HP Data Protector 6.20 Product Announcements, Software Notes, and References

HP Part Number: N/A
Published: December 2011
Edition: Fifth

Contents

Publication version history

Table 1 Edition history

Version	Date	Description
1.0	March 9, 2011	Initial revision
1.0.1	March 29, 2011	Updated version published on the Web
1.0.2	June 29, 2011	Updated version published on the Web
1.1	December 2, 2011	Updated for the following patches: DPWIN_00551, PHSS_42652, DPSOL_00477, DPLNX_00183
1.1.1	December 21, 2011	Updated version published on the Web

About this guide

This guide provides information about:

- Product announcements
- Limitations and known issues
- Installation requirements (such as hardware, operating system patches)
- Obsolete platforms
- Last-minute changes that are not documented elsewhere and documentation errata

Intended audience

This guide is intended for administrators who want to install and deploy Data Protector, with knowledge of:

- Basic operating system commands and utilities

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 10)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

ⓘ **IMPORTANT:** Provides clarifying information or specific instructions.

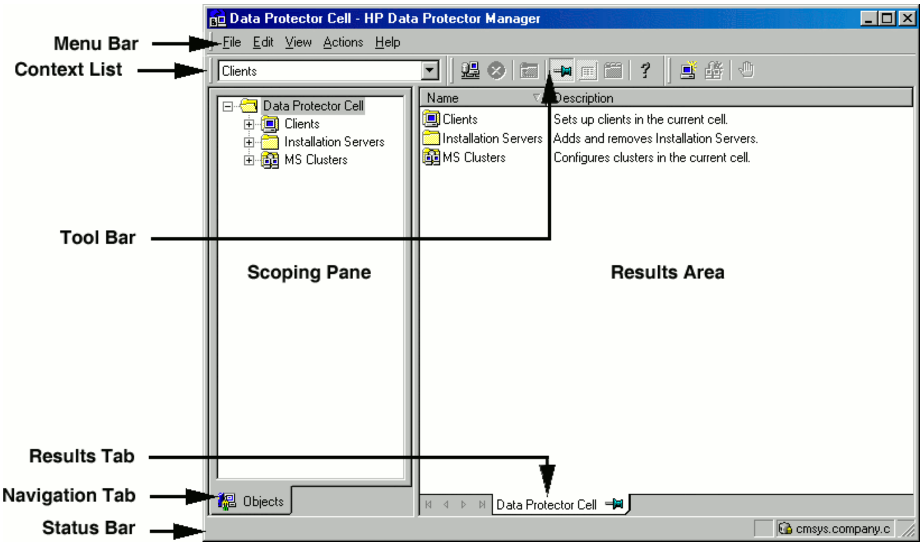
NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Data Protector graphical user interface

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface. You can use the original Data Protector GUI (Windows only) or the Data Protector Java GUI. For information about the Data Protector graphical user interface, see the online Help.

Figure 1 Data Protector graphical user interface



General information

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

HP technical support

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

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

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

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

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/software

- http://www.hp.com/go/imhub
- http://support.openview.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

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

1 Announcements

HP Data Protector automates high performance backup and recovery, from disk or tape, over unlimited distances, to ensure 24x7 business continuity, and seamless integration with HP storage hardware and management 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 HP 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 6.20.

Upgrades

Upgrade information is available in the *HP Data Protector Installation and Licensing Guide*. Procedures for upgrading from Data Protector versions A.06.00, A.06.10, and A.06.11 to Data Protector 6.20 are described.

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 DVD-ROM in the `\DOCS\support_matrices` directory. The following support matrices are available in Portable Document Format (PDF):

- *HP Data Protector 6.20 Device Support Matrix*
- *HP Data Protector 6.20 Disaster Recovery Support Matrix*
- *HP Data Protector 6.20 Media Operations Software Support Matrix*
- *HP Data Protector 6.20 Network Attached Storage (NAS) Support Matrix*
- *HP Data Protector 6.20 Platform and Integration Support Matrix*
- *HP Data Protector 6.20 Virtualization Support Matrix*
- *HP Data Protector 6.20 VSS Integration Support Matrix*
- *HP Data Protector 6.20 Zero Downtime Backup and Instant Recovery Support Matrix for HP P6000 EVA Disk Array Family Using SMI-S Agent*
- *HP Data Protector 6.20 Zero Downtime Backup and Instant Recovery Support Matrix for HP P9000 XP Disk Array Family*
- *HP Data Protector 6.20 Zero Downtime (Split-Mirror) Backup Support Matrix for EMC Arrays*

For the latest version of support matrices on the Web, see http://www.hp.com/support/manuals. In the Storage section, click **Storage Software** and then select your product.

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 *HP Data Protector Command Line Interface Reference*.

Licensing

Data Protector 6.20 leverages the product numbers from Data Protector A.06.00, A.06.10, A.06.11 and Application Recovery Manager A.06.00. All Data Protector, A.06.10, A.06.11 and Application Recovery Manager A.06.00 licenses can be used with Data Protector 6.20 and retain their original functionality. Licenses from previous Data Protector releases are automatically migrated. However, depending on new functionality, you may have to install new product licenses.

For more information, see the *HP Data Protector Installation and Licensing Guide*, chapter *Data Protector licensing*.

Support for older agent versions

Wherever possible, Data Protector components on all clients in a Data Protector cell should be upgraded to version 6.20 during the regular upgrade process. This ensures that customers can benefit from the full feature set of Data Protector 6.20 on all systems in a cell.

However, due to the high demand, support for older agent versions has been extended. Disk Agent and Media Agent components of an older Data Protector version (A.06.00, A.06.10, or A.06.11) are supported in a 6.20 cell with the following constraints:

- Support is limited to the feature set of the older 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.
- Older Media Agent components are not supported in combination with NDMP servers.
- If one Data Protector component on a client is upgraded to 6.20, all other components have to be upgraded to 6.20 as well.

If you have any problems establishing a connection with older agents, consider upgrading to 6.20 as the first resolution step.

Updated information

For the latest version of this document, including corrections and last-minute updates due to known issues, see http://www.hp.com/support/manuals or http://support.openview.hp.com/selfsolve/manuals.

For the latest information about the product, see the Data Protector Web site http://www.hp.com/go/dataprotector.

Patch bundles and related information

Data Protector 6.20 introduces the concept of patch bundles. A patch bundle is a collection of individual yet unreleased patches. Patch bundles are released in patch bundle sets, which contain one patch bundle for each supported Cell Manager platform. A patch bundle set enhances and extends the functionality of a regular product release. A later patch bundle set for a particular product release supersedes earlier patch bundle sets for the same release.

In specific parts of the Data Protector documentation set, information relevant to the patch bundle set 6.21 is specially marked with the following line:

(available with patch bundle set 6.21 and superseding updates)

Patch bundle labels of the patch bundle set 6.21 are the following:

Windows systems: `DPWINBDL_00621`

HP-UX systems: `DPUXBDL_00621`

Solaris systems: `DPSOLBDL_00621`

Linux systems: `DPLNXBDL_00621`

To be able to make full use of all features and enhancements provided by this patch bundle set, you need to install an appropriate patch bundle on every system of the Data Protector cell. For installation instructions, see the document enclosed with the patch bundle installation files.

2 Product features and benefits

Below is a summary of the benefits provided by Data Protector 6.20:

- Data Protector support for Backup to Disk devices and deduplication *(available with patch bundle set 6.21 and superseding updates)*
- Data Protector Granular Recovery Extensions:
    - Data Protector Granular Recovery Extension for Microsoft SharePoint Server
    - Data Protector Granular Recovery Extension for VMware vSphere
- Data Protector solutions for virtualization environments:
    - Data Protector Virtual Environment integration
    - Data Protector Granular Recovery Extension for VMware vSphere
- Data Protector solutions for Microsoft applications:
    - Data Protector Microsoft Exchange Server 2010 integration
    - Data Protector Microsoft SharePoint Server 2007/2010 integration
    - Data Protector Microsoft SharePoint Server 2007/2010 VSS-based solution
    - Data Protector Granular Recovery Extension for Microsoft SharePoint Server
- Enhanced replica management and extended disk array support:
    - Enhanced Data Protector Microsoft Volume Shadow Copy integration
    - Support for HP P4000 SAN Solutions
    - Zero downtime backup and instant recovery on Linux platform
    - Zero downtime backup and instant recovery enhancements for HP disk arrays
- Enhanced disaster recovery and support for disaster recovery on new platforms
- Enhanced communication protocol:
    - Support for IPv6
    - Secure control communication
- Support for new platforms

The rest of the chapter gives a more detailed description of these Data Protector 6.20 features and major changes in comparison to the previous Data Protector version.

Data Protector support for the Backup to Disk devices and StoreOnce software deduplication

(available with patch bundle set 6.21 and superseding updates)

Data Protector 6.20 introduces support for the HP StoreOnce software deduplication. By supporting software deduplication, several new concepts are introduced to Data Protector including the StoreOnce library and a new device type, the Backup to Disk device.

The HP StoreOnce software deduplication engine provides the ability to deploy target-side deduplication on virtually any industry-standard hardware, offers greater flexibility than existing solutions as it can be deployed in a wider range of hardware set-ups, and provides enterprise-class scalability. By deleting redundant (duplicate) data, deduplication significantly reduces the amount of required disk storage space, improves overall backup performance, and reduces storage costs. Additionally, deduplication greatly reduces the amount of backup data transmitted across the company intranet for remote backup, restore, and disaster recovery purposes.

Backup to Disk (B2D) devices, which back up data to physical disk storage and include support for deduplication, have the following advantages:

- Deduplication is performed using the StoreOnce software deduplication engine.
- Because disk-based systems are used, restore service levels are significantly higher and media handling errors are reduced.
- B2D devices support multi-host configurations, that is, physical storage space can be accessed through multiple hosts called gateways. It can further be partitioned into individual stores (or logical storage units) representing specific storage sections, and can therefore be accessed by several B2D devices.

For details, see the *HP Data Protector StoreOnce Software Deduplication White Paper*.

Data Protector Granular Recovery Extensions

Data Protector Granular Recovery Extension for Microsoft SharePoint Server

Data Protector 6.20 introduces the Data Protector Granular Recovery Extension for Microsoft SharePoint Server, a specialized extension that tightly integrates into Microsoft SharePoint Server and provides you detailed control over what is recovered. The extension relies on Data Protector to back up content databases. Use this extension to restore individual web site items, such as Calendar or Task items, or documents.

For details, see the new *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*.

Data Protector Granular Recovery Extension for VMware vSphere

Data Protector 6.20 introduces the Data Protector Granular Recovery Extension for VMware vSphere, a specialized extension that integrates into VMware vCenter Server and provides you detailed control over what is recovered. The extension relies on Data Protector Virtual Environment integration to back up the virtual environments. Use this extension to select and restore individual files instead of the whole virtual disk or virtual machine.

For details, see the new *HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*.

Data Protector solutions for virtualization environments

Data Protector Virtual Environment integration

Data Protector 6.20 offers support for various virtualization environments, enabling you to back up and restore virtual machines. Currently, the virtual environment integration supports VMware vSphere and Microsoft Hyper-V.

Support for VMware vSphere

The virtual environment integration uses the vStorage APIs to communicate with VMware vSphere.

The integration supports vCenter environments, where ESX Server and/or ESXi Server systems are managed through a vCenter Server system (which may be installed in a cluster), standalone environments, with standalone ESX/ESXi Server systems, or a mixture of these environments.

The following backup method is available:

- vStorage Image

You can perform the following backup types:

- Full
- Incr
- Differential

Support for Microsoft Hyper-V

The virtual environment integration uses Microsoft Volume Shadow Copy Service (VSS) technology to integrate with Microsoft Hyper-V. Before a virtual machine is backed up, it is put in a consistent state with the help of VSS. This applies also to the Microsoft applications running in the virtual machine, provided that appropriate VSS writers are available.

The following backup method is available:

- Hyper-V Image

You can perform the following backup type:

- Full

Zero downtime backup (backup using hardware providers) is also supported, but instant recovery is not supported.

Additional Virtual Environment integration enhancements

(available with patch bundle set 6.21 and superseding updates)

Microsoft Hyper-V cluster handling

The Microsoft Hyper-V cluster handling enhancement enables the selection of any of the physical cluster nodes or the virtual cluster system to back up all VMs residing on the cluster. In the Data Protector backup specification, non-cluster VMs are listed under their physical nodes and cluster VMs under their virtual cluster system.

Extended platform support for VMware

- Support for additional VMware platforms that can be backed up using Virtual Environment integration has been added.
- Linux is now supported as a VMware backup host.

For details on what is supported, see the latest support matrices at http://www.hp.com/support/manuals.

New Virtual Environment options

The following Virtual Environment integration options have been introduced:

- The **VE Settings** button has been added to the backup specification to enable displaying the Virtual Environment settings and modifying some of them.
- The new `omnirc` options `OB2_VEAGENT_DISABLE_VMOTION_LOCK`, `OB2_VEAGENT_VDDK_RETRY_COUNTER`, `OB2_VEAGENT_VDDK_RETRY_DELAY`, and `OB2_VEAGENT_CLUSTER_RESOURCE_MOVE_TO_NEW_NODE_TIME_OUT` have been introduced for even better customization of Data Protector Virtual Environment integration clients.

Data Protector Granular Recovery Extension for VMware vSphere

See “Data Protector Granular Recovery Extension for VMware vSphere” (page 16).

Data Protector solutions for Microsoft applications

Data Protector Microsoft Exchange Server 2010 integration

Data Protector 6.20 introduces support for the Microsoft Exchange Server 2010, enabling you to perform backups and restores of the Microsoft Exchange Server 2010 databases.

The Data Protector Microsoft Exchange Server 2010 integration is based on the Volume Shadow Copy Service (VSS) technology.

Backup

During backup, databases can be used actively (online backup). In DAG environments, you can back up active and/or passive database copies.

You can select from among the following Microsoft Exchange Server backup types:

- Full
- Copy
- Incremental
- Differential

Zero downtime backup (ZDB) of the Microsoft Exchange Server 2010 data is also supported.

Restore

Each database can be restored using a different restore method. The following methods are available:

- Repair all passive copies with failed status
- Restore to the latest state
- Restore to a point in time
- Restore to a new mailbox database[1]
- Restore files to a temporary location

Instant recovery of the Microsoft Exchange Server 2010 data is also supported.

For details, see the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server* and the *HP Data Protector Zero Downtime Backup Integration Guide*. For details on what is supported, see the latest support matrices at http://www.hp.com/support/manuals.

Data Protector Microsoft SharePoint Server 2007/2010 integration

Data Protector 6.20 introduces support for the Microsoft Office SharePoint Server 2007 and Microsoft SharePoint Server 2010, enabling you to perform backups and restores of the following Microsoft SharePoint Server objects:

- The configuration database
- The Central Administration content database
- Web applications
- Content databases
- SSP sites
- SSP index files

[1] This method also offers the possibility to restore to a recovery database.

Backup

During backup, the Microsoft SharePoint Server 2007/2010 and related Microsoft SQL Server instances can be used actively (online backup).

Data Protector offers the following backup types:

- Full
- Differential
- Incremental

Zero downtime backup (ZDB) of the Microsoft SharePoint Server 2007/2010 data is not supported.

Restore

You can restore objects:

- To the latest state or to a certain point in time
- To the original location or to a new location

Instant recovery of the Microsoft SharePoint Server 2007/2010 data using this integration is not supported.

For details, see the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*. For details on what is supported see the latest support matrices at http://www.hp.com/support/manuals.

Data Protector Microsoft SharePoint Server 2007/2010 VSS-based solution

Data Protector 6.20 introduces an additional backup and restore solution for Microsoft Office SharePoint Server 2007 and Microsoft SharePoint Server 2010, which is based on the Data Protector Volume Shadow Copy Service (VSS) integration in combination with Perl and PowerShell scripts that simplify the usage. The main advantage of the solution is that it supports zero downtime backup (ZDB) and instant recovery of the Microsoft SharePoint Server 2007/2010 data.

For details, see the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server* and the *HP Data Protector Zero Downtime Backup Integration Guide*. For details on what is supported see the latest support matrices at http://www.hp.com/support/manuals.

Data Protector Granular Recovery Extension for Microsoft SharePoint Server

See "Data Protector Granular Recovery Extension for Microsoft SharePoint Server" (page 16).

Enhanced replica management and extended disk array support

Enhanced Data Protector Microsoft Volume Shadow Copy Service integration

Data Protector 6.20 introduces the following enhancements for the Microsoft Volume Shadow Copy Service integration

- Enhanced support for HP disk arrays:
  - VDS hardware provider independent backup.

    The HP P9000 XP Disk Array Family and HP P6000 EVA Disk Array Family VDS hardware providers are no longer required to perform a ZDB.
  - VDS hardware provider independent VSS instant recovery (VSS LUN Resync).

    A new method for performing instant recovery on Windows Server 2008 R2, that complements the VDS hardware provider and Data Protector ZDB agents. Using the VSS

LUN resync functionality, instant recovery can now be performed using the VSS hardware provider only.

  - Instant recovery using standard P6000 EVA Array snapshots or vsnaps.

- Support for third-party disk arrays
- Other enhancements:
  - Support for GPT disks.
  - Support for Cluster Shared Volumes.

For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

Support for HP P4000 SAN Solutions

Data Protector 6.20 introduces support for HP P4000 SAN Solutions. You can perform any form of ZDB and instant recovery using the HP P4000 SAN Solutions VSS hardware provider in combination with the Microsoft Volume Shadow Copy Service technology. The only supported replica type are snapshots, which use demand-allocated storage space and are based on the “redirect on write” technique.

For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*. On how to configure HP P4000 SAN Solutions for use with Data Protector, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*. For details on the supported operating systems and versions, see the latest support matrices at http://www.hp.com/support/manuals.

Zero downtime backup and instant recovery on Linux platform

Data Protector 6.20 introduces support for zero downtime backup (ZDB) and instant recovery (IR) on Linux platform. On this platform, it can integrate with disk arrays of the following disk array families:

- HP P6000 EVA Disk Array Family, via the HP StorageWorks P6000 EVA SMI-S Agent

  The supported backup objects in ZDB and IR sessions are filesystems, disk images, and Oracle Server data.

- HP P9000 XP Disk Array Family, via the HP StorageWorks P9000 XP Agent

  (available with patch bundle set 6.21 and superseding updates)

  The supported backup objects in ZDB and IR sessions are filesystems, disk images, and Oracle Server data.

To enable Data Protector ZDB and IR sessions on a Linux system, you must install an appropriate multi-path device management software on the application system and the backup system, and configure it appropriately. For details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

For the HP P6000 EVA Disk Array Family and the HP P9000 XP Disk Array Family support specifics, see the latest respective support matrices at http://www.hp.com/support/manuals.

Zero downtime backup and instant recovery enhancements for the HP P6000 EVA Disk Array Family and the HP P9000 XP Disk Array Family

Data Protector 6.20 enhances existing zero downtime backup and instant recovery functionality for the following disk array families, as well as provides additional zero downtime backup options for them:

- HP P6000 EVA Disk Array Family

  (other reference forms used: HP P6000 EVA Disk Array Family, P6000 EVA Array, P6000 EVA)

In the Data Protector documentation, this disk array family had formerly been referred to as HP StorageWorks Enterprise Virtual Array.

- HP P9000 XP Disk Array Family

  (other reference forms used: HP P9000 XP Disk Array Family, P9000 XP Array, P9000 XP)

  This disk array family had formerly been referred to as HP StorageWorks Disk Array XP.

Enhanced zero downtime backup and instant recovery functionality

The following zero downtime backup and instant recovery functionality changes and enhancements are available for the **HP P6000 EVA Disk Array Family**:

- Support for instant recovery using standard snapshots and vsnaps

  With Data Protector 6.20, replicas using any of the snapshot types supported for zero downtime backup can also be used for instant recovery. For standard snapshots and vsnaps, only the "copy-back" instant recovery method is available.

  For ZDB and IR policy planning considerations, see the *HP Data Protector Zero Downtime Backup Concepts Guide*. For procedures and other details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

- Support for the instant recovery method of copying replica data (the “copy-back” method)

  With this instant recovery method, depending on the instant recovery option selected, Data Protector either overwrites data in the source volumes with data from the replica or creates a copy of the replica data in the disk group of the source volumes while preserving the source volumes. In both cases, this instant recovery method enables you to use a particular replica in multiple instant recovery sessions. For details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

- An option to leave the replica mounted

  If configured in the ZDB backup specification, Data Protector can leave the target volumes mounted to the backup system after a ZDB session, thus enabling third-party applications to access them for backup purposes.

- Support for zero downtime backup using mirrorclones

  Mirrorcloning is a local replication facility provided by newer P6000 EVA firmware revisions. A mirrorclone is a dynamic replica of a storage volume, which is kept updated with changes made to the original storage volume via a local replication link. Data Protector 6.20 supports creation of standard snapshots and vsnaps of mirrorclones. In instant recovery sessions, data from mirrorclone snapshots is restored to the original volumes, rather than the mirrorclones themselves. In a ZDB backup specification, if mirrorclone is selected as the snapshot source, but mirrorclones of the selected storage volumes do not exist when the ZDB session is started, Data Protector automatically creates them first.

  For ZDB policy planning considerations, see the *HP Data Protector Zero Downtime Backup Concepts Guide*. For procedures and other details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

- Redundancy level selection for the replica

  The HP P6000 EVA Disk Array Family implements nested (hybrid) storage redundancy (RAID) technology, referred to as Vraid. When configuring a ZDB backup specification, you can choose a specific Vraid type or use the same Vraid type as used for the source volumes. Depending on the version of the installed HP Command View (CV) EVA, type of the P6000 EVA disk group defined for the target volumes, and the selected snapshot type, the following Vraid types can be used: Vraid6, Vraid1, Vraid5, and Vraid0. For details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

- Implicitly enforced strict snapshot policy

  The loose snapshot policy has been made obsolete, and the strict snapshot policy now implicitly applies to all ZDB backup specifications. For information on how to update you existing ZDB backup specifications accordingly, see the *HP Data Protector Installation and Licensing Guide*.

- Support for multisnapping

  Newer HP Command View (CV) EVA versions support simultaneous creation of target volumes so that the backup data is consistent not only on each individual target volume, but also across all the volumes that constitute a snapshot. This process is referred to as multisnapping. Multisnapping is used by Data Protector in zero downtime backup sessions wherever supported by the CV and the P6000 EVA firmware.

  Mutisnapping is a prerequisite for and is automatically used in Data Protector zero downtime backup sessions for backing up the Oracle Server data in configurations using Automatic Storage Management (ASM), but can also be enforced for other ZDB purposes for which cross-volume data consistency is required for the replica.

  For details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Zero Downtime Backup Integration Guide*.

- Support for containers

  Containers are an HP P6000 EVA Disk Array Family feature which speeds up the process of reusing storage space. Rather than deleting it, Data Protector converts each storage volume that is no longer needed, but its storage space is expected to be later used for a standard snapshot, vsnap, or snapclone, into a container. When needed, the target volume is created by converting an existing container, thus reducing the time required for its creation, and improving overall backup performance.

The listed Data Protector enhancements are only available for HP P6000 EVA Disk Array Family configurations that use HP Command View (CV) EVA 9.4 or a newer CV EVA version. For details and further information, see the latest support matrices at http://www.hp.com/support/manuals.

The following zero downtime backup and instant recovery functionality changes and enhancements are available for the **HP P9000 XP Disk Array Family**:

- Support for the snapshot replication technique

  Newer HP P9000 XP Disk Array Family models provide a new type of replica volumes in addition to the already supported mirror copies: snapshots. Allocation of storage space for volumes to be used as snapshots is similar to that of vsnaps on the P6000 EVA disk array. Thus, the main advantage of snapshots over mirror copies is lower storage space consumption. Data Protector 6.20 uses snapshots in the same way as mirror copies, provided that secondary volumes (S-VOLs) are appropriately configured on the disk array in advance. Snapshots can be used for all supported forms of zero downtime backup, for instant recovery, and even for split mirror restore. The maximum number of snapshots that can be created for a specific source volume is limited by the HP P9000 XP Disk Array Family model and its installed firmware revision.

  For details, see the *HP Data Protector Zero Downtime Backup Concepts Guide* and the *HP Data Protector Zero Downtime Backup Administrator's Guide*. For a list of disk array models that support P9000 XP snapshots, see the latest support matrices at http://www.hp.com/support/manuals.

- Support for the user authentication mode

  (available with patch bundle set 6.21 and superseding updates)

  Newer HP P9000 XP Disk Array Family models provide increased security with authorization verification, which is implemented using a special operating mode called user authentication mode. When a command device is operating in this mode, applications must supply user credentials of an appropriate disk array user account when invoking disk array commands through it. The HP StorageWorks P9000 XP Agent of Data Protector 6.20 has been extended to support the user authentication mode. Whenever needed, it supplies the involved command device with preconfigured user credentials from the ZDB database (XPDB). For the purpose of adding and managing stored user credentials, new options have been added to the `omnidbxp` command.

For details, see the *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Command Line Interface Reference*.

This Data Protector enhancement requires an HP P9000 XP Disk Array Family configuration that uses a specific RAID Manager Library version. For the version number and additional information, see the latest support matrices at http://www.hp.com/support/manuals.

Additional zero downtime backup options

Data Protector 6.20 introduces new zero downtime backup options that can be selected in the Data Protector GUI when configuring a ZDB backup specification for the **HP P6000 EVA Disk Array Family** or the **HP P9000 XP Disk Array Family**. These options provide:

- Better control over mount points to which storage volumes are mounted on the backup system

  You can control the composition of paths to the mount points on the backup system for each ZDB backup specification separately, and can choose how name of the application system and the ZDB backup session ID are considered for the composition.

- Increased resilience by automatically dismounting storage volumes from target mount points on the backup system

  If used, this functionality helps in avoiding ZDB session failures in circumstances when arbitrary storage volumes are mounted to target mount points on the backup system before a ZDB session is started.

For a list, descriptions, and default values of the new options, see the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

Enhanced disaster recovery and support for disaster recovery on new platforms

Disaster recovery support for Linux

Data Protector 6.20 introduces support for Enhanced Automated Disaster Recovery (EADR) and One Button Disaster Recovery (OBDR) for Linux. With EADR or OBDR, Cell Managers and clients can be recovered in an automated way.

For disaster recovery specifics applicable to Linux, see the *HP Data Protector Disaster Recovery Guide*. For details on the supported hardware platforms see the latest support matrices at http://www.hp.com/support/manuals.

Disaster recovery support for Windows 7 and Windows Server 2008 R2

Data Protector 6.20 introduces support for Enhanced Automated Disaster Recovery and One Button Disaster Recovery for Windows 7 and Windows Server 2008 R2. This includes support for new Windows 7 and Windows Server 2008 functionality such as hidden boot volumes, new VSS writers, Microsoft Hyper-V volumes, and Cluster Shared Volumes.

For disaster recovery specifics applicable to Microsoft Windows 7 and Windows Server 2008 R2, see the *HP Data Protector Disaster Recovery Guide*. For details on the supported hardware platforms see the latest support matrices at http://www.hp.com/support/manuals.

Recovery to dissimilar hardware

Data Protector 6.20 introduces the ability to perform Enhanced Automated Disaster Recovery to dissimilar hardware, that is, hardware that is partially or completely different from the original. This is only available for Windows-based systems; full details of supported operating systems and limitations of the process are given in the *HP Data Protector Disaster Recovery Guide*.

HP Data Protector Disaster Recovery GUI

(available with patch bundle set 6.21 and superseding updates)

A new HP Data Protector Disaster Recovery GUI is available on Windows Vista, Windows 7, and Windows 2008 Server systems. This GUI contains wizards for unlocking volumes encrypted using BitLocker Drive Encryption, restoring dissimilar hardware, and mapping network adapters. It replaces the old console GUI and improves the product usability.

Disaster recovery enhancements

Data Protector 6.20 introduces the following enhancements:

- Support for booting the DR OS from USB drives.

  This functionality is available on Windows 7 and Windows Server 2008 R2 systems (all supported platforms) and on Windows Server 2008 systems (Itanium).
- Support for booting the DR OS over a network.

  (available with patch bundle set 6.21 and superseding updates)

  Creating a network bootable image and booting the target system over a network is supported on Windows Vista, Windows 7, and Windows Server 2008.
- Support for VSS disk image backup.

  (available with patch bundle set 6.21 and superseding updates)

  VSS disk image backup of the logical volumes can be used for disaster recovery on Windows Vista, Windows 7, and Windows Sever 2008 systems.
- Automatic detection of changed SCSI addresses of local devices during disaster recovery.
- Improved network configuration during disaster recovery where it is possible to switch between a DHCP based or original (static) network configuration.
- Preparation of DR ISO images for client systems that are not present in the current Data Protector cell.

For details, see the *HP Data Protector Disaster Recovery Guide*.

Enhanced communication protocol

Support for Internet Protocol version 6 (IPv6)

Data Protector 6.20 introduces support for Internet Protocol version 6 (IPv6) which has the following advantages over IPv4:

- Increased addressing capacity that overcomes IPv4 address exhaustion problem
- Efficient and hierarchical addressing and routing infrastructure
- Flexible built-in security
- Better support for traffic prioritization
- Extensibility and dynamic reconfigurability

Data Protector 6.20 is able to use both protocols transparently: IPv6 is used where available and IPv4 as a fallback.

When running in an IPv6 environment, the Cell Manager must be configured in a dual-stack mode, thus having both IPv6 as well as IPv4 enabled. The Cell Manager's IPv4 address is used for licensing purposes.

Secure control communication

Data Protector 6.20 enhances the existing encrypting functionality by introducing encrypted control communication, which is based on Secure Socket Layer (SSL), between the Cell Manager and the clients in a Data Protector cell.

The functionality is part of any Starter Pack and does not require an additional license for software based encryption.

Enabling encrypted control communication between Data Protector processes increases security in the cell and helps preventing unauthorized access to your system.

Support for new platforms

Microsoft Windows Server 2008 R2

Data Protector 6.20 introduces support for the Windows Server 2008 R2 operating system for 64-bit processor architectures. The following Data Protector functional areas are available for this platform: Cell Manager, Installation Server, original GUI and Java GUI, Disk Agent, general Media Agent, automigration to VLS devices, automatic disaster recovery, integrations with HP P6000 EVA Disk Array Family and HP P9000 XP Disk Array Family, the majority of application integrations, and commands of the Data Protector CLI that belong to these areas.

In a Microsoft Cluster Server environment, the Cell Manager can be installed in a cluster-aware mode.

On this platform, Data Protector 6.20 handles symbolic links in the same way as NTFS reparse point. Within the Disk Agent functionality, backup of the CONFIGURATION objects is performed using Volume Shadow Copy Service.

For details, see the latest support matrices at http://www.hp.com/support/manuals.

NOTE:

In the Data Protector 6.20 documentation set, all information specific to Windows Server 2008 also applies to Windows Server 2008 R2, except if explicitly stated otherwise. This may, however, not hold for all troubleshooting entries and problem descriptions with workarounds.

Microsoft Windows 7

Data Protector 6.20 introduces support for the Windows 7 operating system for 32-bit and 64-bit processor architectures. The following Data Protector functional areas are for this platform: original GUI and Java GUI, Disk Agent, general Media Agent, automigration to VLS devices, automatic disaster recovery, and commands of the Data Protector CLI that belong to these areas.

On this platform, Data Protector 6.20 handles symbolic links in the same way as NTFS reparse point. Within the Disk Agent functionality, backup of the CONFIGURATION objects is performed using Volume Shadow Copy Service.

For details, see the latest support matrices at http://www.hp.com/support/manuals.

Apple Mac OS X

Data Protector 6.20 introduces support for the Disk Agent (DA) component on Intel (32-bit and 64-bit) platform. For details, see the latest support matrices at http://www.hp.com/support/manuals.

With this support, you can back up and restore data on Mac OS X.

For limitations, see "Mac OS X limitations" (page 35).

Additional changes and improvements

Microsoft SQL Server integration enhancements

(available with patch bundle set 6.21 and superseding updates)

Data Protector 6.20 introduces the following enhancements in the Microsoft SQL Server integration:

- Tail log backup

  Tail log backup is a transaction log backup that creates backup image of the tail of the Microsoft SQL Server database log just before the data is restored. You can enable it by selecting the **Enable tail log backup** restore option. The backup session is invoked by starting the restore, and enables you to restore the database to the state it was in at the moment of the disaster, in the same restore session.

- Log shipping-aware backup

  Log shipping is a Microsoft SQL Server feature which enables synchronization of one or more secondary databases with a primary database. To preserve consistency of secondary databases, transaction logs of the primary database must not be truncated during backup. For this reason, Data Protector preforms a differential database backup instead of a transaction log backup when it detects a log shipping configuration, and notifies the user about it.

- A dialog box for setting the Data Protector Microsoft SQL Server-related environment variables from the Data Protector GUI

  The feature which has been introduced for some other Data Protector integrations is now available also for the Data Protector Microsoft SQL Server integration. The environment variables set from the Data Protector GUI are SQL Server instance-specific and override the options that may be set in the `omnirc` file.

The new functionality is accessible only by using the original Data Protector GUI. It does not support zero downtime backup (ZDB) and instant recovery (IR).

For details, see the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*. For limitations, see “Microsoft SQL Server limitations” (page 45).

Enhanced NDMP integration

Data Protector 6.20 introduces the following enhancements for the NDMP Server integration:

- Dynamic assignment of backup objects to backup devices
- Direct Access Restore for Directories (DDAR) on EMC Celerra NDMP server
- Support for new backup types: NVB backup for EMC Celerra and SnapMirror to Tape (SMTape) for NetApp
- Avoid loading all the media during NDMP restore
- Restore of data to an alternate NDMP Server
- Extended list of supported NDMP devices
- Media copying support for NetApp

  (available with patch bundle set 6.21 and superseding updates)

For details, see the *HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*.

For limitations, see “NDMP limitations” (page 42).

Licensing changes and enhancements

Data Protector 6.20 introduces the following licensing changes and enhancements:

- Advanced backup to disk license checking enhancements

  The Advanced backup to disk extension license-to-use is required to back up to a Data Protector file library and to a Data Protector StoreOnce library, and can be used instead of drive licenses to back up to a Virtual Tape Library (VTL). The changes in the VTL settings and license checker improvements enable you to more precisely check and track the Advanced backup to disk license usage.

- On-line extension licensing in virtual environments

  In addition to on-line backup of databases and application integrations, Data Protector 6.20 On-line extension license-to-use covers also backup in virtual environments, such as Microsoft Hyper-V environment, VMware Virtual Infrastructure, and backup with Microsoft Volume Shadow Copy Integration.

- Consolidated reporting of zero downtime backup (ZDB) and instant recovery (IR) licenses

  Disk array specific zero downtime backup licenses and instant recovery licenses from previous Data Protector releases are reported as generic, disk array independent ZDB and IR licenses.

- Migration of old licenses

  Licenses from previous Data Protector releases, such as multi-drive server licenses, old on-line licenses, direct backup using NDMP licenses, and slot libraries licenses are automatically migrated to Data Protector 6.20.

For details, see the *HP Data Protector Installation and Licensing Guide*, chapter *Data Protector licensing*.

Installation improvements

Data Protector 6.20 introduces the following enhancements to the Data Protector installation process:

- Improved installation package structure and size on UNIX, which results in
  - faster installation on Linux systems
  - reduced disk space requirements for the UNIX Installation Server
  - the possibility to install UNIX clients from the Solaris and Linux installation DVD-ROM
- Ability to use passive nodes of MC/ServiceGuard server cluster as Installation Servers.
- Better error handling during remote installation to Linux systems and improved response in case of installation failures.
- Reduced complexity and increased speed of patching Data Protector installations.

Data Protector localization to Simplified Chinese

Data Protector 6.20 introduces support for Simplified Chinese as part of the default installation, without the need for installing additional patches. This includes the localized original GUI (on Windows systems), Java GUI (on Windows and UNIX systems), CLI messages and notifications (on Windows, HP-UX, and Solaris systems), online Help (including context sensitive (F1) Help), and a limited set of guides.

Documentation enhancements

The documentation for Data Protector 6.20 has been restructured and the following integration guides were introduced:

- *HP Data Protector Integration Guide for Virtualization Environments*

  The new guide describes how to integrate Data Protector and virtualization environments: VMware Virtual Infrastructure and VMware vSphere, Microsoft Hyper-V, and Citrix XenServer. The guide also replaces the *VMware Virtual Infrastructure* chapter from the *HP Data Protector Integration Guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*.

- *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

  The new guide replaces the former *Volume Shadow Copy Service* chapters in the *HP Data Protector Integration Guide for Microsoft Applications* and in the *HP Data Protector Zero Downtime Backup Integration Guide*. It describes how to use the Data Protector Volume Shadow Copy Service integration to back up and restore application data.

For a complete list of guides, see "Data Protector documentation" (page 98).

Support for NetApp SnapManager for Microsoft Exchange and NetApp SnapManager for Microsoft SQL

Data Protector 6.20 introduces support for NetApp SnapManager for Microsoft Exchange (SME) and NetApp SnapManager for Microsoft SQL Server (SMSQL) through the Data Protector NetApp SnapManager backup solution. When used together with standard Data Protector functionality, the solution enables you to back up and restore NetApp SnapManager snapshots of Microsoft Exchange Server and Microsoft SQL Server data.

For details, see the NetApp SnapManager appendix in the *HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*.

Support for the GDS2 filesystem on Linux platform

Data Protector 6.20 adds support for the GFS2 filesystem on Red Hat Enterprise Linux 5.3 for the x86-64 processor architecture with Red Hat Cluster Suite.

Conventional incremental backup with Change Log Provider

Data Protector 6.20 enables you to use the `Use native Filesystem Change Log Provider if available` option with the conventional incremental backup to improve detection of the modified files and to avoid a file tree walk.

Enhanced Windows disk image backup and restore

Disk image backup of logical volumes on Windows clients does not lock the volumes. Applications can continue using this volume when the backup operation is in progress.

Disk image restore can be performed even if a file or disk section is in use by an application.

New enhanced incremental backup database

New enhanced incremental backup database is introduced on Windows, HP-UX, and Linux systems. It occupies much less disk space and only one file per mount point.

Simplified debug log collection

The Data Protector 6.20 GUI was enhanced to enable collection of debug logs from the client systems, which was in previous releases of Data Protector possible only on the Cell Manager using the CLI. The new functionality is available only for the original Data Protector GUI.

For details, see the *HP Data Protector Troubleshooting Guide*.

Minor enhancement of the Informix Server integration

(available with patch bundle set 6.21 and superseding updates)

The Data Protector Informix Server integration introduces support for the critical files (CF) resource type, this enables Data Protector to back up, restore, and recover critical files.

Lotus Notes/Domino Server integration support on Linux platform

(available with patch bundle set 6.21 and superseding updates)

With Data Protector 6.20, the Data Protector Lotus Integration is supported also on Linux platform besides Windows, Solaris, and AIX platforms. It provides support for backing up and restoring the Lotus Notes and Lotus Domino Server data on the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems.

For details, see the latest support matrices at http://www.hp.com/support/manuals.

3 Limitations and recommendations

Limitations

Size limitations

Internal database size

	Data Protector 6.20
Number of filenames[1]	48 GB or approximately 1050 million (UNIX systems) or 675 million (Windows systems)
Number of file versions	10 x number of filenames
Maximum number of DCBF directories[2]	50 (default: 10)
Maximum size per DCBF directory[3]	2047 TB (file system limitations and/or settings may prevail over this limit)
Maximum size per DCBF file	limited by the file system settings
Maximum number of files per DCBF directory	10000
Low space (minimum difference to the maximum size of the DC directory)	2 GB
Maximum number of concurrent drives (DLT7000 and lower performing)	100
Maximum number of concurrent physical drives (DLT8000/SDLT/LTO)	50
Maximum number of concurrent virtual drives (LTO, where a drive concurrency is set to 1)	100

[1] The maximum size of the filename database is 48 GB for the Cell Manager. The number of filenames is an estimate for an average Data Protector environment.

[2] DCBF = Detail Catalog Binary Files

[3] In the GUI you are allowed to set it up to 32768 MB (32 GB) (default: 16 GB).

Number of media

There can be up to 40000 media in one pool.

In total, there can be 500000 media in the Data Protector media management database.

Size of file depots used for file library

It is recommended that you use the default file depot size (5 GB). Note that increasing this value can cause some performance degradation. The maximum supported file depot size is 2 TB.

Number of sessions in the database

There can be up to 1000000 sessions in the database. At the most, 9999 backup sessions can be run in one day.

Number of backups scheduled at one time

The maximum total number of backup sessions running in parallel is 100 on UNIX systems and 60 on Windows systems. The default value is set to 5. This can be increased by reconfiguring the `MaxBSessions` global option. When the number of parallel sessions is larger than 50 (recommended maximum) the probability of hitting one of the system limits on the Cell Manager increases significantly (number of file descriptors, TCP/IP limitations, memory limitations).

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:
  - On HPUX systems: 5 million files
  - On Linux (32-bit) systems: 5 million files
  - On Windows (32-bit): 10 million files

Concurrent activities

- Each backup session can by default use up to 32 devices at the same time. The upper limit for this parameter is controlled by the `MaxMAperSM` global option (it's default value is 32).
- By default, up to 32 Disk Agents (depending on the concurrency of a device) can write to the same device at the same time. This number can be controlled using the `MaxDAperMA` global option.
- Up to 10 media can be imported in the IDB at the same time.

Number of cells in a MoM environment

There can be up to 50 cells in a MoM environment.

Installation limitations

Data Protector cannot be installed if the installation path contains non-ASCII characters.

Upgrade limitations

- A backup of the Internal Database, created with previous versions of Data Protector, cannot be restored with Data Protector A.06.10. After upgrading the Cell Manager, backup the Internal Database before you continue using Data Protector.
- Encrypted backups created with Data Protector A.06.00 cannot be used to create an EADR/OBDR ISO image with Data Protector 6.20. You must perform a new full client backup with Data Protector 6.20 after the upgrade.
- If you are upgrading to Data Protector 6.20 on Windows, HP-UX, and Linux systems, the enhanced incremental backup database cannot be migrated to the new version. The old enhanced incremental backup repository is deleted from the *`Data_Protector_home`*`\enhincrdb\`*`mount_point`* directory. During the first full backup after the client upgrade, a new repository is created at the same location. Notice, that the first backup after the upgrade should be full, otherwise incremental backups will fail with a warning message.
- If you want to use the object consolidation functionality after upgrading to Data Protector 6.20, you must run full backups for all backup specifications that were backed up by using enhanced incremental backup.

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.

Localization limitations

- Data Protector 6.20 is localized to the Japanese and French languages on Windows, HP-UX, Solaris, and Linux operating systems. However, the installation procedure is not localized.
- The Japanese localized version is supported on Microsoft Windows with Japanese language support. International versions of Microsoft Windows are not supported.
- The French localized version is supported on Microsoft Windows with French language support. International versions of Microsoft Windows are 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.
- The maximum size of files and disk images you can back up depends on operating system and filesystem limitations. Data Protector has no file size limitations on the following operating systems: HP-UX, Solaris, AIX, IRIX, Linux, Tru64. On other UNIX systems, Data Protector backs up files and disk images of up to 2 GB.
- 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 64000 items (files in one directory, slots in a library, and so on) in a tree view.
- File names containing quotation marks are not supported.
- To view online Help, you need to have a Web browser installed. You also have to set the Help Mode to default HTML browser in the **Preferences** options from the **File** menu in the GUI.

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.
- Data Protector 6.20 does not support backup and restore of access control lists (ACLs) on Veritas Cluster File System (CFS).
- 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=0` in the global options file. 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.

Tru64 limitations

- Raw device backup is not supported.
- Backup and restore of sockets and FIFOs are not supported.

SCO limitations

- The `Restore Sparse Files` option, which can be selected when setting options for the Restore Session, is not supported.
- The Internet Protocol version 6 (IPv6) is not supported on SCO OpenServer.
- Encrypted control communication is not supported on SCO OpenServer.

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).

Windows limitations

- Windows directory share information can only be restored to a Windows system with a Data Protector 6.20 Disk Agent or newer. 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.
- Microsoft Installer (MSI) 2.0 is required to install Data Protector 6.20. If an older MSI version is installed on the target system, the Data Protector setup will automatically upgrade it to version 2.0. In this case, Data Protector will display a note at the end of the upgrade, stating that MSI was upgraded. It is highly recommended to restart the system, if MSI was upgraded. This applies to remote installation procedure as well (the MSI on the client will be updated and it is recommended to restart the client system).
- Remote installation using secure shell (SSH) is not supported on Windows platforms.
- 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 can display a maximum 64000 items (files in one directory, slots in a library, and so on) in a tree view.
- When installing Data Protector on Windows, you cannot run multiple instances of the `setup.exe` program.
- 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 *HP Data Protector Installation and Licensing 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 Vista, Windows 7, and Windows Server 2008 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 Vista, Windows 7, and Windows Server 2008 systems, 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 Vista, Windows 7, and Windows Sever 2008 systems.
- You can boot the target system over the network only on Windows Vista, Windows 7, and Windows 2008 Server systems.

- The HP Data Protector Disaster Recovery GUI is available only on Windows Vista, Windows 7, and Windows 2008 Server systems. On other Windows systems, a console interface is available.
- On Windows XP Professional systems with only Service Pack 1 installed, the Internet Protocol version 6 (IPv6) is not supported.
- 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 Product Demo for Windows is not supported on 64-bit versions of Windows.
- The glossary is not available in online Help on 64-bit versions of Windows.
- The original Microsoft Windows installation CD-ROM is supported for Automated System Recovery (ASR). The *Windows XP 64-bit Edition Recovery DVD* that comes with Itanium systems cannot be used for 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 6.20 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 XP and Windows Server 2003 limitations

In order to perform Data Protector remote installation if any of the clients are running Windows XP or Windows Server 2003, the Installation Server and the clients must have IPv4 protocol enabled.

Although both systems natively support IPv6, there is a limitation:

- The Windows Remote Procedure Call (RPC) provider does not provide IPv6 support on these systems. As a consequence, accessing remote network shares on systems using IPv6-only configuration may not be possible.

  Network shares are used by Data Protector remote installation in order to install the initial services when performing a clean client installation, as well as accessing the installation depot from the client.

Novell Open Enterprise Server (OES) limitations

- Data Protector 6.20 cannot back up or restore any GroupWise system files.

  When a cross-file system restore is attempted from a Novell Storage Services (NSS) volume to a native Linux volume, the NSS file system specific attributes are lost while the data remains intact.
- Data Protector enhanced incremental backup cannot be used for backing up data that resides on NSS file systems.

- Software data compression is not supported for NSS volumes. Even if the backup option `Software compression` is selected, it has no effect on the data backed up from such volumes.
- The Internet Protocol version 6 (IPv6) is not supported for OES cluster configurations.

Novell NetWare limitations

- The Novell NetWare client must be installed locally on the Novell NetWare system. There is no support for remote installation from an Installation Server.
- Data Protector can restore Novell NetWare files to Novell OES and the other way round, these are the only cross-system restore scenarios supported.
- Software data compression is not supported. Even if the backup option `Software compression` is selected, it has no effect on the data backed up from Novell NetWare systems.
- The restore option `Omit deleted files` is not supported.
- The Internet Protocol version 6 (IPv6) is not supported.
- Encrypted control communication is not supported on Novell NetWare 6.5.
- Enhanced incremental backup is not supported.

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.

- Rawdisk 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.
- Maximum block size for Media Agent on OpenVMS is 63.5 kB. If a device/drive is configured with a bigger block size, it will be changed to 63.5 kB.
- Data Protector file library is not supported on OpenVMS ODS-2 disks.
- All tape media initialized by the Media Agent starts with an ANSI VOL1 label having a non-blank Volume Accessibility character. To mount such a tape volume on OpenVMS, use the `/OVERRIDE=ACCESSIBILITY` qualifier. However, the tape volume does not comply with ANSI tape labeling and can therefore not be used with OpenVMS utilities like DCL-COPY.
- 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 run with the `-session` parameter does not collect the debug files produced during specified session, because session names are not part of the OpenVMS debug filename. 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 disk array integrations

HP 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 http://www.hp.com/support/manuals.
- 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 some 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 HP 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 *HP 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 HP P6000 EVA Disk Array Family storage system. The actual limitation is determined by the storage system's firmware revision. For details, see the HP 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 if your HP P6000 EVA Disk Array Family environment supports multisnapping using vsnaps, see your HP 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 HP technical support.

HP P9000 XP Disk Array Family limitations

- Asynchronous HP 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 http://www.hp.com/support/manuals.
- With the single-host (BC1) configuration, only filesystem and disk image backup is 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 HP Business Copy P9000 XP configuration. Database (application) split-mirror restore is not supported.
- Instant recovery is only available in HP 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 HP 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 *HP 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 HP 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 HP P9000 XP Disk Array Family documentation.

HP P4000 SAN Solutions limitations

- Backup preview is not supported.
- Object copying and object mirroring are not supported for ZDB to disk.
- In a Microsoft server cluster environment, all volumes which are selected for zero downtime backup session must belong to the same cluster.
- 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, which must be used for configuring access to the CIMOM provider of the HP P4000 SAN Solutions, is available only on Windows systems.

EMC Symmetrix disk array limitations

- ZDB to disk, ZDB to disk+tape, and instant recovery are not supported. Only ZDB to tape is supported.
- 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.

NDMP limitations

- Only filesystem backup and restore are available.
- The NDMP integration can handle backup sessions involving up to 20 million files if up to 10% of the total number of backed up files are directories, for an average directory name length of 25 characters, and average filename length of 10 characters. In such a case, the NDMP integration allocates up to 1.9 GB of system memory and 2.8 GB of disk space.

  For optimal performance the recommended number of files and directories for an NDMP backup specification is 10 million. The default upper limit for the number of files for an NDMP backup specification is 5 million. To enable higher values, the `OB2NDMPMEMONLY` omnirc file variable must be set to `0`.
- 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.
- Object copying and object mirroring are not supported for NDMP backup sessions.
- Medium header sanity check is not supported on NDMP clients.
- Restore of data residing on more than one medium using the `List from Media` option is not supported. To perform such a restore, you should first import all related media.
- 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, and the device must be 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.
- Data Protector does not support IPv6 for NDMP backup sessions, therefore the NDMP servers should have IPv4 protocol enabled.

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.
- 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.

VLS automigration limitations

- Smart copies can only be made between slots and copy slots of the same VTL, not to other (virtual) tape libraries. This limitation does not apply to remote copies to other VLS that are transparent to Data Protector (when they appear as physical libraries attached to the VLS).
- Direct access to the media in the physical libraries is not possible. This means that the restore from such media is not possible as long as the media are not moved to drives controlled by Data Protector.
- The VLS filters out slots containing cleaning tapes. Data Protector is not aware of them and is not able to trigger the clean process.
- No more than one physical drive can currently be used per VLS.

Limitations on enhanced incremental backups

Limitations on enhanced incremental backups using Change Log Provider:

- Backup of FAT16 and FAT32 filesystems is not supported.
- Data Protector does not have private access to the Change Journal meaning that other applications might turn it off while Data Protector is using it.

Limitations on the enhanced incremental database:

- 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 on HP-UX, Windows, and Linux systems.

Limitations on application integrations

For additional integration specific limitations not included in this section, see the *HP Data Protector Integration Guide* and *HP 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. The backup seems to be completed without any problems reported, but restore from the session is not possible.
- 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 its default value: home directory of the ASM instance, the authentication mode used by the Data Protector Oracle integration agent to connect to the ASM instance.

SAP R/3 limitations

- If ZDB to tape is used to back up a tablespace in a ZDB environment on Windows, and the `ZDB_ORA_INCLUDE_CF_OLF` `omnirc` variable 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.

Informix Server limitations

- On Windows, 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.
- Running Microsoft SQL Server restore sessions that involve tail log backup and setting of Data Protector Microsoft SQL Server-related environment variables are not available in the Java GUI.

Microsoft SharePoint Server limitations

- The functionality supporting the Data Protector Microsoft SharePoint Server 2007/2010 integration is not available in the Java GUI.

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.

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 Exchange Server 2007

- The functionality supporting the Data Protector Microsoft Volume Shadow Copy Service integration with Microsoft Exchange Server 2007 is not available in the Data Protector Java GUI.

Microsoft Virtual Server 2005

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

Microsoft Hyper-V limitations

- The functionality supporting the Data Protector Virtual Environment integration is not available in the Java GUI.

VMware limitations

Data Protector Virtual Environment integration limitations

- When restoring a virtual machine to a non-original datastore whose block size is not compatible with the virtual machine disks' sizes (that is, a .vmdk file size is not a multiple of the datastore block size), the restore fails.
- The functionality supporting the Data Protector Virtual Environment integration is not available in the Java GUI.

Non-Data Protector limitations:

- *Non-alphanumeric characters:* Data Protector cannot back up virtual machines if the datastore names contain some non-alphanumeric characters (for example, @; only letters, numbers, single quotes, spaces, and hyphens are allowed). This is due to a Virtual Disk Development Kit limitation. For details, see:

  http://www.vmware.com/support/developer/vddk/VDDK-1.2.1-Relnotes.html

Data Protector VMware (Legacy) integration limitations

- *Datacenter path:* In VirtualCenter environments, the length of datacenter paths should not exceed 79 characters. For example, the path `/Mydatacenters/Datacenter1` is acceptable because it consists of only 27 characters.

  In standalone ESX Server environments, datacenter paths cannot exceed 79 characters because they are always `/ha-datacenter`.
- *Virtual machine path:* The virtual machine path should not contain embedded double quotes. You cannot open a backup specification that references such virtual machines.
- *Data Protector graphical user interface:* The functionality supporting the Data Protector VMware (Legacy) integration is not available in the Data Protector Java GUI.
- *Backup methods:*
  - Normally, Data Protector aborts incremental and differential **Snapshot** sessions if they are started after a non-Data Protector snapshot has been created. However, if you start an incremental or differential backup session while the creation of a non-Data Protector snapshot is still in progress, Data Protector does not abort the session nor does it report any errors. Nevertheless, such a backup is corrupted.
  - The **VCBimage** and **VCBfile** backup methods are supported only for virtual machines that reside on SAN datastores.
- *Folder attributes:* When restoring a folder partially (that is, you exclude some files from the folder from restore), attributes of the folder and attributes of all parent folders up to the root folder are not restored.

  For example, suppose you backed up the folder `C:\tmp\MyFolder` that contained two files `MyFile1.txt` and `MyFile2.txt`. If you restore the folder `C:\tmp\MyFolder` and exclude the file `MyFile2.txt` from restore, attributes of the folders `C:\tmp` and `C:\tmp\MyFolder` are not restored.
- *Reparse points:* Backup of reparse point directories is not supported. This means that the content of such a directory is not backed up during a **VCBfile** backup session. However, note that this does not affect the backup of other files.
- *File library:* If you create a file library on the backup proxy system while virtual machine disks are mounted to the backup proxy system, Data Protector offers the virtual machine disks as a possible storage location for the file library. However, this location should be ignored.

Non-Data Protector limitations:

- *Non-ASCII-7 characters:* VirtualCenter 2.0.x does not support non-ASCII-7 characters. If paths to virtual machine files contain non-ASCII-7 characters, the VirtualCenter Server terminates abnormally.

  There are two different workarounds:

  - Ensure that paths to virtual machine files (for example, `/vmfs/volumes/storage2/helios/helios_1.vmdk`) contain only ASCII-7 characters. For example, create virtual machines using only ASCII-7 characters and then rename them using non-ASCII-7 characters. In such cases, paths to virtual machine files remain unchanged (they still contain only ASCII-7 characters).
  - If paths to virtual machine files contain non-ASCII-7 characters, do not connect to the VirtualCenter Server. Instead, manage such virtual machines by connecting to ESX Server systems (`/ha-datacenter`) directly. This workaround cannot be used for the **VCBfile** backup method.

  Regardless of the workaround you select, for the **VCBfile** and **VCBimage** backup methods, you also need to install the corresponding language on the backup proxy system (**Control Panel > Regional and Language Options > Languages**) and set this language for non–Unicode programs (**Control Panel > Regional and Language Options > Advanced**).

Lotus limitations

- On Solaris and AIX systems, offline restore and restore with recover are not supported for Lotus Notes/Domino Server 7.0. and newer versions.

Limitations on clusters

MC/ServiceGuard limitations

- When adding components on MC/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 MoM environment

Debug log collection is not supported in MOM environments.

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 object verification functionality with the Java GUI is not supported.
- The use of Web Reporting with object verification is not supported.
- Only Novell NetWare backup objects can be verified on a Novell Netware target host.

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 encryption

Limitations on data encryption

- Consolidation of objects backed up with software encryption is not supported.
- The display of encryption details for encrypted objects and the media containing them is not supported with the Data Protector Java GUI.

Limitations on encrypted control communication

- Communication between the client, which is using plain control communication and the client with enabled encrypted control communication is not supported. This means, that Data Protector operations will not be executed (for example, remote installation from an Installation Server, which is using plain control communication to the client with enabled encrypted control communication will not succeed).

  However, the Cell Manager can communicate with both types of clients in the Data Protector cell.
- End user authentication is not supported.
- To satisfy U.S. Export Regulations, encrypted control communication uses only export ciphers. Key lengths are limited to 64 bits for symmetric and 512 bits for asymmetric encryption. These regulations are enforced on a code level.

Limitations on licensing

Upgrade limitations

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 after the upgrade to Data Protector 6.20 by default set to 1 TB. 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 *HP Data Protector Installation and Licensing Guide*, and the `omniupload` man page or the *HP Data Protector Command Line Interface Reference*.

Internet Protocol version 6 (IPv6) networking limitation

Data Protector licensing (the IP-based licenses, time-limited or permanent, IP- or subnet-bound, except Instant-on licenses and Emergency Passwords) requires that the Cell Manager must have an IPv4 address. When running in an IPv6 environment, the Cell Manager must be configured in a dual-stack mode, thus having both IPv6 as well as IPv4 enabled. The Cell Manager's IPv4 address is used for licensing purposes.

Limitation on license reporting

- In a cell with Data Protector 6.20 Cell Manager and a client that is not upgraded to Data Protector 6.20, 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.

Device and media limitations

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

  The device filters are defined by the `OB2DEVICEFILTER` `omnirc` variable. For details, see the `omnirc.tmpl` template.

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

  For details on setting `omnirc` variables and `global` options, see the online Help.

Reporting limitations

- Information about physical devices, which is shown in the Device Flow report if the `RptDisplayPhysicalPath` global variable 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 (multi-cell) 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.

User interface limitations

Data Protector Java GUI limitations

- The functionality supporting the following Data Protector integrations is not available in the Java GUI:
  - Virtual Environment integration
  - Microsoft SharePoint Server 2007/2010 integration
  - Microsoft Volume Shadow Copy Service integration with Microsoft Exchange Server 2007
  - VMware (Legacy) integration
- The Java GUI cannot connect to the IPv6-only Cell Managers, therefore the Cell Managers must be configured in a dual-stack mode, thus having both IPv6 as well as IPv4 enabled.
- The Java GUI does not support creation of a bootable USB drive with a DR OS image.
- Using the Java GUI, it is not possible to determine which backup objects are encrypted, to determine which backup media contain encrypted objects, or to obtain encryption details for those objects.
- The use of Data Protector object verification functionality with the Java GUI is not supported.

- On Windows systems, you can create batch files that can be used to run backup sessions for selected backup specification without using the Data Protector GUI at a later time. In contrast to the original Data Protector GUI, the Java GUI does not create shortcuts to such batch files.
- The Java GUI does not support logging of user-triggered events to the Data Protector event log.
- With the Java GUI, the Help Navigator contents do not change automatically, which means that you have to refresh them by pressing `F1` or clicking the question mark icon.
- The Java GUI does not support VSS disk image backup of the logical volumes on Windows Vista, Windows 7, and Windows Sever 2008 systems.
- You cannot create a network bootable image to be able to boot the target system over the network by using the Java GUI.
- The Java GUI does not support running Microsoft SQL Server restore sessions that involve tail log backup and setting of Data Protector Microsoft SQL Server-related environment variables.

Other limitations

- Dynamic disks are not supported.
- 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 2003 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.
- 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 a Cell Manager to DA clients must respond within 10 seconds or the backup 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 or/and 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 online 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, 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 currently not supported if the Media Agent runs on: SCO, Novell NetWare, Linux, AIX.
- 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 path of DR image file is limited to 250 characters, if it is saved on the Cell Manager during backup.
- When recreating volumes during the Phase 1 of automated disaster recovery (EADR or OBDR), the original volume-compression flag is not restored (always saved to non-compressed).

  Workaround: Restore the volume compression flag manually after restore.
- 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**.
- The HP AutoPass utility is not supported on Windows Server 2003 (64–bit), Windows Vista (64–bit), Windows 7 (64–bit), Windows Server 2008 (64–bit), Solaris, and Linux operating systems.
- The `omniinstlic` command, used to administer the HP AutoPass utility, operates only if Java Runtime Environment (JRE) 1.5.0_06 or higher is installed on the Cell Manager.
- 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.
- Disaster recovery functionality in both, the original Data Protector GUI and Data Protector Java GUI is supported only if the platform on which the GUI component is used and the platform of the system which will be recovered are the same. This means, for example, that you cannot use the GUI running on a UNIX system to perform a Windows EADR backup. Additionally, OBDR functionality is available only locally on the system to which the OBDR device is connected.
- If Boot Configuration Data (BCD) is located on removable storage like floppy disk, flash card, CD-ROM or DVD-ROM, Data Protector cannot back up BCD registry entries.
- The Change Log Provider cannot be used with Hierarchical Storage Management (HSM) solutions.
- The maximum size the MS 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 Java GUI and the Data Protector command-line interface (CLI) do not support logging of user-triggered events to the Data Protector event log.
- For Data Protector integration objects, the following actions cannot be restricted by using the `user_restrictions` file:
  - Start backup
  - Start backup specification
  - Start restore

Recommendations

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). A MoM can manage up to 50 Data Protector cells. A cell can contain up to 1000 clients. An environment structured in such a way allows you to manage up to 50000 clients from a central location. However, for better efficiency, it is recommended to have up to a few hundred clients in one cell. For example, if you manage only 100 clients in each cell, you can still centrally manage up to 5000 clients. Furthermore, multiple MoM cells can be centrally managed using the HP Operations Center. Such a setup would allow 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.

The maximum number of clients that you can still efficiently manage within one Data Protector cell depends on the following factors:

- Data Protector Internal Database (IDB) load: filesystem log level, types of objects backed up (disk image, application database, other object types), zero downtime backup sessions, NDMP backup sessions, and so on.
- Network traffic and system load: local versus network backup, level of concurrent backup and other activities, network traffic and system load unrelated to Data Protector.
- Maintenance tasks: user management, configuration of backup specifications, upgrading, patching.

Large number of small files

Backup of a client with a large number (higher than 100000) of small files puts a high load on system resources. If such a system needs to be backed up, the following steps (in the suggested sequence) can be performed to improve the situation:

1. Avoid any other activity on the system where the Media Agent runs during backup.
2. Change the log level option for such filesystems to directory. This way, individual filenames and file versions will not increase the size of the database.
3. Consider disk image backup.
4. Increase the system resources (memory, CPU) on the system where the Media Agent runs first and then on the Cell Manager system.

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.

Enhanced incremental backup

To enable that Data Protector Disk Agent accesses more memory if needed for enhanced incremental backup on HP-UX, set the tunable kernel parameter `maxdsiz` as follows:

- On HPUX 11.11:

  ```
  kmtune set maxdsiz=2147483648
  kmtune set maxdsiz_64bit=2147483648
  ```

- On HPUX 11.23/11.31:

  ```
  kctune set maxdsiz=2147483648
  kctune set maxdsiz_64bit=2147483648
  ```

NDMP backup configuration

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.

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.

Microsoft Exchange single mailbox backup

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

Large file support

It is recommended that the file system where DC directories reside supports files larger than 2 GB, especially if drives with large capacity, for example LTO 4, are used, and more than 10 million files are backed up on tape. In addition, on Windows systems it is strongly recommended to use NTFS files.

Volume Shadow Copy Service recommendations

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 2003 systems (100 MB if the hotfix KB826936 is not installed) and 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 *HP 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, it is recommended that you periodically perform registry management tasks with Microsoft Registry Management Tool.

Allocation policy for DCBF directories

It is recommended to change the allocation policy for DCBF directories from “fill in sequence” (the default) to “balance size”.

Windows Server 2008 recommendations

- **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 6.20 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.

UNIX recommendations

When performing a disk image (rawdisk) backup, it is recommended to unmount disk partitions before the backup and mount it back later.

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

- On Solaris systems, installation DVD-ROM cannot be ejected after installing the Cell Manager.

  Workaround: Stop and start Data Protector services:

  ```
  /opt/omni/sbin/omnisv stop
  /opt/omni/sbin/omnisv start
  ```

- 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.

  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`*`\db40\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.

- If the cluster client is configured under several virtual hostnames, then Data Protector Cell Manager will only update configuration information for cluster virtual node.

  Workaround: This has no effect on the actual state of the Data Protector client - only configuration data is not upgraded. To finish the upgrade, log on to the Cell Manager system and run the command `omnicc -update_host` *`virtual-name`* for every virtual name (other than cluster name).

- 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 *HP Data Protector Installation and Licensing Guide*.

- 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.

- 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 previous version of Data Protector before installing Data Protector 6.20.

- With Data Protector A.06.00 on HP-UX 11.23 and HP-UX 11.31 (Itanium) and SUSE Linux Enterprise Server (x86-64) systems, the maximum size of database files can exceed the preconfigured maximum size of 2 GB. Consequently, during an upgrade from Data Protector A.06.00 to Data Protector 6.20, a warning message is displayed advising to adjust the maximum size of database files.

This adjustment should be done after the upgrade, as it may take a significant amount of time, depending on the database size. Until the adjustment is performed, Data Protector 6.20 will report incorrect tablespace sizes as is the case with A.06.00. However, it is still possible to perform backup and restore.

For a details on how to adjust the file sizes, see the *HP Data Protector Installation and Licensing Guide*, chapter *Troubleshooting*.

- 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.

- In a MC/ServiceGuard cluster for HP-UX PA-RISC, 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.

  If the cluster fails over, the check on the now active node succeeds.

- 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 *HP Data Protector Installation and Licensing Guide*.

- 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.

- HP Autopass installation on HP-UX 11.11 from DVD fails if the DVD is mounted with default mount options, using `pfs_mount`.

  Workaround: To mount the DVD, use the `mount` command with the following options:

  ```
  mount -F cdfs -o ro,rr,noauto device_name mount_directory
  ```

  For example:

  ```
  mount -F cdfs -o ro,rr,noauto /dev/cdrom /cdrom
  ```

  To unmount the DVD, use:

  ```
  umount mount_directory
  ```

- On HP-UX systems, after upgrading a Data Protector A.06.00, A.06.10, or A.06.11 Cell Manager to Data Protector 6.20, the Instant-On passwords (licenses) will expire. Permanent passwords (licenses) are not affected. The issue does not appear with a new installation.
- After updating the Data Protector Virtual Environment integration component with patch bundle set 6.21, passwords of all virtual environment hosts will no longer work. To solve this, run the following command:

  ```
  vepa_util.exe --upgrade-cell_info
  ```

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.

- After installing the patch bundle set 6.21, previously configured VLS devices used for automigration will not work.

  Workaround: Update the password for the specified VLS user.

  1. In the Context List, click **Clients**.
  2. In the Scoping Pane, expand **Data Protector Cell** and then **Clients**. All clients are displayed.
  3. Right-click the client that you want to modify and click **Properties**.
  4. In the Object Properties window, click the **Storage Appliance** tab and re-enter the password for the specified user.
  5. Click **Apply** to save the changes.

User interface related issues

- When using Data Protector CLI on Windows 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 online Help index: "internationalization".

- On Windows Server 2003 systems, after saving backup specifications whose names include non-Latin characters (for example, Russian or Greek), names of the backup specifications may appear corrupted in the Data Protector GUI.

  Workaround: Install Windows Server 2003 Service Pack 2 on the system where Data Protector GUI is installed.

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

  Workaround: None.

Disk Agent related issues

- 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 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/`*`computer.company.com`*`/BC/fs/LVM/VXFS` it actually displays the corresponding application source mount point `/BC/fs/LVM/VXFS`.
- 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@host1.test.com "host2.test.com [/H]" Time:
  27/09/10 16:58:40 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.

- When trying to back up directory structure with more than 100 directories (on HP-UX 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@computer.company.com "C:" Time: 8/31/2010 11:04:52
  AM
  ```

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

- When backing up mount point on Windows, if a subdirectory is deselected and therefore excluded from backup, the whole mount point might be backed up nevertheless.
- When trying to expand the empty Windows mount point in tree view, the following error is reported:

  ```
  Cannot read directory contents.
  ```

- When a restore of the configuration on a Novell NetWare platform is attempted, the `TSA.nlm` module might report an error similar to the following:

  ```
  [Minor] From: HPVRDA@host "CONFIGURATION:" Time: xx/xx/xxxx
  xx:xx:xxTSA: Error (TSAFS.NLM 6.50 272) The program was processing
  a record or sub record and did not find the Trailer field.
  ```

- 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.
- When backing up Macintosh files on a Windows system, 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.

- Data backed up from a shared network folder using Data Protector Disk Agent installed on a Windows Vista, Windows 7, or Windows Server 2008 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.

- On Windows Server 2008 systems, backup of the CONFIGURATION object made with Data Protector A.06.00 cannot be restored with Data Protector A.06.11. Restore of the Active Directory to the default location fails.

  Workaround: Use the **Restore As/Into** option in the GUI and enter the path `c:\windows\ntds` or the location where Active Directory is installed. This should be done in Directory Services Restore Mode so that the files can be restored to the Active Directory location.

- On HP-UX systems, when performing a disk image (rawdisk) 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.

Media Agent related issues

- 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` variable `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.

- Detection of the WORM tape is supported on Windows platforms only. On other platforms Data Protector does not recognize the tape as not rewritable and treats it as any other tape. When an attempt to overwrite data on a WORM medium fails, the medium is marked as poor.

  Workaround: Set the backup protection for WORM media to Permanent. Keep WORM media and rewritable media in separate media pools.

- 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` variables on the affected Media Agent system: `OB2MAREADRETRY`, `OB2MAXREADRETRIES`, `OB2MAREADRETRYDELAY`, `OB2MAWRITERETRY`, `OB2MAXWRITERETRIES`, and `OB2MAWRITERETRYDELAY`.

- In previous Data Protector releases the `devbra` command on Linux and Solaris systems reported rewind on close device files (`/dev/st*` on Linux and `/dev/rmt/*mb` on Solaris) during the configuration instead of no rewind on close devices (`/dev/nst*` on Linux and `/dev/rmt/*mbn` on Solaris). Thus, the devices were configured as rewind on close devices. As a result, Data Protector can overwrite the media headers and renders the backup unusable. The problem occurs in SAN environments, for example if the path (rewind on close) of one device points to another device that is currently in use on another host.

  Workaround: Ensure that there are no rewind on close devices configured. Review your device configuration on Linux and Solaris systems and reconfigure all rewind on close devices as no rewind on close devices.

  During an upgrade, the rewind on close devices are not upgraded automatically, instead a warning is displayed with an advice to reconfigure the devices. Reconfigure devices manually before you perform the next backup.

- 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.
- 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.
- 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.
- 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.
- 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.

- Data Protector UNIX Restore Session Manager sometimes fails to start restore Media Agents in parallel on Novell NetWare clients with an error message like, for example, `Could not connect to inet` or `Connection reset by peer`. It is possible that some parallel restore sessions are completed without errors, while other restore sessions are not even started.

  Workaround: Set the `SmMaxAgentStartupRetries` variable in the Data Protector global options file (located in `/etc/opt/omni/server/options/global`) to `2` or more (max. 50). This variable specifies the maximum number of retries for the session manager to restart the failed agent before it fails. For more information on the Data Protector global options file, see the online Help index: "global options file".

- After upgrading to Data Protector 6.20, you cannot use devices that were configured as different device types in previous releases. For example, you cannot use 9940 devices that were configured as 9840 devices, 3592 devices that were configured as 3590 devices or SuperDLT devices that were configured as DLT devices. The following error is reported:

  ```
  [Critical] From: BMA@ukulele.company.com "SDLT" Time: 2/22/2011
  5:12:34 PM [90:43] /dev/rmt/1m Invalid physical device type =>
  aborting
  ```

  Workaround: Manually reconfigure these devices using the `mchange` command, located on the Cell Manager in the following directory:

  Windows: `Data_Protector_home\bin\utilns\NT`

  HP-UX: `/opt/omni/sbin/utilns/HPUX`

  Solaris: `/opt/omni/sbin/utilns/SOL`

  Linux: `/opt/omni/sbin/utilns/LINUX`

  The syntax of the `mchange` command is: `mchange -pool` *`PoolName`* `-newtype` *`NewMediaClass`* where *`PoolName`* is the name of the media pool with devices that are currently configured and should be reconfigured (such as Default DLT or Default T9840), and *`NewMediaClass`* is the new media type of the devices (for example, T9940 for 9940 devices, T3592 for 3592 devices, and SuperDLT for SuperDLT devices).

  This command changes media types for all media, drives and libraries that use the defined media pool. After you have executed this command for each device you changed, move the media associated with the reconfigured devices from the current media pool to the media pool corresponding to these media. For example, move the media associated with the reconfigured 9940 devices to the Default T9940 media pool, media associated with the reconfigured 3592 devices to the Default T3590 media pool, and the media associated with the reconfigured SuperDLT devices to the Default SuperDLT media pool. For related procedures, see the online Help.

- When restoring data using List From Media functionality, the session may fail with the following message:

  ```
  [Critical] From: MSM@computer.company.com "FUYL" Time: 13.8.10
  11:29:16 Failed to allocate memory. [Normal] From:
  MMA@computer.company.com "FUYL" Time: 13.8.10 11:29:16 ABORTED Media
  Agent "FUYL"
  ```

  Backups with a large number of files require a large amount of memory when List From Media functionality is used.

  Workaround: Import the medium to add detailed information about backed up data on the medium into the IDB and then browse it for a restore.

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

- When utilizing autoloader devices, messages from the `HPUMA.nlm` module might be unreadable. For example:

  ```
  [Normal] From: HPBMA@host "device name" Time: xx/xx/xxxx xx:xx:xx
  ?T?y??K?
  ```

- 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.

- For copying older application objects (backed up with a pre-A.05.50 version of Data Protector), one of the following conditions must be fulfilled:
  - Object copy with the target MA running on the same platform where the original backup was made must be performed.
  - Object copy must be performed and at least one copy or the original in the IDB (with permanent catalog protection) must always be retained.
- An object copy session containing numerous objects (more than 200) or complex object media relations (see below) may become unresponsive.

  Workarounds:

  - 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.

- 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).

Integration related issues

Common issues

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

  Workaround: None.

Microsoft Exchange Server

- 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.

- By default, Data Protector does not support restoring data to Recovery Storage Group of Exchange Server 2003. If you enable Recovery Storage Group, the restore will fail if database selected for the restore operation is not present in the Recovery Storage Group.

  Workaround: Remove the recovery storage group or set the `Recovery Storage Group Override` registry key. For details, see the Microsoft web page http://support.microsoft.com/kb/824126.

Microsoft Exchange Single Mailbox

- 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

- 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.

Microsoft Volume Shadow Copy Service

- 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 in this case), they are not shown in the restore page.

  Workaround: None. Only the **Restore components** mode is available in such cases.

- The VSS integration agent (VSSBAR agent) does not print application pre- and post-exec options output in the session log when called by the Virtual Environment integration agent for Microsoft Hyper-V.

SAP R/3

- 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`*.

- 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.

  Workaround: None.

Oracle

- 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.
- The `ZDB_ORA_INCLUDE_CF_OLF`, `ZDB_ORA_INCLUDE_SPF`, and `ZDB_ORA_NO_CHECKCONF_IR` `omnirc` variables 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.

- 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 will fail.

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

- With Oracle 11.2.0.2 or subsequent versions in an RAC environment, a Data Protector managed backup control file 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 to `/var/opt/omni/tmp` (UNIX systems) or `Data_Protector_home\tmp` (Windows systems) directory.

  Workaround: With Oracle 11.2.0.2 or subsequent versions in a RAC environment, this destination must be located on a shared disk, accessible from all the nodes. To avoid this issue, specify a destination directory by setting the `OB2_DPMCTL_SHRLOC` environment variable for the control file copy.

VMware (Legacy)

- 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) can 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:
   1. Go to the folder `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\Logs`
   2. Find the log file `vpxd-xx.log` (where *xx* is the latest number).
   3. Open the log file and look for the following two lines:

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

      ```
      "Max buffered response size is 104857600bytes"
      ```

NDMP

- On 64-bit Windows Server 2003 systems, a backup may fail with the following error message:

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

  Workaround: None. The issue will be solved in a subsequent patch release.

Disk array integrations

- 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` variable in the *HP Data Protector Zero Downtime Backup Administrator's Guide*.

- 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.

- 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.

  Workaround: None.

Granular Recovery Extension issues

VMware vSphere

- When requesting a restore using the Data Protector Granular Recovery Extension for VMware vSphere, backup sessions of a datacenter that resides inside a folder in the VMware inventory hierarchy (such as `/folder1/subfolder2/`*`Datacenter`*) are not listed in the **Backup start time** drop-down list.

  Workarounds:

  - Ensure that datacenters are not inside folders.
  - If you cannot change the inventory hierarchy, select **All Datacenters** from the **Datacenter** drop-down list when creating a Virtual Environment backup specification.

Disaster recovery issues

- An encrypted IDB backup (a prerequisite for Cell Manager disaster recovery) will fail unless an active encryption key was created prior to the backup.

  Workaround: Create an active encryption key prior to performing an encrypted IDB backup. For details, see the `omnikeytool` man page or the *HP Data Protector Command Line Interface Reference*.

- On Windows Server 2003 systems, when performing EADR on a ProLiant BL460c system, the DR OS cannot find the network card and a restore cannot be started.

  Workaround:

  Enable the safe boot mode:

  - Edit the `drm.cfg` file *before* creating the ISO image:
    1. Open the file `drm.cfg.tmpl` in `\\OmniBack\bin\drim\config`
    2. Edit the variable `safe_boot`:

       ```
       safe_boot = normal
       ```

    3. Save the file `drm.cfg.tmpl` and rename it to `drm.cfg`.
    4. Create the ISO image.

    The disaster recovery process should now start normally.

  - Or, if you are already performing disaster recovery, edit the `boot.ini` file and restart the system.
    1. Once the DR OS boots and Disaster Recovery Wizard starts, abort the countdown.
    2. Start a command prompt and launch Notepad.
    3. Open the file `C:\boot.ini` and search for the string `/SAFEBOOT:NETWORK`.
    4. Remove the string from the `boot.ini` file and save it.
    5. Reboot the computer and leave boot sequence to start from the disk (do not boot from CD-ROM again).
    6. When the system logs on, proceed with the standard disaster recovery procedure.

- 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.

Cluster-related issues

Common issues

- 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.

- 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.

- 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 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 a cluster 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 MC/ServiceGuard

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

  ```
  [Critical] From: SSEA@wartburg.company.com"" Time: 11/8/2010 11:43:09
  AM

  Data consistency check failed!
  ```

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

Two workarounds are possible:

- 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.

- If you export a physical node from an MC/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: Run the command `/opt/omni/sbin/install/omniforsg.ksh -primary -upgrade`.

Issues in Microsoft Cluster Server

- 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.
- 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.

Networking and communication related issues

- 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. It is not advisable to remove this existing path since some applications may rely on it.

- 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@company.com.
  ```

  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@company.com
     ```

  3. Reconfigure the user impersonation for the specified client using the `omniinetpasswd` command:

     ```
     omniinetpasswd -add myuser@company.com
     ```

For details of the `omniinetpasswd` command, see the *HP Data Protector Command Line Interface Reference*.

Other known issues

- 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**.

- 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 variable `ConsolidationAutomatedMaxObjects`.

- 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.

- 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, it is suggested to split the consolidation of multiple objects into more than one session.

- 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**.

- The following applications are not recommended to be installed together with Data Protector on the same system:

  - WebQoS.
  - CyberSitter 2000
  - NEC E-border AUTOSOCKS

  Coexistence of Data Protector Media Agent and HP OpenView Storage Allocater may cause unexpected results. For most recent patch information, see the HP web page http://www.itrc.hp.com.

- 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, run the command `fuser -kc /oracle/P01`.

- 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.

- 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.

- 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.

- On HP OpenVMS, a restore session may become ceaseless 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.

- 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.

- 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 run the `omnisv -start` command.

- 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.
- If more than one `omnidbutil -purge -filenames` session is started, `omnidbutil` reports that it cannot communicate with the Cell Manager.

  Workaround: None. To avoid running into such situation, do not start more than one session.

- 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, run:

    `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.

- 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.

Known non-Data Protector issues and workarounds

Non-Data Protector issues related to installation or upgrade

- On Windows systems, after an installation or upgrade to Data Protector 6.20, the operating system may report that an application is not installed or that its reinstallation is required. The reason is an error in the Microsoft Installer upgrade procedure.

  Workaround: For a solution, see the Microsoft web page http://support.microsoft.com/kb/324906.

- 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.

- On Windows XP systems, an additional dialog box may pop up during uninstallation of the CORE patch.

  Workaround: For a possible resolution, see the InstallShield support web page http://support.installshield.com/kb/view.asp?articleid=Q107094.

- 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.

  Workarounds:

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

- On Windows XP and Windows Server 2003 systems, the installation fails if the installation destination directory is a virtual drive, created for example with the `subst` command. The following error message is displayed:

  ```
  Error: 1320. The specified Path is too long.
  ```

  The Windows Installer service is running under a different user account than the `subst` command. As a result, the installation fails.

  Workarounds:

  - Use the UNC path specification (for example `\\computer.company.com\shared_folder`) instead of the virtual drive. This is the preferred solution.
  - Run the `subst` command under the Local System user account.

- 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

- 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.

- On UNIX systems, when viewing the Data Protector online Help in Mozilla Firefox 2.0, pop-up windows with the glossary and options topics may display significantly slower than expected.

  Workaround: If available for your particular operating system, upgrade Mozilla Firefox to the version 3.0 or newer.

Non-Data Protector issues related to Disk Agent

- If the LSI Logic 53C1010-66 card is used on an HP Server rx2600 Itanium 2 client with Windows Server 2003 Enterprise Edition, restore may fail with an internal error.
- 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.

  Workaround: None.

- On Windows systems, after backing up a volume containing long filenames with associated 8.3 short filenames, the short filenames previously associated with the long filenames may not be retained after a restore. This problem occurs due to a Windows limitation described on the Microsoft web page http://support.microsoft.com/kb/176014. It may cause certain applications to fail if specific 8.3 short filenames are incorrectly associated with long filename files. The problem most likely affects Microsoft SQL Server users because Microsoft SQL Server keeps paths to its databases stored in the 8.3 short filename notation.

  Workaround: After restoring the directory containing the files that are not correctly associated with the 8.3 short filenames, move those files temporarily to another directory and then move them back to the original directory in exactly the same order as they were initially created. This way, the same 8.3 short filenames will be assigned to those filenames as before the restore.

- 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`.
- On Solaris 9 systems, filesystem backup may fail with error messages similar to the following:

  ```
  Cannot open attribute directory /BC/fs/VxVM/UFS/Test6.doc: read-only
  filesystem! Extended attributes not backed up.
  ```

  Workaround: Set the `omnirc` variable `OB2SOL9EXTATTR` to `0` to disable the backup of extended attributes.

- On Novell NetWare systems, due to a known issue in the `TSAFS.NLM` module, the following error is reported during the restore with the `Trustee only restore` option enabled:

  ```
  The program was processing a record or subrecord and did not find
  the Trailer field.
  ```

  The restore is performed successfully and the error message can be ignored.

  Workaround: For potential solution, check the available patches for Novell NetWare.

Non-Data Protector issues related to Media Agent

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

  ```
  [Major] From: MMA@lada.com "MO-lada" Time: 5/6/2010 3:52:37 PM
  [90:90] /dev/rdsk/c2t0d1 Cannot erase disk surface ([22] Invalid
  argument) => aborting
  ```

- 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 variables 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
- Data Protector Media Agent cannot coexist with CA ArcServe installed on the same Windows client system. Such setup may lead to a data loss.
- When a DLT8000 (DLT 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@hkgbkup3 "HKGBKUP3_1m" Time: 10/31/10 19:52:35
  [90:182] Cannot forward segment. ([5] I/O error)
  [Major] From: MMA@hkgbkup3 "HKGBKUP3_1m" Time: 10/31/10 19:52:35
  [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 HP 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.

- On AIX 5.2 systems, the `devbra` utility cannot retrieve serial numbers of the devices connected through the CAMBEX driver. As a consequence, device autoconfiguration and automatic discovery of changed SCSI addresses do not function properly.

  Workaround: Configure the devices manually. Do not use automatic discovery of changed SCSI addresses for such devices.

- When moving a physical tape from a mail slot to a smart copy slot, it does not appear in Data Protector.

  After ejecting a smart copy tape through Data Protector it visually disappears from the slot in Data Protector. However, when it is moved back into a smart copy slot using the VLS GUI, this slot still appears empty in the Data Protector GUI. There is a mismatch between what VLS shows in its own GUI and what it lists when queried through SMI-S (the management interface that Data Protector uses).

  Workaround: Restart emulations on VLS, this updates the cache behind the SMI-S interface. In the VLS GUI navigate to **System > System Maintenance**, click **Restart Emulations** and follow the instructions.

- If during a backup session that writes backup data to a tape library, a medium is unloaded from this tape drive and another medium is loaded, a Media Agent running on an AIX system may not appropriately handle the latter. As a result, the backup session fails.

  The problem occurs due to an AIX operating system limitation in shared memory allocation functionality, and is more frequent when a relatively high Disk Agent concurrency is used.

Workaround: Enable the AIX extended shared memory model by setting the `omnirc` variable `EXTSHM` to the value `ON`.

- 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.

Non-Data Protector issues related to integrations

Microsoft Exchange Server

- If a Microsoft Exchange Server backup fails with an error message like `cannot wait for synchronization event`, the reason may be that the backup was run concurrently with a filesystem defragmentation process.

  Workaround: See the Microsoft web page http://support.microsoft.com/kb/183675.

- 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 Exchange Single Mailbox

- A reconfiguration of the Data Protector Singe Mailbox integration fails with the following error: `[12:8562] The Data Protector Single Mailbox integration cannot be configured.`

  The issue appears with the Microsoft Exchange Server 2003 if the Data Protector MAPI profile cannot be deleted (for example if other processes are using the library `mapi32.dll`, possibly also from other terminal connections to the system on which the Exchange server is running).

  Workaround: Try to exit all processes that use the library `mapi32.dll` before reconfiguring the integration. If this fails, you can delete the profile `$$$Data Protector` from the registry and perform a clean configuration.

Microsoft SQL Server

- Instant recovery of Microsoft SQL Server databases fails.

  Workaround: Follow the instant recovery procedure in the *HP 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

- The following MSDE and MS SQL writer components cannot be restored while the SQL server is online: `master`, `model`, and `msdb`.
- 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 web page http://support.microsoft.com/kb/910250.
- With HP 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 HP Command View (CV) EVA to the latest version.
- With HP 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.
- With HP 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 HP MPIO DSM for HP P9000 XP Disk Array Family.

  Workaround: Ensure that you are using a supported version of HP MPIO.
- When using the HP Business Copy (BC) P9000 XP functionality of the Disk Array XP1024 or XP128 together with the P9000 XP Array VDS hardware providers, backup fails with an error, stating that there is no VDS provider installed. The issue occurs with P9000 XP Array hardware provider version 5.00.00.

  Workaround: Contact your HP support representative to request a hardware provider version that fixes the defect, “QXCR1000903367: The HWP does not work for XP1024/XP128 arrays“.
- The full path of any virtual disk in the HP 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.
- 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.
- 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@tpc211.company.com "MSVSSW" Time:
  11.01.2011 10:17:31 Failed to break Shadow Copy Set of session
  '2011/01/11-4:tpc211'.

  [Warning] From: OB2BAR_VSSBAR@tpc211.company.com "MSVSSW" Time:
  11.01.2011 10:17:31 [145:714] Rescanning system due to Break Shadow
  Copy Set failure.

  [Minor] From: OB2BAR_VSSBAR@tpc211.company.com "MSVSSW" Time:
  11.01.2011 10:17:40 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.

- 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 in future, remove the VDS hardware provider. Note that there are use cases which require the VDS hardware provider to be installed. For details, see the *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*.

- If two command devices are configured for a disk array of the HP 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 HP StorageWorks P9000 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 *HP Data Protector Command Line Interface Reference* or the `omnidbxp` man page.

  - Disable the user authentication mode on the command device.

  - Prevent the HP StorageWorks P9000 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` variable to `1`.
      2. Remove the data belonging to the command device from the XPDB using the `omnidbxp -cm -remove` command.

Microsoft SharePoint Server

- 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

- 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 errors if filenames contain spaces.

  Workaround:

  - On Windows systems:
    1. **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. **2.** Restart the database.
  - On HP-UX and Linux systems:
    1. **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. **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).

- On SUSE Linux Enterprise Server 10 x86-64 systems with SAP MaxDB 7.6 installed, you cannot back up SAP MaxDB data with more than 19 streams. If you set the **Parallelism** option to a higher value, the session fails.

  Workaround: Contact SAP MaxDB support.

Oracle Server

- 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 HP 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 instance and execute a backup session.

- 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
  ```

  The processing of each message may take up to 20 seconds. This considerably slows down backups of databases with a large number of datafiles (200 or more).

Sybase Server

- 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

- The Data Protector integration with HP 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 it is strongly recommended 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 HP support.

- 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 HP web page http://www.itrc.hp.com.

- When using the Secure Path 4.0C driver, unrecoverable error occurs occasionally on the backup system.
- 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:

  1. 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` variable `SMISA_FORCE_DISMOUNT` (in the case of the Data Protector HP StorageWorks P6000 EVA SMI-S Agent) or `SSEA_FORCE_DISMOUNT` (in the case of Data Protector HP StorageWorks P9000 XP Agent) to `1`.
  2. Restart the session that failed.

- In circumstances when several ZDB sessions that involve the P6000 EVA 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 the HP Customer Support Service or the Microsoft Support directly.

- On Windows Server 2008 R2 systems, when using the Data Protector Microsoft Volume Shadow Copy Service integration or the Data Protector HP StorageWorks P6000 EVA 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. HP is collaborating with external partners to find a solution.

  - 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.

- On SUSE Linux Enterprise Server 10.3 and 11.1 and on Oracle Enterprise Linux 5.3, after multiple simultaneous zero downtime backup sessions that involve a P6000 EVA Array and the same backup system have been running continuously for a longer period, the virtual disks of the disk array are unexpectedly unpresented from the backup system. Additionally, creation of the virtual disk device files on the backup system fails sporadically, even after a user-triggered disk rescan is complete.

  Workaround: Restart the backup system, and rerun the problematic zero downtime backup sessions.

- If two command devices are configured for a disk array of the HP 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 HP StorageWorks P9000 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 *HP Data Protector Command Line Interface Reference* or the `omnidbxp` man page.

  - Disable the user authentication mode on the command device.

  - Prevent the HP StorageWorks P9000 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` variable to `1`.
      2. Remove the data belonging to the command device from the XPDB using the `omnidbxp -cm -remove` command.

Non-Data Protector issues related to disaster recovery

- 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

- 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 web page http://support.microsoft.com/kb/265293.

- If a Data Protector Cell 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.

- 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.

- When viewing web reports using Netscape Navigator, after resizing the browser window the applet does not automatically adjust its size appropriately.

  Workaround: Start the Netscape Navigator manually, resize the window to the desired size and only then open the `WebReporting.html` file.

- 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.

- 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.

- 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.
- 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)**.
- 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 non-Data Protector issues

- 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.
- 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.

  On HP-UX

  Set the `OB2SHMEM_IPCGLOBAL` variable to 1 in the file `/opt/omni/.omnirc`.

  On Solaris

  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.

On SCO UnixWare

Increase the value of the SHMMAX kernel variable using the scoadmin command. The minimum value required by Data Protector can be calculated using the following equation:

```
minimum value for SHMMAX = (Disk Agent buffers * Block size in kB
* 1024) + 16
```

You can get the values of Disk Agent buffers and Block size from the Advanced Options dialog box for the target backup device. It is recommended to set a higher value for SHMMAX.

- If an IRIX 6.5 disk is connected to the second SCSI controller, there might be a problem detecting if the disk is mounted.

  Workaround: Before you perform disk image (rawdisk) restore, ensure that the disk is not mounted.

- 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.

- 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.

- When creating a file system backup for a Windows Vista, Windows 7, or Windows Server 2008 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.

- When creating a file system backup for a Windows Vista, Windows 7, or Windows Server 2008 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.

- If a FAT32 boot partition exists on a Windows XP or Windows Server 2003 system, you cannot use a Windows Vista client for creating an ISO image for this system, since the resulting CD-ROM cannot be used to start the system.

  Workaround: Use the Windows XP or Windows Server 2003 system to create the ISO image.

- 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.

- 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.

5 Installation requirements

This chapter gives a description of Cell Manager, Installation Server, and client installation requirements. It also provides a list of upgrade requirements.

General installation requirements:

- Free TCP/IP port: 5555 by default
- Have the port number 5556 free to install the Java GUI Server or the Java GUI Client.
- The TCP/IP protocol must be installed and running. The protocol must be able to resolve all hostnames in the Data Protector cell.

Cell Manager requirements

The Data Protector Cell Manager does not support the IDB on a filesystem that is mounted as NFS type.

On systems running HP-UX

The Cell Manager must meet the following minimum requirements:

- The Soft File Limit per Process on the Cell Manager should be at least 1024.
- 256 MB of RAM (512 MB recommended)

  For each parallel backup session 40 MB of RAM are required and 5–8 MB per data segment size. This means that, for example, if you want to run 60 parallel backup sessions 3 GB of RAM plus 512 MB for data segments are needed.
- 350–550 MB of disk space + approximately up to 2% of planned data to be backed up (for use by the IDB).
- It is recommended to modify the kernel parameters as follows:
  - set `maxdsiz` (Max Data Segment Size) or `maxdsiz_64` (for 64–bit systems) to at least 134217728 bytes (128 MB).
  - set `semmnu` (Number of Semaphore Undo Structures) to at least 256.

  After committing these changes, recompile the kernel and restart the system.
- The `inetd` daemon must be installed and running.

For the Java GUI Client requirements, see “Java GUI Client requirements” (page 90).

For HP-UX 11.11, the IPv6NCF11i bundle or TOUR/IPv6 support is required to enable the Internet Protocol version 6 (IPv6). For details, see “HP-UX system patches required by Data Protector” (page 93).

On systems running Solaris

The Cell Manager must meet the following minimum requirements:

- 256 MB of RAM (512 MB recommended)

  For each parallel backup session 40 MB of RAM are required and 5–8 MB per data segment size. This means that, for example, if you want to run 60 parallel backup sessions 3 GB of RAM plus 512 MB of data segments are needed.
- 350–550 MB of disk space + approximately up to 2% of planned data to be backed up (for use by the IDB)

- The following values of kernel parameters are recommended: SEMMNI (maximum number of semaphore sets in the entire system) = 100 SEMMNS (maximum semaphores on the system) = 256

  A system restart is necessary for kernel changes to take effect.

- The `inetd` daemon must be installed and running.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

On systems running Linux

The Cell Manager must meet the following minimum requirements:

- 256 MB of RAM (512 MB recommended)

  For each parallel backup session 40 MB of RAM are required and 5–8 MB per data segment size. This means that, for example, if you want to run 60 parallel backup sessions 3 GB of RAM plus 512 MB for data segments are needed.

- 350–550 MB of disk space + approximately up to 2% of planned data to be backed up (for use by the IDB).
- If the version of libstdc++ on the system is not 5 (for example libstdc++.so.6 instead of libstdc++.so.5) you need to install the compatibility package `compat-2004` or `compat-libstdc++`.
- To install the Java GUI Server on Red Hat Enterprise Linux 4.0, the `libstdc++-4.0.2-8.fc4.x86_64.rpm` package is required. If your system does not already contain a 64–bit version of `libstdc++.so.5` then you must install it with `libstdc++-3.3.3-7.x86_64.rpm`.
- To run the Java GUI Server on SUSE Linux Enterprise Server 9 (64–bit), the package `compat-libstdc++-lsb-4.0.2_20050901-0.4.x86_64.rpm` is required.
- The `inetd` or `xinetd` daemon must be installed and running.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

On systems running Windows XP

The Cell Manager must meet the following minimum requirements:

- 256 MB of RAM (512 MB recommended).

  For each parallel backup session 40 MB of RAM are required. This means that, for example, if you want to run 60 parallel backup sessions 3 GB of RAM are needed.

- On Windows XP Professional systems, Service Pack 1 must be installed.
- 190 MB of disk space + approximately up to 2% of planned data to be backed up (for use by the IDB)
- `2 x` *`size_of_the_biggest_package_to_be_installed`* `+ 5MB` of disk space needed on system drive

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

On systems running Windows Server 2003 or Windows Server 2008

The Cell Manager must meet the following minimum requirements:

- 256 MB of RAM (512 MB recommended).

  For each parallel backup session 40 MB of RAM are required. This means that, for example, if you want to run 60 parallel backup sessions 3 GB of RAM are needed.

- 190 MB of disk space + approximately up to 2% of planned data to be backed up (for use by the IDB)
- `2 × size_of_the_biggest_package_to_be_installed + 5 MB` of disk space needed on system drive
- On Windows Server 2008 systems, the firewall must be configured to additionally accept "Remote Service Administration" (NP) connections (port 445).
- On Windows Server 2008 systems, administrative privileges are required to install Data Protector 6.20.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

Operating systems supported by HP AutoPass

The following Windows operating systems are supported by HP AutoPass:

- Windows XP
- Windows Server 2003 (32-bit)
- Windows Vista (32-bit)
- Windows Server 2008 (32-bit)
- Windows 7 (32-bit)

The following HP-UX operating systems are supported by HP AutoPass:

- HP-UX 11.00, HP-UX 11.11 (PA-RISC)
- HP-UX 11.23, HP-UX 11.31 (PA-RISC, Itanium)

The following Solaris operating systems are supported by HP AutoPass:

- Solaris 8, Solaris 9, Solaris 10 (SPARC)

Linux operating systems are not supported.

Installation Server requirements

On systems running HP-UX

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 1.5 GB of disk space
- The `inetd` daemon must be installed and running.

On systems running Solaris

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 1.5 GB of disk space
- The `inetd` daemon must be installed and running.

On systems running Linux

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 1.5 MB of disk space
- The `inetd` or `xinetd` daemon must be installed and running.

On systems running Windows XP

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 1 GB of disk space
- On Windows XP Professional systems, Service Pack 1 must be installed.

On systems running Windows Server 2003 or Windows Server 2008

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 1 GB of disk space
- On Windows Server 2008 systems, administrative privileges are required to install Data Protector 6.20.
- On Windows Server 2008 systems, you must configure the user whose credentials will be used during remote installation.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

Client system requirements

On systems running UNIX

The prerequisites for remote installation of the Data Protector client are the following:

- The `inetd` or `xinetd` (on Linux) daemon must be either up and running or set up so that Data Protector is able to start it on the remote client system.
- It is recommended that the `ssh` is installed and enabled to enable secure installation of remote clients.

  If `ssh` is not installed, the `rsh/rexec` service must be enabled. For details on how to enable the services, see your operating system documentation.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

RAM and disk space requirements for the Data Protector client components on UNIX systems

The following table presents the minimum RAM and disk space requirements for different Data Protector client components on UNIX systems:

Client system component	RAM (MB)	Disk space (MB)
Java GUI	512 (1000 recommended)	40 (60 recommended)
Disk Agent	64 (recommended 128)	10
Media Agent	64 (recommended 128)	20
Integration modules	64 (recommended 128)	20
English Documentation (Guides, Help)	N/A	80

The figures indicate requirements for the components only. For example, the "disk space" figure does not include space allocation for the operating system, paging file, or other applications.

HP-UX systems

When installing or upgrading remotely, the available disk space in the folder `/tmp` should be at least of the same size as the biggest package being installed.

For HP-UX 11.11, the IPv6NCF11i bundle or TOUR/IPv6 support is required to enable the Internet Protocol version 6 (IPv6). For details, see "HP-UX system patches required by Data Protector" (page 93).

Solaris systems

When installing a Media Agent, make sure that the following entry is in the file `/etc/system`:

```
set semsys:seminfo semmni=100
```

When installing or upgrading remotely, the available disk space in folders `/tmp` and `/var/tmp` should be at least the size of the biggest package being installed.

The Solaris installation DVD-ROM is in the pkg stream format, which is not recognized by the standard tar utility. That is why the HP-UX, and not the Solaris installation DVD-ROM must be used for the local installation/upgrade of Solaris clients.

Linux systems

- The RPM module must be installed and enabled on a Linux Debian client system, as Data Protector uses the rpm package format for installing.
- On SUSE Linux Enterprise Server 10 and 11, the package `compat-libstdc++++-296-2.96-132.7.2` with 2.96-RH compatibility standard C++ libraries must be installed on the system.

Mac OS X systems

When installing remotely, a UNIX based installation server (Linux, HP-UX, or Solaris) is required for accommodating the Mac OS X remote installation packages (Core and Disk Agent).

On systems running Windows

The prerequisites for Windows user interface installation and remote installation on the client are:

- On Microsoft Windows XP Professional systems, Service Pack 1 must be installed.
- On Microsoft Windows Server 2003 systems, Service Pack 1 must be installed.

For the Java GUI Client requirements, see "Java GUI Client requirements" (page 90).

RAM and disk space requirements for the Data Protector client components on Windows systems

The following table presents the minimum RAM and disk space requirements for different Data Protector client components on Windows systems:

Client system component	RAM (MB)	Disk space (MB)
Original GUI	256[1]	150[2]
Java GUI[3]	512 (1000 recommended)	40 (60 recommended)
Disk Agent	64 (recommended 128)	10
Media Agent	64 (recommended 128)	20
Integration modules	64 (recommended 128)	20
English Documentation (Guides, Help)	N/A	85

[1] Memory requirements for the GUI system vary significantly with the number of elements that need to be displayed at a time. This consideration applies to the worst case (like expanding a single directory). You do not need to consider all directories and file names on a client, unless you want to expand all directories while viewing. It has been shown that 2 MB memory are required per 1000 elements (directories or file names) to display plus a base need for about 50 MB. So the 256 MB of RAM are enough to display about the maximum number of file names.

[2] Regarding the disk space, keep in mind that the page file alone should be able to grow to about 3 times the physical memory.

[3] In addition to RAM and disk space requirements, Java GUI requires a faster processor than original GUI: at least 1 GHz Pentium III or equivalent is required, while a 2.6 GHz Pentium IV or equivalent is recommended.

The figures indicate requirements for the components only. For example, the "disk space" figure does not include space allocation for the operating system, paging file, or other applications.

Newer Windows operating systems and service packs

Windows XP Service Pack 2, Windows Server 2003 Service Pack 1, Windows Vista, Windows 7, and Windows Server 2008 introduce an improved version of the Internet Connection Firewall (ICF), under a new name as Microsoft Firewall. The firewall is turned on by default. During the installation of a new Data Protector client using the Installation Server, the installation agent is started on the remote computer. The Installation Server then connects to this agent through the Data Protector cell port (by default 5555). However, if Microsoft Firewall is running, the connection cannot be established and the installation fails. To resolve this, perform one of the following steps:

- Configure Windows Firewall to allow connection through a specific port.
- If the `omnirc` variable `OB2FWPASSTHRU` is set on the Installation Server, the installation agent automatically registers itself with Windows Firewall and the installation continues normally.

Java GUI Client requirements

To be able to start the Java GUI Client, you must install one of the supported Java runtime environments:

Windows Server 2008 systems based on the Itanium 2 processor architecture:

- Oracle JRockit 5.0 1.5.0_06 or a newer update (for example, 1.5.0_07)

You can download Oracle JRockit at http://www.oracle.com/technetwork/java/index-jsp-141438.html.

Other operating systems:

- Java Runtime Environment (JRE) 1.5.0_06 or a newer update (for example, 1.5.0_07)
- JRE 1.6.0 or a newer update (for example, 1.6.0_01)

You can download JRE at http://www.oracle.com/technetwork/java/index-jsp-141438.html.

Java web reporting requirements

To use Data Protector Java web reporting, the following prerequisites must be fulfilled:

- a supported Web browser must be installed on the system

  The supported Web browsers are the same as for viewing the Data Protector online Help. For details, see "Requirements for viewing Data Protector documentation" (page 91).

- a supported Java runtime environment must be installed on the system and enabled in the Web browser

  The supported Java runtime environment is Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07). You can download JRE at http://www.oracle.com/technetwork/java/index-jsp-141438.html.

Novell NetWare system requirements

- Any Novell NetWare system that is part of a Data Protector cell must have TCP/IP version 3.1 or later installed.
- Novell Netware 6.5 must have the Support pack 1 or later installed.

Local client installation

UNIX clients are installed locally using the installation script `omnisetup.sh`. You can install the client locally from the UNIX installation DVD-ROM and import it to the Cell Manager using automated procedure.

For the installation procedure, see the *HP Data Protector Installation and Licensing Guide*.

Windows XP Home Edition, Novell NetWare, and HP OpenVMS clients can be installed locally. Remote installation is not supported.

Upgrade

The procedures for upgrading to Data Protector 6.20 from Data Protector A.06.00, A.06.10, and A.06.11are documented in the *HP Data Protector Installation and Licensing Guide*. To upgrade from an even earlier version, you need to first upgrade to Data Protector A.06.00, and then upgrade to Data Protector 6.20 following the procedures in the *HP Data Protector Installation and Licensing Guide*.

Requirements for viewing Data Protector documentation

To view the Data Protector guides and the Data Protector online Help, you must install a supported PDF document viewer and a supported Web browser. Below is a list of applications and versions that are supported. HP recommends to use the newest version available for your operating system:

- For viewing the guides, you need Adobe Reader 7 or newer version, or another PDF document viewer.

  You can download Adobe Reader at http://get.adobe.com/reader/ (for Windows, Solaris, and Linux systems) or ftp://ftp.adobe.com/pub/adobe/reader/unix/7x/7.0.9/enu/ (for HP-UX systems).

- For viewing the online Help, you need a Web browser that is able to run under the same account as the Data Protector GUI process. JavaScript must be enabled in the Web browser. The following Web browsers are supported:

  Windows systems: Windows Internet Explorer 7.0 or newer version

  To enable proper display of the WebHelp format of the online Help in Internet Explorer 8.0 and newer versions, you need to turn on Internet Explorer Compatibility View as follows:

  1. Open Internet Explorer and display its menu bar.
  2. In the Tools menu, click **Compatibility View Settings**.
  3. In the Compatibility View Settings dialog box, select the option **Display all websites in Compatibility View** and click **Close**.
  4. Close Internet Explorer.

  HP-UX systems: Mozilla Firefox 3.5 or newer version

  You can download it at https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJAVAFFTB.

  Solaris systems: Mozilla Firefox 2.0 or newer version

  You can download it at http://www.sunfreeware.com/mozilla.html or http://releases.mozilla.org/pub/mozilla.org/firefox/releases/ (from the `contrib` folders).

  Linux systems: Mozilla Firefox 2.0 or newer version

You can also download it at http://www.mozilla.com/en-US/firefox/all.html.

Note that with Firefox 2.0, pop-up windows with the glossary and option topics may display significantly slower than expected.

Requirements for Data Protector services on Windows Server 2003 and Windows Server 2008

Data Protector uses four services:

`Inet`	Backup client service
`CRS`	Cell Manager service
`RDS`	Cell Manager Database service
`UIProxy`	User Interface proxy service

By default, `Inet` and `RDS` services are running under the Local System account, and `CRS` and `UIProxy` services are running under the Administrator account.

You can change the account information for any of these services. However, the following are minimum requirements that must be met by the new accounts:

Service	**Resource**	**Minimum resource permission required by service**

`RDS`	*`Data_Protector_program_data`*`\db40` (Windows Server 2008)
	`Data_Protector_home``\db40`
	`HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII`
		Full access
		Read

`CRS`	*`Data_Protector_program_data`* (Windows Server 2008) *`Data_Protector_home`* `HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII`	Full access Full access
`Inet`	Backup and Restore Take Ownership	- -
`UIProxy`	- `HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII`	- Read

Files installed in the %SystemRoot%\system32 folder

The following files are placed (depending on the components selected) into *`%SystemRoot%`*`\system32` folder on Windows systems:

`BrandChgUni.dll` This is a resource library. It is used only internally; however, it also contains the path to registry settings, so it must be located in a well-known location where it can be accessed by integration libraries.

`libarm32.dll` This is a NULL shared library for ARM instrumentation. It may be replaced by third-party monitoring software.

`ob2informix.dll` This library is used to integrate with the Informix Server database.

`snmpOB2.dll` This library is used to implement system SNMP traps.

6 Required patches

For Data Protector patches, please consult http://support.hp.com for the latest information. For systems running Windows, contact the Microsoft Corporation for the latest Microsoft Windows Service Pack. For patches on systems running the HP-UX operating systems please consult http://www.itrc.hp.com for the latest information or check with the Response Center to get the current patch numbers. Install the latest patches before calling support. The patches listed can be replaced with newer patches.

We recommend that you regularly install the Extension Software Package delivered for HP-UX. This is a collection of recommended patches, some of which are listed below. Contact HP Support for the current version of the HP-UX Extension Software Package.

HP-UX system patches required by Data Protector

HP-UX 11.11

The following HP-UX 11.11 patch bundles are required by Data Protector:

Service pack	Bundle name	Description
Use latest	GOLDQPK11i	Current patch bundle for HP-UX 11.11
Use latest	HWEnable11i	Required hardware enablement patches

The following HP-UX 11.11 individual patches are required on Data Protector Cell Manager systems, but are also recommended to be installed on other Data Protector systems:

Patch name	Hardware platform	Description
PHCO_40310	s700, s800	libc cumulative patch
PHSS_41214	s700, s800	ld(1) and linker tools cumulative patch
KRNG11i	s700, s800	Strong Random Number Generator[1]

[1] Required to enable encrypted control communication.

The following HP-UX 11.11 individual patches are recommended to be installed on any Data Protector system:

Patch name	Hardware platform	Description
Use latest	s700, s800	MC/ServiceGuard patches for the version you use

The following product and HP-UX 11.11 patch must be installed on each Data Protector Disk Agent system from which data will be backed up in the AES 256-bit encrypted form:

Product number or patch name	Hardware platform	Description
KRNG11I	s700, s800	HP-UX Strong Random Number Generator
PHKL_27750	s700, s800	vpar enablement, krng enablement

Additionally, to use IPv6 on HP-UX 11.11, the following bundle and patches are required by Data Protector:

Bundle or patch name	Hardware platform	Description
IPv6NCF11i bundle or the TOUR transition patches	s700, s800	Transport Transition patch

HP-UX 11.23

The following HP-UX 11.23 patch bundles are required by Data Protector:

Service pack	Bundle name	Description
Use latest	QPK1123	Current patch bundle for HP-UX 11.23

The following HP-UX 11.23 individual patches are recommended to be installed on any Data Protector system:

Patch name	Hardware platform	Description
PHKL_32272[1]	s700, s800	Changes to fix intermittent failures in getacl/setacl.
PHSS_41178	s700, s800	linker and fdp cumulative patch

[1] This patch is required to support the access control list (ACL) functionality.

HP-UX 11.31

The following HP-UX 11.31 patch bundles are required by Data Protector:

Service pack	Bundle name	Description
Use latest	QPK1131	Current patch bundle for HP-UX 11.31

The following HP-UX 11.31 individual patches are required to be installed on any Data Protector system:

Patch name	Hardware platform	Description
PHCO_38050	IA64, PA-RISC	pthread library cumulative patch
PHKL_38055	IA64, PA-RISC	Scheduler cumulative patch
PHSS_41179	IA64, PA-RISC	linker and fdp cumulative patch

Solaris system patches required by Data Protector

Operating System Patch: Use the latest kernel patch from Sun Microsystems. Sun provides patch information at: http://sunsolve.sun.com.

In order to start the Data Protector GUI the following patches are required:

Operating system version	Patch	Description
Solaris 8	108434-13	32-bit Shared library patch for C++ for SunOS 8
Solaris 8	108773-18	IIIM and X Input & Output Method patch for SunOS 8
Solaris 8	111721-04	Math Library (libm) patch for SunOS 8

Operating system version	Patch	Description
Solaris 8	112438-03	/kernel/drv/random
Solaris 9	111711-11	Shared library for Solaris 8 and 9
Solaris 9	111712-11	Shared library for Solaris 8 and 9

Novell NetWare patches required by Data Protector

Use the latest recommended patches on Novell NetWare clients:

- the latest filesystem patch (NSS)
- TSAx.NLM patches
- the latest Support Pack

See patch information at Novell NetWare Web page: http://support.novell.com.

SUSE Linux Enterprise Server system patches required by Data Protector

Use the latest recommended system patches provided by Novell.

Red Hat Enterprise Linux system patches required by Data Protector

Use the latest recommended system patches provided by Red Hat.

Tru64 system patches required by Data Protector

To support the access control list (ACL) functionality, the following Tru64 patch is required:

- QAR 98885

7 Obsolete platforms and integrations

You can find the relevant version information regarding supported platforms in the Data Protector support matrices. Information in this chapter is provided for your convenience, but may not be exhaustive.

For the latest list of support matrices on the Web, see http://www.hp.com/support/manuals. In the Storage section, click **Storage Software** and then select your product.

Obsolete platforms

The following platforms are no longer supported in Data Protector 6.20:

- Microsoft Windows 2000
- Novell Open Enterprise Server for Linux 1.0
- Multi-Programming Executive (MPE/iX)
- Red Hat Enterprise Linux 2.1, 3.0
- United Linux 1.0
- Debian Linux 4.0
- SNI SINIX

Obsolete integrations

Integrations with the following software applications are no longer supported in Data Protector 6.20:

- Oracle 9i
- Informix IDS 9.x, 10.x
- Sybase 12.5
- Microsoft SQL Server 7
- Microsoft Exchange 2000 Server
- IBM DB2 UDB 8.x
- Lotus Domino 6.x
- SAP DB/MaxDB 7.4, 7.5
- all SAP R/3 versions except BR*Tools 7.x
- HP Performance Manager and HP Performance Agent
- HP Reporter
- HP Service Information Portal
- Symantec NetBackup Server/Enterprise Server 5.x

Integration with the following family of disk array systems is no longer supported in Data Protector 6.20, although the related functionality is still visible in the Data Protector user interfaces for compatibility reasons:

- HP Virtual Array

Integrations with the following products are no longer supported in Data Protector 6.20:

- specific models of the HP P6000 EVA Disk Array Family and specific versions of HP Command View (CV) EVA

  For a list of supported P6000 EVA Array models and CV versions, see the latest support matrices at http://www.hp.com/support/manuals.

- specific models of the HP P9000 XP Disk Array Family

  For a list of supported P9000 XP Array models, see the latest support matrices at http://www.hp.com/support/manuals.

Obsolete functionality

The following functionality is no longer supported in Data Protector 6.20, although it is still visible in the Data Protector user interfaces for compatibility reasons:

- direct backup for HP P9000 XP Disk Array Family

End-of-support plans

The following Data Protector functional areas will become no longer supported on the listed operating systems in one of the future Data Protector releases:

- Cell Manager:
  - Solaris
- client:
  - Tru64
  - Novell NetWare

8 Data Protector documentation

Documentation set

Other documents and online Help provide related information.

Guides

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

You can find these documents from the Manuals page of the HP Information Management Digital Hub website:

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

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

- *HP Data Protector Concepts Guide*

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

- *HP Data Protector Installation and Licensing Guide*

  This guide describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This guide also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.

- *HP Data Protector Troubleshooting Guide*

  This guide describes how to troubleshoot problems you may encounter when using Data Protector.

- *HP Data Protector Disaster Recovery Guide*

  This guide describes how to plan, prepare for, test, and perform a disaster recovery.

- *HP Data Protector Integration Guides*

  These guides describe how to configure and use Data Protector to back up and restore various databases and applications. They are intended for backup administrators or operators. There are six guides:

  - *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*

    This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server.

  - *HP Data Protector Integration Guide for Oracle and SAP*

    This guide describes the integrations of Data Protector with Oracle Server, SAP R/3, and SAP MaxDB.

  - *HP Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino*

    This guide describes the integrations of Data Protector with the following IBM applications: Informix Server, IBM DB2 UDB, and Lotus Notes/Domino Server.

  - *HP Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server*

    This guide describes the integrations of Data Protector with Sybase Server, HP Network Node Manager, and Network Data Management Protocol Server.

  - *HP Data Protector Integration Guide for Virtualization Environments*

    This guide describes the integrations of Data Protector with virtualization environments: VMware Virtual Infrastructure and VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.

  - *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

    This guide describes the integration of Data Protector with the Microsoft Volume Shadow Copy Service. This guide also documents application writer specifics.

- *HP Data Protector Integration Guide for HP Operations Manager for UNIX*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX.

- *HP Data Protector Integration Guide for HP Operations Manager for Windows*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager on Windows.

- *HP Data Protector Zero Downtime Backup Concepts Guide*

  This guide describes Data Protector zero downtime backup and instant recovery concepts and provides background information on how Data Protector works in a zero downtime backup environment. It is intended to be used with the task-oriented *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Zero Downtime Backup Integration Guide*.

- *HP Data Protector Zero Downtime Backup Administrator's Guide*

  This guide describes how to configure and use the integration of Data Protector with HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, HP P4000 SAN Solutions, and EMC Symmetrix Remote Data Facility and TimeFinder. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

- *HP Data Protector Zero Downtime Backup Integration Guide*

  This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle Server, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases.

- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for Microsoft SharePoint Server. The Data Protector Granular Recovery Extension is integrated into Microsoft SharePoint Server Central Administration and enables you to recover individual items. This guide is intended for Microsoft SharePoint Server administrators and Data Protector backup administrators.

- *HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for VMware vSphere. The Data Protector Granular Recovery Extension is integrated into VMware vCenter Server and enables you to recover individual items. This guide is intended for VMware vCenter Server users and Data Protector backup administrators.

- *HP Data Protector Media Operations User Guide*

  This guide provides information for network administrators responsible for maintaining and backing up systems on the tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.

- *HP Data Protector Product Announcements, Software Notes, and References*

  This guide gives a description of new features of HP Data Protector 6.20. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.

- *HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager*

  This guide fulfills a similar function for the HP Operations Manager integration.

- *HP Data Protector Media Operations Product Announcements, Software Notes, and References*

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector Command Line Interface Reference*

  This guide describes the Data Protector command-line interface, command options and their usage as well as providing some basic command-line examples.

Online Help

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

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

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

Documentation map

Abbreviations

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

Abbreviation	**Guide**
CLI	Command Line Interface Reference
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
GRE-SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	Online Help
IG-IBM	Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server
IG-O/S	Integration Guide for Oracle and SAP

Abbreviation	Guide
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server
IG-VirtEnv	Integration Guide for Virtualization Environments
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	Installation and Licensing Guide
MO GS	Media Operations Getting Started Guide
MO RN	Media Operations Product Announcements, Software Notes, and References
MO UG	Media Operations User Guide
PA	Product Announcements, Software Notes, and References
Trouble	Troubleshooting Guide
ZDB Admin	ZDB Administrator's Guide
ZDB Concept	ZDB Concepts Guide
ZDB IG	ZDB Integration Guide

Map

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

								Integration Guides								ZDB			GRE		MO			
	Help	GS	Concepts	Install	Trouble	DR	PA	MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	SPS	VMware	GS	User	PA	CLI
Backup	X	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	X	X				
Disaster recovery	X		X			**X**																		
Installation/ upgrade	X	X		**X**			X							X	X						X	X		
Instant recovery	X		X													X	**X**	X						
Licensing	X			**X**			X															**X**		
Limitations	X				X		X	X	X	X	X	X	X					X					X	
New features	X						**X**																X	
Planning strategy	X		**X**													X								
Procedures/ tasks	**X**			X	X	X		X	X	X	X	X	X	X	X		X	X	X	X		X		
Recommendations			X				X									X							X	
Requirements				X			X	X	X	X	X	X	X	X	X						X	X	X	
Restore	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	X				

Integrations

Look in these guides for details of the integrations with the following software applications:

Software application	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO User
Microsoft Exchange Server	IG-MS, ZDB IG
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Network Data Management Protocol (NDMP) Server	IG-Var
Oracle Server	IG-O/S, ZDB IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase Server	IG-Var
VMware vSphere	IG-VirtEnv, GRE-VMware

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
HP P4000 SAN Solutions	ZDB Concept, ZDB Admin, IG-VSS
HP P6000 EVA Disk Array Family	all ZDB, IG-VSS
HP P9000 XP Disk Array Family	all ZDB, IG-VSS

Localization

Data Protector is localized into French, Japanese, and Simplified Chinese.

IMPORTANT: Documentation updates, improvements, and fixes accompanying the Data Protector patch bundle set 6.21 are not localized.

The following end-user documentation items are localized into French:

- *HP Data Protector Getting Started Guide*
- *HP Data Protector Concepts Guide*
- *HP Data Protector Installation and Licensing Guide*
- *HP Data Protector Zero Downtime Backup Concepts Guide*
- *online Help*

The following end-user documentation items are localized into Japanese:

- *HP Data Protector Getting Started Guide*
- *HP Data Protector Concepts Guide*
- *HP Data Protector Disaster Recovery Guide*
- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*
- *HP Data Protector Installation and Licensing Guide*
- *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*
- *HP Data Protector Integration Guide for Oracle and SAP*
- *HP Data Protector Product Announcements, Software Notes, and References*
- *HP Data Protector Troubleshooting Guide*
- *HP Data Protector Zero Downtime Backup Concepts Guide*
- *online Help*

The following end-user documentation items are localized into Simplified Chinese:

- *HP Data Protector Getting Started Guide*
- *HP Data Protector Concepts Guide*
- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*
- *HP Data Protector Installation and Licensing Guide*
- *HP Data Protector Product Announcements, Software Notes, and References*
- *HP Data Protector Zero Downtime Backup Concepts Guide*
- *online Help*

Data Protector 6.20 errata

This section contains updates to the Data Protector documentation not included in:

- Localized versions of the documents. See “Localization specific errata” (page 103).

Localization specific errata

This section includes updates of the Data Protector 6.20 release documentation that are not included in the localized versions of the documents. Updates released in the Data Protector patch bundle set 6.21 are not listed.

Last-minute changes in the HP Data Protector Product Announcements, Software Notes, and References

The English version of the *HP Data Protector Product Announcements, Software Notes, and References* contains several last-minute changes that were not included in the localized versions of the documents.

Important updates include among others:

- updated list of required patches for HP-UX 11.11
- collected Java GUI limitations

  To provide better overview of all Java GUI-related limitations, they were collected and listed in a separate section. Additional Java GUI limitations were added.

- described Data Protector support for NetApp SnapManager

  A brief description of the Data Protector support for NetApp SnapManager was added to "Product features and benefits" (page 15).

- added descriptions of ZDB issues with P6000 EVA Array

  Descriptions of serious issues that occur when several zero downtime backup sessions involving a disk array of the HP P6000 EVA Disk Array Family are running simultaneously and continuously for a longer period were added.

- added documentation errata

Additional minor last-minute updates may be included in the version of the document that is published on the Web at http://www.hp.com/support/manuals.

Data Protector Virtual Environment integration

Due to last-minute changes in the integration interface, the related online Help topics (including F1 topics) have been updated.

Data Protector Granular Recovery Extension for Microsoft SharePoint

Additional known issues and workarounds related to the installation and removal of the extension were added to the troubleshooting chapter of the *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*.

Data Protector Granular Recovery Extension for VMware vSphere

The installation procedure for the Data Protector Granular Recovery Extension for VMware vSphere was updated in the *HP Data Protector Installation and Licensing Guide*.

Inet service user impersonation

Information about the Data Protector Inet service user impersonation was updated in the online Help and in the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*.

Additional prerequisite for the Data Protector Microsoft Exchange Single Mailbox integration

A prerequisite for enabling a backup of Microsoft Exchange Server 2007 mailboxes was added.

Preparing a Microsoft server cluster running on Windows Server 2008 for Data Protector installation

Steps 5 and 6 of the procedure documented in the *Appendix B* of the *HP Data Protector Installation and Licensing Guide* only apply to Data Protector Cell Manager installation.

Mirrorclones and the selected replica redundancy level

The redundancy level that is selected in a ZDB backup specification for target volumes residing on a disk array of the HP P6000 EVA Disk Array Family is not used for the creation of mirrorclones. The mirrorclones automatically created by Data Protector always use the storage redundancy level of the source volumes (original volumes).

Other updates in the integration guides

- Updates in the *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*:
  - A prerequisite for backup was added to the chapter "Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution".
  - Information on Microsoft FAST Search Server 2010 support was added to the to the chapter "Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution".

  - Information about the restore chain was updated in the chapter “Data Protector Microsoft Exchange Server 2010 integration”.
  - Additional known issues and workarounds were added to the troubleshooting sections of the “Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution” and ”Data Protector Microsoft SharePoint Server 2007/2010 integration” chapters.
- A prerequisite for configuration was added to the chapter “Data Protector Oracle Server integration” of the *HP Data Protector Integration Guide for Oracle and SAP*.

A List of enhancements and issues fixed in Data Protector 6.20

List of enhancements and issues fixed in Data Protector 6.20

The list of enhancements and fixed defects can be found on any Data Protector installation DVD-ROM in the `\DOCS` directory, in the file `DP62_EnhancementsResolvedDefects.pdf`.

List of defects resolved in Data Protector A.06.00, A.06.10, and A.06.11 but not resolved in Data Protector 6.20

The list of enhancements and defects which were resolved in Data Protector A.06.00, A.06.10, and A.06.11 but were not resolved in Data Protector 6.20 can be found on any Data Protector installation DVD-ROM in the `\DOCS` directory, in the file `DP62_OpenEnhancementsDefects.pdf`.