starting and are not visible in Home screen after upgrade

QCCR2A76177	The DBSM abnormally terminates in FUN_LISTPOOLS when no pools exist in IDB
QCCR2A76181	Improve omnicreatedl command - modify specific datalist attribute/value
QCCR2A76189	Restore fails with the "Cannot create: (|17| File exists)" error
QCCR2A76192	The CRS ends abnormaly when lic.dat file is too big
QCCR2A76193	PostgreSQL 9.6 support
QCCR2A76194	THe BSM reports the "Object details of the object are corrupted" error
QCCR2A76198	Cross CM replication objects protection
QCCR2A76215	SAP HANA backup fills up the debug.log
QCCR2A76231	The command "omnimm -merge_library" fails to merge teamed stores
QCCR2A76235	DP 10.01: GUI warning is missing and (scheduled) backup fails (aborting duplicate objects)
QCCR2A76251	DP 9.09_116: Exchange GRE fails to display restore progress and capacity
QCCR2A76260	After upgrade to 10.01 the internal error is shown in the Dashboard
QCCR2A76261	PowerOn from object/session copy fails - document power on \ live migrate behaviour of copy sessions
QCCR2A76268	Increase default value of OB2RELSTATSLEEP to 180 seconds
QCCR2A76290	DPServer.log flooded with the "AutoPassJ exception:|null|!" messages
QCCR2A76322	Poor post-backup replication session performance
QCCR2A76324	The "IPC Read Error"
QCCR2A76329	GRE with Linux mount proxy - attempting to browse the partitions causes the mount proxy server to stop responding
QCCR2A76334	DP 9.07 b110: Copy session fails, source protection removed anyway
QCCR2A76372	The Max. Number of Parallel Streams per Gateway option is not working a expected
QCCR2A76373	Major errors if disabled gateway host is down during the FS backup
QCCR2A76374	Mixing B2D and non-B2D devices in same specification results in strange device order
QCCR2A76375	DP 9.07: Not able to restore the database
QCCR2A76384	Extended message for "duplicate objects" error
QCCR2A76388	install_telemetry_client_service.bat uninstall fails to stop the service
QCCR2A76443	Binary master does not start install service with -ecmd parameter during hotfix push
QCCR2A76452	DP 10.00 - The new scheduler does not display some entries

QCCR2A76477	Certificate generation on AIX fails
QCCR2A76494	The omnicellinfo -cell command reports duplicates
QCCR2A76511	DP 10.01 REST API example page sends wrong parameters to REST API
QCCR2A76521	Import of MS cluster fails
QCCR2A76531	SharePoint 2013 with AlwaysOn MS SQL 2012 Suport
QCCR2A76532	Cell Manager console freezes at IBM Tape Library discovering on MA (edit device)
QCCR2A76537	DP 9.09 ZDB backups which are using mirror devices stop responding
QCCR2A76556	Incremental backup ignores preceding incremental backups if the chain ends with a full backup completed with errors
QCCR2A76579	Several csm.exe processes are not ending when copy sessions ends
QCCR2A76606	Automatically discover changed SCSI address messes up device configuration
QCCR2A76610	The "Cannot open: (|2| The system cannot find the file specified.)" warning message
QCCR2A76688	GRE with Linux mount proxy - cannot browse logical volumes
QCCR2A76536	Information needs to be added to Deduplication.pdf, also the .pdf is missing on DP 9.09+

Chapter 6: Data Protector documentation

> **NOTE:**
> The documentation set available at the HPE support website at https://softwaresupport.hpe.com/ contains the latest updates and corrections.

You can access the Data Protector documentation set from the following locations:

- Data Protector installation directory.

  Windows systems: *Data_Protector_home*\docs

  UNIX systems: /opt/omni/doc/C
- **Help** menu of the Data Protector GUI.
- HPE Support website at https://softwaresupport.hpe.com/

Documentation map

The following table shows where to find information of different kinds. Squares shaded in gray are a good place to look first.

	Admin	Help	Getting Started	Concepts	Install	Troubleshooting	DR	CLI	PA	Integration VSS	Integration Guide MSFT	Oracle/SAP	IBM	Sybase/NDMP	Virtual Env	ZDB Guides ZDB Admin	ZDB IG	GRE Guide Exchange	SharePoint	VMware
Admin tasks	X	X																		
Backup		X	X	X						X	X	X	X	X	X	X	X			
CLI								X												
Concepts, techniques		X		X						X	X	X	X	X	X	X	X	X	X	X
Disaster recovery				X			X													
Installation, upgrade			X		X					X										
Instant recovery				X	X											X	X			
Licensing					X					X										
Limitations		X			X	X				X	X	X	X	X	X		X			
New features		X								X										
Planning strategy		X		X																
Procedures, tasks	X	X			X	X	X			X	X	X	X	X	X	X	X	X	X	X
Recommendations				X					X											
Requirements					X					X	X	X	X	X	X					
Restore	X	X	X	X						X	X	X	X	X	X	X	X	X	X	X
Supported configurations				X																
Troubleshooting		X				X	X			X	X	X	X	X	X	X	X	X	X	X

Abbreviations

Abbreviations in the documentation map above are explained below. The documentation item titles are all preceded by the words "HPE Data Protector."

Abbreviation	Documentation item	
Admin	Administrator's Guide	This guide describes administrative tasks in Data Protector.
CLI	Command Line Interface Reference	This guide describes the Data Protector command-line interface, command options, and their usage as well as provides some basic command-line examples.
Concepts	Concepts Guide	This guide describes Data Protector concepts, zero downtime backup (ZDB) concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented Help.
DR	Disaster Recovery Guide	This guide describes how to plan, prepare for, test, and perform a disaster recovery.
Getting Started	Getting Started Guide	This guide contains information to get you started with using Data Protector. It lists installation prerequisites, provides instructions on installing and configuring a basic backup environment and procedures for performing backup and restore. It also lists resources for further information.
GRE Guide	Granular Recovery Extension User Guide for Microsoft SharePoint Server, Exchange and VMware	This guide describes how to configure and use the Data Protector Granular Recovery Extension for: • Microsoft SharePoint Server • Exchange Server • VMware vSphere
Help	Help	
Install	Installation Guide	This guide describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This guide details how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.

Abbreviation	Documentation item	
Integration Guide	Integration Guide	This guide describes the integrations of Data Protector with the following applications: • **MSFT:** Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server. • **IBM:** Informix Server, IBM DB2 UDB, and Lotus Notes/Domino Server. • **Oracle/SAP:** Oracle Server, MySQL, SAP R3, SAP MaxDB, and SAP HANA Appliance. • **Sybase/NDMP:** Sybase and Network Data Management Protocol Server. • **Virtual Env:** Virtualization environments integration with VMware vSphere, VMware vCloud Director, and Microsoft Hyper-V.
Integration VSS	Integration Guide for Microsoft Volume Shadow Copy Service	This guide describes the integrations of Data Protector with Microsoft Volume Shadow Copy Service (VSS).
PA	Product Announcements, Software Notes, and References	This guide gives a description of new features of the latest release. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.
Troubleshooting	Troubleshooting Guide	This guide describes how to troubleshoot problems you may encounter when using Data Protector.
ZDB Admin	ZDB Administrator's Guide	This guide describes how to configure and use the integration of Data Protector with HPE P4000 SAN Solutions, HPE P6000 EVA Disk Array Family, HPE P9000 XP Disk Array Family, HPE 3PAR StoreServ Storage, NetApp Storage, EMC VNX Storage Family, EMC VMAX Storage Family, and EMC Symmetrix Remote Data Facility and TimeFinder. It is intended for backup administrators or operators. It covers the zero downtime

Abbreviation	Documentation item	
		backup, instant recovery, and the restore of filesystems and disk images.
ZDB IG	ZDB Integration Guide	This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle Server, SAP R/3, Microsoft Exchange Server, Microsoft SQL Server databases, and Virtual Environment for VMware .

Integrations

Software Application Integrations

Software application	Guides
IBM DB2 UDB	Integration Guide
Informix Server	Integration Guide
Lotus Notes/Domino Server	Integration Guide
Microsoft Exchange Server	Integration Guide, ZDB IG, GRE Guide
Microsoft Hyper-V	Integration Guide
Microsoft SharePoint Server	Integration Guide, ZDB IG, GRE Guide
Microsoft SQL Server	Integration Guide, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	Integration VSS
Network Data Management Protocol (NDMP) Server	Integration Guide
Oracle Server	Integration Guide, ZDB IG
MySQL	Integration Guide
SAP HANA Appliance	Integration Guide
SAP MaxDB	Integration Guide
SAP R/3	Integration Guide, ZDB IG

Software application	Guides
Sybase Server	Integration Guide
VMware vCloud Director	Integration Guide
VMware vSphere	Integration Guide, ZDB IG, GRE Guide

Disk Array System Integrations

Look in these guides for details of the integrations with the following families of disk array systems:

Disk array family	Guides
EMC Symmetrix	all ZDB
HPE P4000 SAN Solutions	Concepts, ZDB Admin, Integration Guide
HPE P6000 EVA Disk Array Family	all ZDB, Integration Guide
HPE P9000 XP Disk Array Family	all ZDB, Integration Guide
HPE 3PAR StoreServ Storage	Concepts, ZDB Admin, Integration Guide
NetApp Storage	Concepts, ZDB Admin, ZDB IG
EMC VNX Storage	Concepts, ZDB Admin, ZDB IG
EMC VMAX Storage	Concepts, ZDB Admin, ZDB IG

Localized documentation

Data Protector is localized into French, Japanese, and Simplified Chinese. The localized documentation set is available in French, Japanese, and Simplified Chinese for Data Protector 10.00.

The following end-user documents are localized to French, Japanese, and Simplified Chinese:

- *HPE Data Protector Getting Started Guide*
- *HPE Data Protector Concepts Guide*
- *HPE Data Protector Administrator's Guide*
- *HPE Data Protector Disaster Recovery Guide*
- *HPE Data Protector Installation Guide*

- *HPE Data Protector Product Announcements, Software Notes, and References*
- *HPE Data Protector Troubleshooting Guide*
- *HPE Data Protector Help*

Data Protector 10.00 localization specific errata

This section lists the updates added to the English version of the HPE Data Protector 10.00 documentation, which are not included in the localized versions of the documents.

Important updates include among others:

- Updated all documents per the latest HPE Data Protector 10.00 Obsolescence Document, available at https://softwaresupport.hpe.com/km/KM02816923.

HPE Data Protector Administrator's Guide

The following prerequisites are added in the chapter, Home Context.

- **Browser recommendation**: To access the different functionalities available from Home context, the system must have Microsoft Internet Explorer v10 or v11 installed.

  > **TIP:**
  > For optimal user experience, HPE recommends that you use Microsoft Internet Explorer v11.

- **Security settings**: When launching Home Context Web pages, the following **Security Alert** window appears.

  This window appears if the certificate is not added to the root trust store, and therefore the connection is flagged as untrusted .To avoid viewing this warning message, complete the following steps:

  1. Copy the file `ascert.crt` from Cell Manager to any temporary directory in the Cell Console client. The `ascert.crt` file is available at the following location in the Cell Manager:

     - Windows: `Data Protector_program_data\OmniBack\Config\Server\AppServer`
     - Linux/HP-UX: `/etc/opt/omni/server/AppServer`

  2. On the Cell Console client, open the command prompt and run the following command:

     `certutil -addstore root ascert.crt`

     This command adds the certificate to the root trust store.

  3. Restart the Data Protector GUI.

The following troubleshooting section is added in the chapter, Home Context:

Icons and buttons are not visible

Problem
The icons and Web page buttons are not visible in for different Home Context Web pages, such as Dashboard, Telemetry, and Scheduler.

Action
The problem appears if Internet Explorer Enhanced Security Configuration (IE ESC) is enabled.   To disable the IE ESC settings, complete the following steps: 1. Close all instances of Microsoft Internet Explorer.   2. Navigate to Windows **Start** menu, point to **Administrative Tools**, and then click **Server Manager**.   3. Under Security Information, click **Configure IE ECS**.   4. Under Administrators, click **Off**.   5. Under Users, click **Off**.   6. Click **OK**.

Updated the Scheduler section in the chapter, Home Context.

HPE Data Protector Installation Guide

The following sections are added in the chapter, Upgrading the Data Protector:

- Upgrading from Data Protector 8.1x and later
- Upgrading to Data Protector 10.00
- Migrating schedules from previous versions

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 Product Announcements, Software Notes, and References (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!