HP Data Protector A.06.10

Product announcements, software notes, and references

Part number: B6960-96040
First edition: November 2008

Legal and notice information

Printed in the US

Contents

Figures

Tables

Publication version history

Table 1 Edition history

Version	Date	Description
1.0	November 6, 2008	Initial version
1.0.1	November 21, 2008	Updated known issues and errata
1.0.2 (Web only)	December 12, 2008	Updated disaster recovery limitations and issues

About this guide

This guide provides information about:

- Product announcements
- Limitations and known issues
- Installation requirements (such as hardware, OS 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: Table 2 on page 15	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values

Convention	Element
Monospace, italic text	• Code variables • Command variables
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.

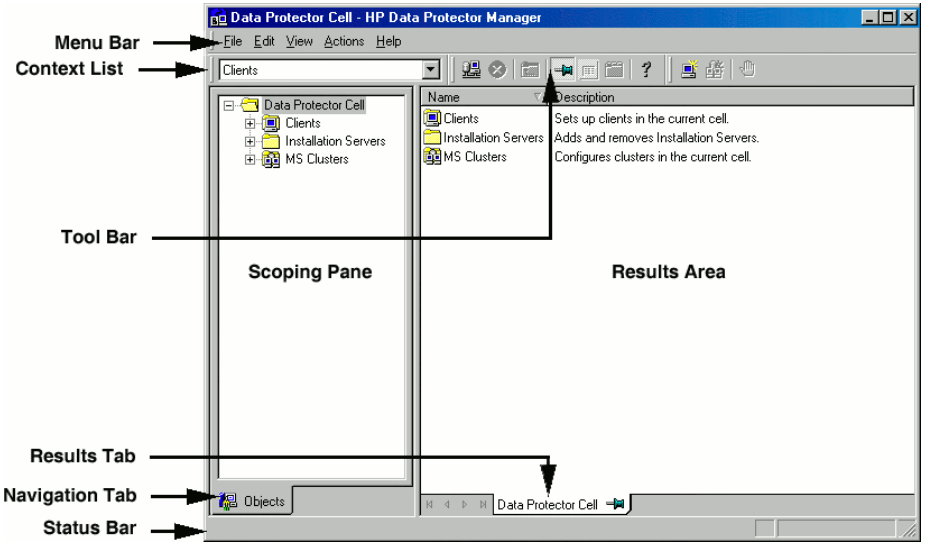

Figure 1 Data Protector graphical user interface

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/support/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 a key member of the fast-growing HP storage 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 A.06.10.

Upgrades

Upgrade information is available in the *HP Data Protector installation and licensing guide*. Procedures for upgrading from Data Protector versions A.05.10, A.05.50, and A.06.00 to Data Protector A.06.10 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 A.06.10 platform and integration support matrix*
- *HP Data Protector A.06.10 device support matrix*
- *HP Data Protector A.06.10 zero downtime (split-mirror) backup and instant recovery support matrix for HP StorageWorks Disk Array XP*
- *HP Data Protector A.06.10 zero downtime backup and instant recovery support matrix for HP StorageWorks Virtual Array*

- *HP Data Protector A.06.10 zero downtime backup and instant recovery support matrix for HP StorageWorks Enterprise Virtual Array using SMI-S Agent*
- *HP Data Protector A.06.10 EMC split-mirror backup integration support matrix*
- *HP Data Protector A.06.10 disaster recovery support matrix*
- *HP Data Protector A.06.10 VSS integration support matrix*
- *HP Data Protector A.06.10 network attached storage (NAS) support matrix*
- *HP Data Protector A.06.10 direct backup support matrix*
- *HP Data Protector A.06.10 integrations into HP software support matrix*
- *HP Data Protector A.06.10 Media Operations software support matrix*

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.

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

Supported command-line interface (CLI) commands for Data Protector are documented in the *HP Data Protector command line interface reference*.

Licensing

Data Protector A.06.10 leverages the product numbers from Data Protector A.05.10, A.05.50, A.06.00 and Application Recovery Manager A.06.00. All Data Protector A.05.10, A.05.50, A.06.00 and Application Recovery Manager A.06.00 licenses can be used with Data Protector A.06.10 and retain their original functionality. No license migration is required. 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*.

Support for old agents

Wherever possible, all clients in a Data Protector cell should be upgraded to version A.06.10 during the regular upgrade process. This ensures that customers can benefit from the full feature set of Data Protector A.06.10 on all systems in a cell.

However, due to the high demand, support for older agents has been extended. Disk agents and media agents of the same Data Protector version (A.05.10, A.05.50, and A.06.00) are supported in an A.06.10 cell with the following constraints:

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

- Operations involving clients on different systems (for example, media export and media import) have to be performed using agents of the same version.
- Older media agents are not supported in combination with NDMP servers.
- If one Data Protector component on a client is upgraded to A.06.10, all other components have to be upgraded to A.06.10 as well.
- Version A.05.10 disk agents must be upgraded to A.06.10, if you plan to back up files which contain non-ASCII characters in their file names.

If you have any problems establishing a connection with older agents, consider upgrading to A.06.10 as the first resolution step.

Updated information

For the latest information, including corrections to documentation, see the Data Protector website http://www.hp.com/go/dataprotector.

2 Product features and benefits

Below is a summary of the benefits provided by Data Protector A.06.10:

- Encryption
- Data Protector Java GUI
- Data Protector VMware Virtual Infrastructure integration
- Data Protector Microsoft SharePoint Portal Server Integration
- Data Protector backup to HP Integrated Archiving Platform (IAP)
- Support for new platforms
- Disaster recovery enhancements and support for new platforms
- Enhanced Data Protector integrations: Microsoft Volume Shadow Copy Service, Microsoft SQL Server, Oracle Server, SAP R/3, Microsoft Exchange Server, and Lotus Notes/Domino Server
- Disk Agent enhancements
- Device enhancements
- Support for Smart Media Copying Using HP StorageWorks Virtual Library System (VLS)
- Internal Database enhancements
- Improved reporting

The rest of the chapter gives a more detailed description of these Data Protector A.06.10 features and major changes in comparison to the previous Data Protector version.

Encryption

Data Protector A.06.10 enhances the existing encoding functionality by introducing the following advanced encryption techniques:

- AES 256-bit encryption

- Drive-based encryption

AES 256-bit encryption

Data Protector software encryption, referred to as AES 256-bit encryption, is based on the Advanced Encryption Standard (AES) cryptographic algorithm that uses a symmetric key for both encryption and decryption. Data is encrypted before it is transferred over the network and written to media.

You can encrypt all or selected objects in a backup specification and also combine encrypted and unencrypted sessions on the same medium.

Drive-based encryption

Data Protector drive-based encryption uses the encryption functionality of the drive. The actual implementation and encryption strength depend on the drive's firmware. Data Protector only turns on the feature and manages encryption keys. For an up-to-date list of devices that support drive-based encryption, see the support matrices in the *HP Data Protector product announcements, software notes, and references*.

Drive-based encryption can be used with backup, object consolidation, object copy, and automated media copy operations. It can be enabled at the time of each operation or centrally in the properties of the drives used for these operations.

Data Protector Java GUI

Data Protector A.06.10 introduces a Java-based graphical user interface with a client-server architecture, which enables backup management with the same look and feel as the original Data Protector GUI.

As Java can run on numerous platforms, the Data Protector Java GUI is supported on a larger number of platforms than the original Data Protector GUI. Due to the one-to-one relationship with the original Data Protector GUI, no re-learning effort is required. In addition, both user interfaces can run simultaneously on the same computer.

Benefits of Java GUI

The Data Protector Java GUI has the following advantages over the original Data Protector GUI:

- Portability

The Data Protector Java GUI architecture enables you to install Java GUI Clients on most platforms that support Java Runtime Environment (JRE).

- Easy firewall configuration

  For details, see the Data Protector support matrices under specifications at http://www.hp.com/support/manuals.

  The Java GUI Client uses port 5556 to connect to the Java GUI Server. It is easier to configure Java GUI in a firewall environment because only one port needs to be opened.

- Improved localization and internationalization

  Only one installation package is needed for all locales. The Java GUI enables better display in all locales, since controls are automatically resized to match the size of the text.

- Non-blocking behavior

  The Java GUI Server transmits only data for the current context, which reduces the network traffic between the Java GUI Server and the Java GUI Client. Due to its non-blocking behavior, you can work on different contexts while Java GUI Server processes your requests in the background.

Data Protector VMware Virtual Infrastructure integration

Data Protector A.06.10 introduces support for the VMware Virtual Infrastructure environment, enabling you to perform backups and restores of the following VMware objects:

- Virtual machines
- Filesystems of virtual machines (running Windows operating systems)

Backup

During backup, virtual machines can be online and actively used.

Data Protector offers the following backup methods:

- Snapshot
- Suspend
- VCBimage
- VCBfile

Data Protector offers interactive and scheduled backups of the following types:

- Full
- Incremental
- Differential

Restore

Virtual machines can be restored to the original or a different datacenter and ESX Server system.

Using the restore options, you can specify what to do once the virtual machines are restored. You can:

- Register virtual machines
- Power on virtual machines
- Consolidate virtual machine snapshot files to a single file

Filesystems can be restored to any Windows system (physical or virtual) that has the `VMware Integration` component installed.

If virtual machines or filesystems to be restored already exist in the destination, the restore options also enable you to specify whether you want to keep or overwrite the existing files.

Scripting solution

VMware ESX Server scripting solution that was provided by previous Data Protector versions is no longer supported. Virtual machines backed up such scripts can still be restored using the standard Disk Agent (common filesystem restore). If the virtual machines to be restored already exist in the destination datacenter, put them offline before you start the session.

Data Protector Microsoft SharePoint Portal Server Integration

Data Protector A.06.10 introduces support for the Microsoft SharePoint Portal Server application, enabling you to perform backups and restores of the following SharePoint Portal Server objects:

- Team databases

- Site databases (*portal_name*_SITE, *portal_name*_SERV, *portal_name*_PROF)
- Index servers
- Single sign-on database
- Document library

Team databases, site databases, and the single sign-on database are SQL Server databases.

During backup, the SharePoint Portal Server and the SQL Server instances are online and actively used. The SharePoint Portal Server integration provides the following backup types:

- Full
- Trans (MS SQL Server objects only)
- Differential (MS SQL Server objects only)

When performing a restore, Data Protector offers an option to specify the restore destination for SQL Server databases and index servers.

You can restore an SQL Server database to the original location or:

- To another SQL Server system
- To another SQL Server instance
- Under a different name

You can restore a SharePoint Portal index server to the original location or:

- To another client
- To another directory

If your SharePoint Portal Server farm is centralized (having the master portal and child portals), you have two options of how to restore the master portal:

- Restore the old master portal as a child on the current master portal
- Remove the current master portal and restore the old master portal

Data Protector Backup to HP Integrated Archiving Platform (IAP)

Data Protector A.06.10 introduces the integration with the HP Integrated Archiving Platform (IAP) that provides the data backup directly to the IAP appliance. This solution takes advantage of the powerful IAP capabilities, such as the ability of holding many

terabytes of data, eliminating redundancies in the stored data, powerful search tools and user-initiated information retrieval. Among the benefits of backup to IAP are:

- Increased storage capacity by using the smart cell storage approach.
- Maximized storage efficiency by eliminating unnecessary duplication of data.
- Information accessibility by using IAP capabilities to search the stored data.
- No need for performing periodic full backups. If you store the data into IAP, only the very first backup needs to be full, and all the subsequent backups are incremental.
- Reliable and fast single file point-in-time restores.

This solution was specially designed to meet the requirements of the following Data Protector customer groups:

- Customers who need to have constant access to their backed up data
- Customers who want to minimize their storage costs and achieve the optimal data storage
- Customers who need to have indexing capabilities and retrieve data by context and/or by metadata

The files backed up to the IAP appliance can be restored using the Search/Browse WebGUI.

Before using the Data Protector IAP integration, check for the latest available patches.

Support for new platforms

Microsoft Windows Server 2008

Data Protector A.06.10 introduces support for the Windows Server 2008 operating system for 64-bit processor architectures. The following Data Protector components are available for this platform:

- Cell Manager (including Manager-of-Managers)
- Installation Server
- User Interface
- Java GUI Client
- Manager-of-Managers User Interface
- Disk Agent
- General Media Agent

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

On a Windows Server 2008 platform, you can run backup sessions for backing up data residing on local file systems or remote network shares.

Symbolic links are a new filesystem feature available in Windows Server 2008. On this platform, Data Protector A.06.10 handles symbolic links in the same way as NTFS reparse points.

Microsoft Windows Vista

Data Protector A.06.10 introduces support for the Windows Vista operating system for 64-bit processor architecture. The following Data Protector components are available for this platform:

- User Interface
- Java GUI Client
- Disk Agent
- General Media Agent

On a Windows Vista platform, you can run backup sessions for backing up data residing on local file systems or remote network shares.

Symbolic links are a new filesystem feature available in Windows Vista. On this platform, Data Protector A.06.10 handles symbolic links in the same way as NTFS reparse points.

On Windows Vista systems, within the Disk Agent functionality, backup of CONFIGURATION objects is performed using Volume Shadow Copy Service.

HP-UX 11.31

Data Protector A.06.10 introduces support for the following components on HP-UX 11.31 operating system:

- Media Agent
- Disk Agent
- HP StorageWorks XP Agent
- HP StorageWorks EVA SMI-S Agent

With this support, Data Protector now recognizes **legacy** and **agile (multi-pathing and path-independent)** Device Special Files (DSFs) as backup objects and restore objects.

The agile DSFs are also called **persistent** DSFs.

Benefits of the agile DSFs naming model

Data Protector A.06.10 introduces support for the agile DSFs on HP-UX 11.31 systems. The agile naming model has the following benefits over the legacy naming model:

- Adaptability

  Agile DSFs are not affected by any physical changes in the paths to the device.
- Reliability

  Agile DSFs are more reliable than legacy DSFs, and are not affected by the number of paths leading to the device.
- Availability

  Agile DSFs are path-independent. This way using multi-path, high-availability software is no longer necessary (for example, the HP StorageWorks Secure Path).
- Scalability

  Agile DSFs support large size LUNs.

For more information, see the HP-UX related documentation.

Novell Open Enterprise Server (OES)

Data Protector A.06.10 introduces support for Novell OES running on 32-bit SUSE Linux Enterprise Server 9.0. This support enables you to run backup and restore of Novell Storage Services (NSS) volumes, native Linux volumes, and Novell Cluster Services volumes.

Disaster recovery enhancements and support for new hardware platforms and operating systems

New supported hardware platforms and operating systems

Data Protector A.06.10 introduces Enhanced Automated Disaster Recovery (EADR) and One Button Disaster Recovery (OBDR) on new platforms:

- Microsoft Windows Vista
- Microsoft Windows 2003 Server SP1 and R2 (on x64 and Itanium platforms)
- Microsoft Windows XP Professional SP2 (on x64 and Itanium platforms)

For details, see the latest support matrices at http://www.hp.com/support/manuals and the *HP Data Protector disaster recovery guide*.

Disaster recovery enhancements

Data Protector A.06.10 introduces the following disaster recovery enhancements:

- Support for Automated System Recovery (ASR) on nodes in Majority Node Set (MNS) Quorum server clusters.

  This enhancement enables you to create ASR disk sets and then perform an ASR on such server clusters.

Enhanced Data Protector Microsoft Volume Shadow Copy Service integration

Data Protector A.06.10 enhances the Microsoft VSS integration for zero downtime backup and instant recovery support through the VSS interface using Data Protector ZDB agents, and introduces support for additional applications through the VSS interface.

Microsoft VSS integration enhancements for zero downtime backup (ZDB) and instant recovery

Support for integration with Data Protector ZDB agents

Data Protector A.06.10 extends functionality of the Microsoft VSS integration by using HP StorageWorks EVA SMI-S Agent and HP StorageWorks XP Agent.

Support for Disk Array XP hardware provider provides two configuration modes: VSS compliant mode and resync mode. Resync mode requires HP StorageWorks XP Agent. Instant recovery method available depends on the configuration mode selected during ZDB to disk.

Support for EVA hardware provider together with HP StorageWorks EVA SMIS-S Agent introduces new instant recovery methods.

Filesystem backup

Data Protector A.06.10 supports backup of entire volumes (disks) with NTFS filesystem through the VSS/VDS interface. With hardware providers, volumes with FAT filesystem can also be backed up.

New instant recovery methods using ZDB agents

Using SMI-S Agent and XP Agent, Data Protector A.06.10 supports two new instant recovery methods:

- Copy of replica data with the source volume retained (using SMI-S Agent only)

  Instead of presenting the replica, a copy is created first and then presented during instant recovery. Another restore from the same backup data is possible and the source volume is retained.

- Copy of replica data with the source volume not retained (using SMI-S Agent or using XP Agent after backup in the resync configuration mode)

  During instant recovery, the source volume is directly overwritten by the replica. Another restore from the same backup is possible, but the source volume is lost.

For more information on using Data Protector Microsoft VSS integration together with ZDB integrations, see *HP Data Protector zero downtime backup integration guide*.

Mounting replicas to backup system

Replicas created during ZDB sessions can be mounted on the backup system. This enables you to perform additional, non-backup or restore related tasks, such as data mining.

Waiting for snapclone to complete

For HP StorageWorks EVA, Data Protector A.06.10 offers the option **Wait for the replica to complete** to wait for a specified period of time until the snapclone creation completes, before continuing with backup.

Support for new and improved support for existing writers

Microsoft SQL Server 2005

Data Protector A.06.10 introduces support for the Microsoft SQL Server 2005 writer. Only Full and Copy backup types are supported.

Microsoft Exchange Server 2007

Data Protector A.06.10 introduces support for the Microsoft Exchange Server 2007 writer, together with two Exchange Server models of replication for data protection: local continuous replication (LCR) and cluster continuous replication (CCR). With VSS integration, you can back up LCR or CCR replicas of databases and storage groups.

With Microsoft Exchange Server 2007 writer, you can restore (or perform instant recovery) a whole storage group or a single store not only to the original location but also to a different location:

- Different storage group
- Different server
- Non-Exchange location, with optional creation of the recovery storage group after restore

Improved support for Microsoft Exchange Server consistency check

Data Protector A.06.10 offers an improved support for consistency check of the Microsoft Exchange Server 2003/2007 writer. The consistency check can now be enabled from the Data Protector GUI or CLI and throttled to optimize restore performance.

Microsoft Virtual Server 2005

Data Protector A.06.10 introduces support for the Microsoft Virtual Server 2005 writer. You can back up individual virtual machines and the Virtual Server configuration using the Data Protector Microsoft VSS integration.

For more information on Data Protector Microsoft VSS integration and its new features, see *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*.

Enhanced Data Protector Microsoft SQL Server integration

Enhanced configuration

Until now, if you wanted to enable Data Protector to connect to the SQL Server instance with a Windows domain user account, you had to restart the Data Protector `Inet` service under this account and select the Data Protector Integrated security option during the Data Protector SQL Server configuration. Since different SQL Server instances could have different Windows administrative accounts, you had to restart the Data Protector `Inet` service whenever you wanted to back up a different SQL Server instance.

Data Protector A.06.10 provides a new option in the Configure the SQL Server dialog box, enabling you to specify a Windows domain user account for each SQL Server instance separately.

Support for Windows x64 platform

Data Protector A.06.10 introduces support for Microsoft SQL Server 2005 running on the 64-bit Windows x64 platform. This support enables you to run standard backups and restores of Microsoft SQL Server 2005 databases, as well as ZDB and instant recovery sessions.

Enhanced Data Protector Oracle Server integration

Simplified configuration

The configuration of the Data Protector Oracle Server integration is now much simpler. You no longer have to create symbolic links to the Data Protector MML on UNIX Oracle clients. Therefore, if you have upgraded UNIX clients from an older version of Data Protector, it is recommended that you remove the existing symbolic links.

Enhanced Oracle integration on OpenVMS platforms

Data Protector A.06.10 introduces support for Oracle 10g on OpenVMS platforms. See the *HP Data Protector integration guide for Oracle and SAP* for details.

Enhanced Data Protector SAP R/3 integration

Enhanced configuration

The configuration of the Data Protector SAP R/3 integration for the RMAN mode is now much simpler. You no longer have to install and configure the Data Protector Oracle Server integration.

Authentication improvements

Data Protector A.06.10 introduces a new authentication mode for accessing SAP R/3 databases: operating system authentication. The Data Protector SAP R/3 integration can now use two authentication modes when backing up and restoring Oracle databases that are used by SAP R/3:

- database authentication mode
- operating system authentication mode

With database authentication mode, you need to re-configure the SAP R/3 integration for an SAP R/3 database each time the corresponding Oracle database user account changes. Such a reconfiguration is not needed if the operating system authentication mode is used.

You select the preferred authentication mode when you configure the SAP R/3 integration for a particular SAP R/3 database.

SAP compliant ZDB sessions

In previous releases, you could start ZDB sessions (more specifically, BRBACKUP) only on the application system. With A.06.10, you can configure Data Protector to start ZDB sessions on the backup system, which is what SAP recommends.

Enhanced Data Protector Microsoft Exchange Server integration

Data Protector A.06.10 introduces support for Microsoft Exchange Server 2007 running on the 64-bit Windows x64 platform. This support enables backup and restore of Exchange Server databases, as well as individual mailboxes and Public

Folders. Backup and restore are performed in the same way as with previous Exchange Server versions.

Zero downtime backup (ZDB) and instant recovery of Exchange Server 2007 data are not supported.

Enhanced Data Protector Lotus Notes/Domino Server integration

Data Protector A.06.10 introduces an enhanced Lotus Notes/Domino Server integration agent, which significantly improves backup and restore performance, and simplifies the configuration of the integration. The new agent reduces the time needed for backup as well as the CPU usage and memory consumption on the Cell Manager.

Disk agent enhancements

Data Protector A.06.10 Disk Agent enhanced Windows platform support for Microsoft Volume Shadow Copy Service

The Data Protector A.06.10 Disk Agent supports Microsoft Volume Shadow Copy Service filesystem backup on Windows XP Home Edition, Windows XP Professional 32–bit Edition, and Windows XP Professional 64–bit Edition operating systems running on AMD64/Intel EM64T or Itanium processors.

Windows Disk Agent performance improvement

Data Protector A.06.10 introduces asynchronous reading to improve Disk Agent performance of Windows filesystem backup. Asynchronous reading improves performance of the Disk Agent when backing up data on disk arrays, especially if large files are backed up. You can set the **Asynchronous reading** option for the whole backup specification or for an individual backup object.

Device enhancements

Data Protector A.06.10 introduces the following device enhancements:

- Automatic restore device selection

Until now, if the devices that were used for backup were not available during restore, Data Protector would wait for the devices to become available. This would cause a delay in the restore session. In Data Protector A.06.10, you can configure Data Protector to automatically replace unavailable devices with available devices of the same subtype.

- Automatic device disable

  This enhancement enables you to configure Data Protector to automatically disable devices on which a certain number of unknown errors has occurred. You determine the threshold value by setting the `SmDeviceErrorThreshold` global option.

- Reserve or release SCSI robotics or drive

  This enhancement enables SCSI Reserve/Release. By selecting this option, the devices are reserved only for Data Protector operations.

Support for Smart Media Copying Using HP StorageWorks Virtual Library System (VLS)

Data Protector A.06.10 enhances the media copy functionality by introducing the migration of the backed up data from the HP StorageWorks Virtual Library System (VLS) to a physical tape library using Data Protector. In this solution, the data is first backed up to a virtual tape of a virtual tape library (VTL) configured on the VLS; then, a copy of a virtual tape containing a backup is made to the physical library attached to the VLS in a process called automigration. Data Protector triggers the copy process and manages it in the same way as a standard media copy allowing you to monitor the status of a copy operation and retrieve the information on physical libraries.

The data transfer from a VLS to a physical library, which is supported by Data Protector, is called smart copying. Smart copies are initiated by Data Protector and then performed by the VLS. In a smart copy operation, Data Protector adds its own media header to the copies on the target media thus allowing to distinguish between the source and the target medium and enabling media management. You can use smart copies for disaster recovery and archiving purposes. The existence of multiple copies on disk and tape increases the availability of the backed up data and adds security to your backups.

The VLS automigration integrated into Data Protector brings the following benefits:

- Easy management, as smart copies are managed as standard Data Protector media copies meaning that Data Protector tracks the status of copy operations and monitors copy sessions. The information about smart copies is stored in the Data Protector IDB.

- Increased backup performance and significantly decreased backup window. The fast primary backups to the VLS' disk-based virtual tapes are made with the minimal impact on your environment. Smart copying takes place as a secondary task without causing any disruption to the application performance.
- Additional protection against data loss due to the existence of multiple copies on disk and tape.
- The ability to start several smart copy sessions simultaneously. The number of concurrent sessions depends on the number of physical libraries connected to the VLS.
- The ability to create smart copies allows you to keep your data available for restore or data archiving for longer periods of time without exceeding the capacity of a virtual library.
- Fast and reliable restores using the Data Protector restore functionality.

You can configure interactive and automated smart copying. Interactive smart copying is started manually. Automated smart copying can be configured to occur after the completion of a backup session (post-backup smart copying). As a result, the media used in that particular session are copied. You can also create a copy of a medium used in a particular backup session at a scheduled time (scheduled smart copying).

Internal database enhancements

Flexible time frame filtering options in the Internal Database

Data Protector A.06.10 provides more flexible filtering options to view sessions in the Internal Database. You can customize the filtering options according to your needs by specifying the exact start date and time as well as the end date and time.

DCBF limit

With previous versions of Data Protector, the size of detail catalog binary files was limited to 2 GB. Data Protector A.06.10 increases the maximum size for DCBF files as well as for DCBF directories. DCBF files are now limited only by the file system settings.

Improved reporting

Data Protector A.06.10 introduces backup session auditing functionality, enhanced reporting functionality, and provides you with additional information on your backup environment:

- Backup session auditing

  Data Protector A.06.10 introduces backup session auditing, which stores non-tamperable and non-overwritable information about all backup tasks that were performed over user-defined periods for the whole Data Protector A.06.10 cell. The auditing information is retrievable on demand in an integral and printable fashion for auditing or administrative purposes.

- Object copy and consolidation reporting

  Most relevant reports are now modified to include information regarding the object copy and object consolidation functionalities. Several reports are renamed to more generic names, so that, for example, the names of those that apply only to backup reflect that. In addition, they are two new reports.

- Enhanced Drive Flow report

  Until now, only logical device names were shown in the Device Flow report. In Data Protector A.06.10, you can configure the report to show also the physical representation of devices (lock names and serial numbers). In addition, devices with the same physical representation are grouped together.

  The MoM enterprise (multi-cell) Device Flow report has also changed. The summary lines that separate different Cell Managers make the report easier to scan quickly.

Change Log Provider

Data Protector A.06.10 enhances the incremental backup functionality by introducing the enhanced incremental backup using the Windows NTFS Change Log Provider. The Change Log Provider is based on the Windows Change Journal that records all changes made to the files and directories on an NTFS volume. Data Protector uses the Change Journal as a tracking mechanism to generate a list of files that have been modified since the last full backup. The main change from a traditional enhanced incremental backup is that a list of files to be backed up is generated by querying the Change Journal rather than performing a file tree walk, which can take a considerable amount of time to complete.

Using the Change Log Provider for incremental backups results in improved backup speed, since Data Protector queries the Change Journal to get a list of changed files rather that uses a file tree walk that scans all files on a filesystem. This reduces the

amount of time needed to perform an incremental backup and improves the overall incremental backup performance in the environments that contain millions of files only a few of which change between backups.

To perform an enhanced incremental backup using the Change Log Provider, select the **Use native Filesystem Change Log Provider if available** backup option in a backup specification. If the Change Journal is not active at the backup time, you need to turn it on for each filesystem. A set of new commands and omnirc variables is provided to control and administer the Change Journal and optimize the Change Log Provider performance.

Additional changes and improvements

Enhanced HP AutoPass functionality

HP AutoPass, the utility used for automatic retrieval and installation of Data Protector license passwords, has been extended with new options and additional platform coverage. For more information on AutoPass, see the *HP Data Protector installation and licensing guide* and the HP AutoPass online Help.

Scheduler enhancements

Data Protector A.06.10 offers an improved and extended scheduling functionality:

- Backups can be scheduled up to the year 2038.
- Finer scheduler granularity enables you to tune your scheduling to the nearest minute.
- Time zone independence allows you to see all scheduler-related times as seen on the Cell Manager system, not taking into account time zone differences.

Recycling of failed source objects

Data Protector A.06.10 enables you to recycle failed backup objects on your media. A new option, **Recycle data and catalog protection of failed source objects**, has been introduced to remove data and catalog protection of failed objects. Consequently, the media can be reused for new backups. The option is available in the post-backup or scheduled object copy specification.

Single session restore from GUI

Data Protector A.06.10 introduces restore from a single incremental session, enabling you to restore files without having to restore the entire restore chain. This feature simplifies and speeds up the restore.

Debug log collector enhancements

Data Protector A.06.10 offers a new version of the debug log file collector utility (the Data Protector `omnidlc` command), enabling you to add user-specific information to the debug data that you send to the HP Customer Support Service. In addition, you can now exclude the configuration information from the collected data.

Separate English language documentation and online Help installation package

In previous Data Protector releases, you could only install the documentation and online Help together with the graphical user interface. Data Protector A.06.10 introduces a new English language documentation and online Help installation package that is independent of the graphical user interface.

3 Limitations and recommendations

Size limitations

Internal database size

	Data Protector A.06.10
Number of filenames[1]	48 GB or approximately. 1,050 million (UNIX systems) or 675 million (Windows systems)
Number of file versions	10 x number of filenames
Maximum number of DCBF [2] directories	50
Maximum size per DCBF directory [3]	2,047 TB
Maximum size per DCBF file	limited by the file system settings
Maximum number of files per DCBF directory	10,000
Maximum number of concurrent drives (DLT7000 and lower performing)	100

	Data Protector A.06.10
Maximum number of concurrent drives (DLT8000/SDLT/LTO)	50

[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 32,768 MB (32 GB).

Number of media

There can be up to 40,000 media in one pool.

In total, there can be 500,000 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 1,000,000 sessions in the database. At the most, 9,999 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).

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.

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 A.06.10. You must perform a new full client backup with Data Protector A.06.10 after the upgrade.

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 A.06.10 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 vice versa. File objects however, can be restored to a different filesystem without ACLs.
- Cross-platform restore of ACLs is not supported. This limitation is due to different internal ACL data structures on different operating systems.
- Modification of ACL entries does not affect the modification time of the file object, so the file object (and the modified ACL) is not backed up during an incremental backup.
- The GUI can display a maximum 64,000 items (files in one directory, slots in a library, and so on) in a tree view.
- File names containing quotation marks are not supported.
- 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 A.06.10 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.

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.

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.

- SNMP traps are not supported on 64-bit Linux systems (x86-64).
- Cross-platform restore of ACLs between 32-bit and 64-bit Linux operating systems is not supported.

Windows limitations

- Windows directory share information can only be restored to a Windows system with a Data Protector A.06.10 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 A.06.10. 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 64,000 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 2000 systems, Data Protector Cell Manager cannot be installed if NetLimiter is installed on the same system.

- On Windows 2000 systems, Data Protector cannot be installed if any of the products from the Citrix MetaFrame application family is installed on the system (QXCR1000109889).
- On Windows Vista 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 and Windows Server 2008 systems, the broadcast message send method is not supported.

32-bit Windows 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.

64-bit Windows 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 native 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 A.06.10 does not support Web Reporting on the 64-bit versions of Windows XP and Windows Server 2003, as JVM does not include support for Itanium 2 on Windows.
- On AMD64/Intel EM64T systems, sending notifications and reports by e-mail using MAPI is supported only with Microsoft Outlook Express, and not Microsoft Outlook.

Windows Server 2008 limitations

- **Server roles and CONFIGURATION backup on Windows Server 2008**

  Similarly to previous Windows Server operating system releases, Microsoft extended the concept of server roles in Windows Server 2008. To enable backup and restore of data belonging to each particular server role, the Data Protector

CONFIGURATION backup and restore functionality is extended appropriately. Data Protector A.06.10 supports backing up data that belong to the following Windows Server 2008 server roles:

- Active Directory Domain Services (AD DS)
- Application Server (requires IIS 6 compatibility)
- Dynamic Host Configuration Protocol (DHCP) Server
- DNS Server
- Terminal Services
- Web Services (IIS) (requires IIS 6 compatibility)

Backup of server roles introduced with Windows Server 2008, like Active Directory Certificate Services, Hyper-V, and Network Policy and Access Services, is not supported. However, particular server roles exist, for example Active Directory Lightweight Directory Services (AD LDS), whose data can be backed up using the Data Protector filesystem backup functionality. For a consistent backup, you need to select the **Use Shadow Copy** option on the **WinFS options** property page of the **Filesystem Options** window.

To determine which CONFIGURATION items will be backed up on a system, expand the CONFIGURATION object in the filesystem browser window of the Data Protector GUI. It is recommended that you always back up the system volume together with all CONFIGURATION items.

- **Active Directory Domain Service restore**

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

Novell Open Enterprise Server (OES) limitations

- Data Protector A.06.10 cannot backup or restore:
  - Any GroupWise system files.
  - eDirectory information (not supported by Novell).

  When a cross-file system restore is attempted from NSS to a native Linux volume, the NSS file system specific attributes will be lost while the data will be intact.

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 vice versa, these are the only cross-system restore scenarios supported.
- The restore option `Omit deleted files` is not supported.

MPE/iX limitations

- The MPE/iX client must be installed locally on the MPE/iX system. There is no support for a remote installation from an Installation Server.
- The maximum number of MPE/iX Disk Agents that can be running at the same time is limited to 15.
- The backup of MPE/iX configuration files or operating system is not possible. If you need to recover the MPE/iX configuration files or operating system, you should create a System Load Tape (SLT).
- The TurboSTORE/iX 7x24 True-Online product musts be installed on the system in order to use the online and true-online backup options (option `ONLINE` and `ONLINE = START`).
- True-online backup with the `ONLINE = END` option is not supported.
- Cross-platform restore is not supported.
- The maximum length of arguments (trees and directories) for Data Protector `-tree` and `-exclude` Disk Agent options is 210 characters. It is recommended to back up whole accounts and groups on MPE/iX filesystem, instead of backing up individual files in one backup session.
- Backup preview with option`-exclude` uses POSIX wildcards (`*`, `?`). Backup with option `-exclude` uses specific MPE/iX wildcards `@` (replace zero or more alphanumeric characters) and `?` (replace one alphanumeric character).
- Maximum Media Agent communication buffer is 32 KB.
- On MPE/iX clients, only the `omnib` command is supported.
- The following TurboSTORE/iX options are not supported and must not be used: `FCRANGE`, `FCRANGE`, `FILES`, `LOGVOLSET`, `MAXTAPEBUF`, `NOTIFY`, `ONERROR`, `PURGE`, `RENAME`, `SPLITVS`, `STOREDIRECTORY`, `STORESET`, and `TRANSPORT`.
- The following TurboSTORE/iX options are not supported by the TurboSTORE/iX API (which is used by Data Protector A.06.10 for backup and restore): `COMPRESS`, `FCRANGE`, `FILES`, `FULLDB`, `INTER`, `LOGVOLSET`, `MAXTAPEBUF`, `NOTIFY`, `ONERROR`, `ONLINE=END`, `PARALLEL`, `PARTIALDB`, `PURGE`, `RENAME`, `SPLITVS`, `STOREDIRECTORY`, `STORESET`, and `TRANSPORT`.
- A tape device on a MPE/iX system needs to be brought online after every Media Agent operation before attempting the next operation.
- Tape statistics functionality is not supported on Media Agents running on MPE/iX.

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. See the OpenVMS Software Product Description (SPD) for a complete list of tape drives.
- 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 logfile 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.

Limitations on disk array integrations

HP StorageWorks Disk Array XP limitations

- Asynchronous CA configuration is not supported.
- With BC1 configurations, only filesystem and disk image backup is supported.
- Split-mirror restore (restore to a secondary volume and synchronizing to the primary volume) is supported for the filesystems and disk images in the BC configuration. Database (application) split-mirror restore is not supported.
- Instant recovery is only possible to restore the data backed up in BC 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 StorageWorks Disk Array XP 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.

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.

HP StorageWorks Virtual Array limitations

- Only one logical volume can reside on one HP StorageWorks Virtual Array LUN in case LVM Mirroring is used.
- LUN0 is used as a command device and is accessed by all hosts connected to the disk array. Follow the array guidelines with configuration of LUN0 and make sure it does not contain user data.
- Dynamic disks are not supported.
- 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.
- Due to a hardware limitation, it is not possible to perform instant recovery if extra snapshots, associated with the same parent LUNs as those to be restored are existing on the HP StorageWorks Virtual Array.

  Workaround: Delete (either using `omnidbva` or manually) these extra snapshots before you start the instant recovery. Snapshots created by Data Protector can be identified using the `omnidbva -lun` command.

- If instant recovery is performed, all snapshots for the parent LUNs involved in the instant recovery session will be deleted automatically before the restore takes place.
- 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.

HP StorageWorks Enterprise Virtual Array limitations

- 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.
- For ZDB-to-disk and ZDB-to-disk+tape sessions (instant recovery enabled), only snapclones can be used.
- 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.
- 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.

NDMP limitations

- Only filesystem backup and restore is possible.
- The NDMP integration can handle backups of 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`.
- Load balancing is not supported.
- Only Full and Incr1 backup levels are supported.
- Maximum device concurrency is 1.
- Device selection as well as filesystem browsing is not possible.
- Supported device block sizes arethe following:

NAS device	Block size range (KB)
ONTAP < 6.5.3	64
ONTAP ≥ 6.5.3	64 ≤ *Size* ≤ 256
Celerra	64 ≤ *Size* ≤ 256

- 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, object mirroring, and media copying 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.

- Restore preview is not supported.

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.

Celerra

- If you select directory restore using the Direct Access Restore functionality, only the selected directory will be restored without its contents. To restore an entire directory tree, set `DIRECT=N`.

IAP backup limitations

- Only Windows NTFS filesystem backup is supported.
- Backup of Windows CONFIGURATION is not supported.
- Backup of network shares (CIFS, SMB) is not supported.
- Backup of FAT16 and FAT32 filesystems is not supported.
- Data encoding and compression is not possible.
- Backup of sparse files and reparse points is not supported; these objects are skipped from backup with an appropriate warning message.
- Disk image backup is not supported.
- Hard links are backed up as files.
- Only unnamed stream (file content) is stored into IAP; alternate NTFS streams are not backed up and restored.
- A backup specification containing IAP devices cannot contain other devices (tape devices, file devices, and so on).
- Disaster recovery is not supported.
- Object copy and object consolidation are not supported.
- Object mirroring is not supported.

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.

Direct backup limitations

- In a direct backup environment, the backup and restore of an Oracle database installed on raw partitions (rawdisk or raw logical volumes) are not supported.
- Instant Recovery of data backed up in a direct backup environment is supported only if:
  - Control files and online redo logs do not reside on the same logical volumes as data files.
  - A whole database backup had been performed, meaning that all data files that belong to the Oracle Server instance had been selected during the backup.
- The pre-exec and post-exec options for backup objects are not available for direct backup of raw logical volumes. They are available for Oracle direct backup.
- The systems in the direct backup environment must use HP-UX 11.11 operating system.

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 database 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 vice versa.
- The Oracle backup set ZDB method is not supported if the database is installed on raw disks.

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_OLFomnirc` 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.

SAP DB/MaxDB limitations

- You cannot perform transactional backups (log backups) of SAP DB database instances with SAP DB versions prior to 7.04.03.

Informix Server limitations

- On Windows, due to an Informix Server known issue, you cannot perform an Informix Server restore by a logical log number with the Informix Server version 7.31.TC2.
- On Windows, cold restore of non-critical dbspaces is not possible.

Microsoft Exchange Server limitations

- Backup preview is not supported.

Microsoft SQL Server limitations

- Backup preview is not supported.

VSS limitations

Common VSS limitations

- Backup preview is only available for VSS filesystem backup sessions.

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

- Functionality for VSS 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.

VMware Virtual Infrastructure limitations

Data Protector 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:** Functionality for integration with VMware Virtual Infrastructure 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.
- **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**).

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.

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: EVA or 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 vice versa.
- 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.
- 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 1,024 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 not currently supported if the Media Agent runs on: MPE/iX, SCO, Novell NetWare, Linux, Sinix, 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 1,023 characters.
- Devices of type file library are not supported for filesystem which have compression turned on.
- The length of the directory names which can be configured for devices of type file library cannot exceed 46 characters.
- The length of the pathname 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, Windows Server 2008, 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 is not available in the Data Protector Java GUI.
- If Boot Configuration Data (BCD) is located on removable storage like floppy disk, flash card, CD-ROM or DVD-ROM, Data Protector cannot backup BCD registry entries.

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.

Recommendations

Number of clients in a cell

In typical environments, 100 clients per cell is a recommended number. In some customer environments, it is possible to have several hundred clients in one cell, depending on factors like:

- IDB load: types of objects backed up, filesystem log level, image, online database, split-mirror backup/zero downtime backup, NDMP, and so on.
- Network and system load: local versus network backup, level of concurrent backup activities.
- Maintenance tasks: user management, configuration of backup specifications, upgrading, patching.

The maximum number of clients per cell should not exceed 1,000.

Large number of small files

Backup of a client with a large number (higher than 100,000) 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.

Synthetic backup – object consolidation frequency

When consolidating a large number of objects 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.

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.

GUI on UNIX systems

When using the GUI on UNIX systems, it is strongly recommended to set the locale to a locale that uses UTF-8 encoding in order to:

- enable switching between different encodings, thus enabling proper display of file names and session messages containing non-ASCII characters in mixed environments.
- ensure that names of devices, backup specifications, and such, containing non-ASCII characters, which were created in UNIX GUI, also display properly in Windows GUI, and vice versa.
- prevent failures to create a backup specification or other similar items when using an S-JIS locale on UNIX, typically when using characters with second byte equal to '\' (backslash).

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.

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”.

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 to the Cell Manager system and run the command `omnicc -update_host` *`virtual-name`* for every virtual name (other than cluster name).

- When installing Data Protector clients remotely in a cluster environment, the Data Protector GUI allows you to push the components to a virtual host, even though the components must not be added to the virtual host.

  Workaround: None. Do not push the components to the virtual host, but install the clients locally as described in the documentation.

- 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 a 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 A.06.10.

- On HP-UX 11.23 and HP-UX 11.31 (Itanium) and SuSE Linux (x86-64) systems, the maximum size of database files can exceed the preconfigured maximum size of 2 GB. Consequently, during an upgrade to Data Protector A.06.10 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 A.06.10 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.

- Backups fail after upgrading a Data Protector A.05.10 or A.05.50 SAP R/3 client to Data Protector A.06.10.

  Workaround: Set the ORA_NLS_CHARACTERSET parameter to the encoding used by the Oracle database by running:

  ```
  util_cmd –putopt SAP SAP_instance ORA_NLS_CHARACTERSET
  Oracle_encoding
  ```

- Automatic disaster recovery (EADR, OBDR) is *not* supported on the Microsoft Windows Server 2008 operating system. However, when installing on a Windows Server 2008 system, the Setup Wizard lists the Automatic Disaster Recovery component, allows you to select it, and even installs it without a warning. Data Protector also allows remote installation of the Automatic Disaster Recovery component to a Windows Server 2008 system.

  Workaround: Do not select the Automatic Disaster Recovery component when installing on a Windows Server 2008 system.

- In a MC/ServiceGuard cluster, 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*.

- 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
  ```

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".

- Interactive backup does not start if you start it from the Data Protector Java GUI from the **Objects** navigation tab and the backup specifications are sorted **By Name** (in the Cell Manager) or **By Manager** (in the MoM).

  Workaround: Sort the backup specifications **By Type** or **By Group** and then start an interactive backup, or start an interactive backup from the **Tasks** navigation tab.

Media agent and disk agent related issues

- 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.
- 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`.
- 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.
- If you restart the system during a backup session, the medium to which data is backed up may get 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.
- 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: 27/09/00 16:58:40 Nothing restored
  ```

  Workaround: 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.
- 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 A.06.10, 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:
  2/22/2003 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.

- If you are upgrading from Data Protector A.05.10, the default block size for file devices, file libraries, and jukebox devices is changed from 16 kB to 64 kB after the upgrade. The media append and import operations with such devices are not possible if the media were configured with the default block size setting before the upgrade.

  Workarounds:

  - If you still need the data on the media, change the block size setting to 16 kB for the devices used with the needed media.

- If you do not need the data on the media, recycle or reformat the media using the new default block size setting.

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

  ```
  [Critical] From: MSM@vinyl.hermes.com "FUYL" Time: 13.8.04
  11:29:16 Failed to allocate memory. [Normal] From:
  MMA@vinyl.hermes.com "FUYL" Time: 13.8.04 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 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: 8/31/2004
  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.
```

- 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?
  ```

- 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.
- 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 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.

- On Windows systems, Data Protector ignores the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`. Files and folders listed in this key do get backed up.

  Workaround: When creating a Data Protector backup specification, do not rely on the above registry key, but exclude from backup all files and folders that you do not want to back up.

- Data backed up from a shared network folder using Data Protector Disk Agent installed on a Windows Vista 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.

- 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.

  - 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

- ZDB session involving Microsoft Exchange 2000 Server (which was upgraded to SP3) fails with the following error:

  ```
  [Normal] From: SNAPA@tuljan.ipr.com
  <mailto:SNAPA@tuljan.ipr.com> "" Time: 7/24/2002 10:26:52
  AM Executing the split pre-exec script. (omniex2000.exe
  -dismount -storage_group 'Accept' -appsrv vaexchg.ipr.com)
  [Critical] From: SNAPA@tuljan.ipr.com
  <mailto:SNAPA@tuljan.ipr.com> "" Time: 7/24/2002 10:26:53
  AM [224:501] Split links pre-exec command failed with exit
  code -1.
  ```

  Workaround: After Exchange 2000 Server is upgraded to SP3, `omniex2000.dll` must be unregistered and registered again. From *`Data_Protector_home`*`\bin` directory on the Exchange 2000 Server system, run the `regsrv32.exe` command.

  To unregister, run `regsvr32 /u omniex2000.dll`.

  To register, run `regsvr32 omniex2000.dll`.

- 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.

- For remote administration purposes, to be able to run the `omniex2000SM.bat` script from a Windows Data Protector client that does not have the MS Exchange

Integration software component installed, you must copy the `omniex2000SM.bat` to such a client.

- By default, Data Protector does not support restoring data to Recovery Storage Group of Exchange Server 2003. However, if you enable Recovery Storage Group, the restore will fail.

  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.
- It is not possible to perform Single mailbox backup on Exchange 2007 running on Windows Server 2008. The GUI reports an error while browsing the mailboxes, and when all mailboxes are selected, the backup reports an error:

  ```
  [Critical] From: OB2BAR_Main@host.domain.com "Single Mailbox" Time: 11/20/2008 8:31:43 PM
  The information store could not be opened.
  ```

  Workaround: None.

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.

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 split-mirror 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/XP 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 not 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.

Informix Server

- Restore of Informix Server objects from backup data created before upgrade from Data Protector A.05.10 becomes unresponsive if backup was session used a file device, file library, or jukebox device and if the default block size setting was used for the media in such devices. This is due to the change of the default block size for file devices, file libraries, and jukebox devices from 16 kB to 64 kB during the upgrade from Data Protector A.05.10 to Data Protector A.06.10.

  Workaround: Change the block size setting for the devices used with the media needed for the restore from the default (64 kB) to 16 kB.

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*.
- To prevent creation of two volume groups with the same minor number after two backup sessions are started concurrently, HP StorageWorks Disk Array XP agent (SSEA) locks the backup system for the entire backup preparation phase. However, the lock is required only during the volume group creation. Consequently, there may be considerable delays in execution of concurrent backup sessions.

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 *HP Data Protector command line interface reference*.

- An *offline* or *local* EADR or OBDR will fail if the backup that is used for disaster recovery was encrypted using LTO4 drive-based encryption without AES 256-bit encryption, because Data Protector does not recognize the backup as encrypted.

  Online disaster recovery works properly.

  The issue does *not* occur when only the AES 256-bit encryption is used or if drive-based encryption is used together with AES 256-bit encryption.

  Workaround:

  Follow these steps when performing a disaster recovery:

  1. Start the disaster recovery, but abort the recovery process immediately by pressing any key when prompted and open the Command Prompt.
  2. In the folder `\$DRM$\$BKP$\Disk1\`, open the `recovery.srd` file with a plain text editor, replace all occurrences of the string `-encrypt StrNull` with `-encrypt "aes256"` and save the changes.
  3. Close the Command Prompt and resume the disaster recovery procedure.
  4. When prompted to enter the encryption key, provide the location of the previously exported key.

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 7,200 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 with 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: 11/8/2001
  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 with 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.

Disk Array XP integration issues in a cluster environment

- In a cluster environment, if an instant recovery is performed on a different node than the backup (in case of a failover between the ZDB and instant recovery sessions), the instant recovery fails with an error similar to the following:

  ```
  [Warning] From: SSEA@x64-node2.x64ring.com "" Time:
  2/19/2008 2:35:46 PM Failed to get command device from XPDB
  for LDEV 8690.
  ```

  This problem occurs if different command devices are configured for each node.

  Workarounds:

  - Ensure that the same command device is used on both nodes.
  - Use the `omnidbxp` command to manually add the missing command device. For details on how to add a command device using `omnidbxp`, 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 `CopyAutomatedMaxObjects`.

- 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 (e.g. 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 (e.g. 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, inc1, inc2, inc3...), 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 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.
- 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 my 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.

- If more than one `omnidbutil -purge` session is started, `omnidbutil` reports that it cannot communicate with the Cell Manager. To avoid this, do not start more than one session.
- 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.

- 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.

Known non-Data Protector issues and workarounds

Non-Data Protector issues related to installation or upgrade

- On Windows systems, after installation or upgrade to Data Protector A.06.10, the operating system may report that some application is not installed or that its reinstallation is required. The reason is an error in the Microsoft Installer upgrade procedure.

  Workaround: Forr problem 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 uninstall Data Protector packages if you specify several packages in one command. 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 packages 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. To eliminate this problem, start the desktop in your desired locale.

- Due to known Java issues with modality, if two or more modal dialogs are opened in the Data Protector Java GUI, the latest opened dialog must be closed first.

  Workaround: Close the dialogs in the opposite order as you opened them.

- On HP-UX, Solaris, and Linux systems, when you open the Data Protector online Help in the Mozilla web browser, the navigation pane of the online Help system is not displayed correctly. The navigation pane occupies only a small portion of the available space in the browser window, making the Contents, Index, Search, and Glossary pages inconvenient to use.

  Workaround: None.

Non-Data Protector issues related to media agent and disk 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: 5/6/2002 3:52:37
  PM [90:90] /dev/rdsk/c2t0d1 Cannot erase disk surface ([22]
  Invalid argument) => aborting
  ```

- If physical address expansion (PAE) is enabled for a Windows 2000 system, Data Protector is not able to correctly manage devices such as LTO Ultrium. Device operations fail with the following error:

  ```
  error 87 cannot write to device the parameter is incorrect.
  ```

  This problem occurs if the tape that is being restored was created while the physical address extensions (PAE) feature was disabled.

  Workaround: Set the registry key `MaximumSGList` to a value of 17. `MaximumSGList` should be located at `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<adapter>\Parameters` where *<adapter>* represents the ID of a SCSI interface used for controlling the device, for example aic78u2 for Adaptec.

- 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.
- 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.
- Due to known issue in Windows 2000 operating system, the backup of Active Directory may fail, especially in cases when several backup sessions are started within a short period of time.

  Workaround: Install the Microsoft Windows 2000 Service Pack 2. For more information, see the Microsoft web page http://support.microsoft.com/support/kb/articles/Q282/5/22.ASP.

- When a DLT8000 (StorageWorks_E 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: 10/31/01
  19:52:35
  [90:182] Cannot forward segment. ([5] I/O error)
  [Major] From: MMA@hkgbkup3 "HKGBKUP3_1m" Time: 10/31/01
  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. For firmware upgrade instructions, see the firmware upgrade web page http://www.hp.com/cposupport/swindexes/hpsurestor18551_swen.html. More details about the firmware changes can be found in Service Note A5597A-27.

- 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 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.
- 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.
- 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.

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 SQL Server

- Data Protector does not properly integrate with Microsoft SQL Server 7.0 installed as a cluster-aware application.

  Workaround: Update Microsoft SQL Server 7.0 with Microsoft SQL Server 7.0 Service Pack 1.

- 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.

SAP R/3

- On Solaris systems, version 4.6C of SAP R/3 BRTOOLS cannot properly back up SAP R/3 datafiles, although backup sessions for backing up databases and tablespaces succeed.
- Backing up an SAP R/3 database using the zero down time backup functionality and Oracle Recovery Manager at the same time fails.

  During such backup session, the following error may occur:

  ```
  BR002I BRARCHIVE 4.6D (17) BR252E Function fopen() failed
  for '/oracle/YP1/817_64/saparch/adhjhzoc.cpd' at location
  main-4 BR253E errno 2: No such file or directory BR121E
  Processing log file /oracle/YP1/817_64/saparch/adhjhzoc.cpd
  failed sh: 12312 Memory fault [Warning] From: OB2BAR@sv005
  "OMNISAP" Time: 02/20/02 10:54:03 BRARCHIVE
  /usr/sap/YP1/SYS/exe/run/brarchive -d util_file -scd -c
  returned 35584
  ```

  Workaround: Add the Oracle `NLS_LANG` environment variable into the SAP R/3 configuration file:

  ```
  NLS_LANG=AMERICAN_AMERICA.WE8DEC
  SAPDATA_HOME=/oracle/YP1
  ```

- On Solaris systems, offline SAP R/3 ZDB to disk (SPLITINT) sesson fails with the following error message:

  ```
  BR0253E errno 4: Interrupted system call
  ```

  Workaround: None. The problem may be solved by using a newer version of SAP R/3 BRTOOLS.

SAP DB/MaxDB

- Backup completes with errors if filenames contain spaces.

  Workaround:

  - On Windows systems:
    1. Change the RUNDIRECTORY parameter to short (8+3) path names and edit filenames in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\SAP\SAP DBTech\IndepData`.
    2. Restart the database.
  - On HP-UX and Linux systems:

1. Create a symbolic link to the directory with a space in the name and adjust the RUNDIRECTORY parameter of the database to use the symbolic link.
2. Adjust the values of the `IndepData` parameter in the file `/var/spool/sql/ini/SAP_DBTech.ini` (on HP-UX) or `/usr/spool/sql/ini/SAP_DBTech.ini` (on Linux).

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

  Workaround: Contact MaxDB support.

Oracle

- 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 StorageWorks XP 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).

Informix Server

- On Windows 2000 systems, due to an Informix Dynamic Server known issue, the point in time restore for Informix Dynamic Server 7.31 TC8 does not function properly.

  Workaround: Contact Informix Server support for an appropriate patch.

- With 64-bit version of Informix Dynamic Server 7.3x , the `onbar` command located in the directory `$INFORMIXDIR/bin` does not work properly.

  Workaround: Copy the `onbar` command from 32-bit version of Informix Dynamic Server 7.3x or contact Informix Dynamic Server support.

- On Windows 2000 systems, due to an Informix Dynamic Server 7.31.TC2 known issue, you cannot perform restore by a logical log number.

Sybase

- 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 StorageWorks EVA 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 HP StorageWorks EVA, 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.
- When HP StorageWorks EVA is used as a VSS hardware provider, the option `Snapshot Type` is ignored by the provider.

  Workaround: Use the EVA configuration tool to select the desired type of a shadow copy, for example snapshot, vsnap, or snapclone.

- When HP StorageWorks EVA is used as a VSS Hardware Provider, sometimes VSSBAR reports that shadow copies creation was started, and then the EVA provider consumes 99% of the CPU and becomes unresponsive. The session cannot be aborted.

  Workaround: None. To abort the backup session and lower the CPU usage, proceed as follows:

  1. Stop the provider service using Service Manager.
  2. If the service cannot be stopped, terminate its process using Task Manager.
  3. Stop the VSS and VDS services. Delete the VSS Snapshot Database. To locate the VSS Snapshot Database files, use Registry Editor to determine values of the following registry keys:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     BackupRestore\FilesNotToBackup\VSS Service DB
     ```

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     BackupRestore\FilesNotToBackup\VSS Service Alternate
     DB.
     ```

  4. Connect to the management appliance, identify the shadow copies (if any) and delete them.
  5. Start the backup once again. If the same error persists, repeat the procedure and restart the system.

- The hardware shadow copy provider may fail with an error similar to the following:

  ```
  INFO: HardwareProvider::LocateLuns() - Failed.INFO:
  HSV_ElementMgr::enableAccess() - FAILED errorMsg =
  '\Hosts\VSSQA\levstik:Api The presented unit already exists.
  Command ignored' cellName = 'EVA-4 (Kolosej)' unitID =
  '1f200710b4080560ff4e0100001001000000e54e' unitName =
  \Virtual Disks\VSSQA\Levstik\LevstikExch7\CPQHWP-3f38d17d
  LUN ID = '21'
  ```

  Workaround: None. To clean up the system, restart the provider, delete the provider information from the VSS Snapshot Database on the backup server, and delete the snapshots on EVA.

  To get the provider ID, run the command `vssadmin list providers`. To locate the VSS Snapshot Database files, use the registry editor to determine the value of the following registry keys:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  BackupRestore\FilesNotToBackup\VSS Service DB
  ```

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  BackupRestore\FilesNotToBackup\VSS Service Alternate DB
  ```

- On Solaris systems, if an HP StorageWorks Disk Array XP split-mirror backup session is started with the GUI option **Leave the backup system enabled** selected or the CLI option `leave_enabled_bs` specified, and the `SSEA_MOUNT_PATH` `omnirc` variable is changed after the session is finished, the next split-mirror backup or split-mirror restore session for the same mount point will fail.

  Workaround: Manually unmount the volume from the old backup system mount point and restart the session.

Volume Shadow Copy Service

- The following MSDE writer components cannot be restored while the SQL server is online: `master`, `model`, and `msdb`.
- When restoring the MSDE writer data while the SQL server is offline, the session completes with an error message similar to the following:

  ```
  [Major] From: OB2BAR@computer.company.com "MSVSSW" Time:
  8/7/2003 1:49:49 PMComponent 'master' reported:
  'CSqlRestor::PrepareToRestore failed with HRESULT =
  0x8000ffff'.
  ```

  Workaround: None. The problem may be resolved in a future Microsoft Windows Server 2003 Service Pack.
- When restoring the MSDE writer data while the SQL server is offline, the restore completes with an error message similar to the following:

  ```
  [Major] From: OB2BAR@concord.ipr2.hermes "MSVSSW" Time:
  8/7/2003 1:49:49 PM Component 'master' reported:
  'CSqlRestor::PrepareToRestore failed with HRESULT =
  0x8000ffff'.
  ```

  Workaround: None. The problem may be resolved in a future Microsoft Windows Server 2003 Service Pack.
- 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.
- On Enterprise Virtual Array, 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.

- During a VSS transportable backup the following error is reported by the VSSBAR on the backup system:

  ```
  Import failed
  ```

  If the backup system is inspected afterwards, the snapshots are actually visible as new disks in Device Manager, as well as in Disk Manager. In the Disk Manager window the volumes may even be visible together with the volume labels, but the Windows `mountvol` command does neither detect nor show them. All subsequent backup sessions fail.

  Workaround: Delete the VSS Snapshot Database on the backup system and restart the system. To locate the VSS Snapshot Database files, use Registry Editor to determine the value of the following registry keys:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  BackupRestore\FilesNotToBackup\VSS Service DB
  ```

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  BackupRestore\FilesNotToBackup\VSS Service Alternate DB
  ```

- On Disk Array XP, if a large number of LUNs or LDEVs is configured, for example more than 2,000, and all of them are visible to the hardware provider, the backup or instant recovery session may fail and report the following:

  ```
  [Major] Failed to resolve volume: STORAGE#Volume#...
  ```

  The hardware provider is resolving the volumes too slowly and is causing timeouts in the Data Protector agent.

  Workaround: Reconfigure the disk array so that the number of LDEVs the provider will detect is reduced (for example to 512 or less), thereby improving its performance. This can be done by creating several Storage Management Logical Partitions (SLPRs) or by zoning the ports on the Fibre Channel switch.

- On Disk Array XP 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 Disk Array XP.

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

Non-Data Protector issues related to reporting

- While using Microsoft Outlook XP or 2003, 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. This problem also occurs if you install the latest security update for Microsoft Outlook 2000 or 98 (Microsoft Knowledge Base article IDs: Q262617, Q267319, Q262700). 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 2000 or 98, see the Microsoft web page http://support.microsoft.com/kb/263296. For Microsoft Outlook XP or 2003, 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 Windows 2000 and newer versions and is the default MAPI handler on these 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 on how to configure SMTP on Microsoft Exchange Serve systemr, 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)**.

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 that the `SHMMAX` value is set to a higher value.

- 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.
- When connecting a Windows 2000 Data Protector GUI client to a Cell Manager, the following error may be reported:

  ```
  You do not have access to any Data Protector functionality
  ...
  ```

  The issue might be that the system name (including the domain suffix) is set at two places on Windows 2000 systems. You have to ensure that the fully qualified domain names in the (**system properties** > **Computer Name** > **Change** > **More** > **Primary DNS suffix**...) and (**local area connection properties** > **Internet Protocol (TCP/IP)** > **Properties** > **Advanced** > **DNS** > **DNS suffix**...) settings on the client are identical and are the same as the system names (including their DNS suffix) defined in the Data Protector **User Context**.
- 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 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 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 which will be backed up.

- If a FAT32 boot partition exists on a Windows 2000, 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 2000, Windows XP, or Windows Server 2003 system to create the ISO image.

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 Java GUI Server or 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.
- 300–425 MB of disk space + approximately 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.

Requirements for viewing online Help on the Data Protector Cell Manager are the same as on Data Protector clients. See "Client system requirements" on page 112.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

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.
- 300–425 MB of disk space + approximately 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.

Requirements for viewing online Help on the Data Protector Cell Manager are the same as on Data Protector clients. See "Client system requirements" on page 112.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

On systems running Windows 2000 or 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 2000 systems, Service Pack 3 or later must be installed.
- On Windows XP Professional systems, Service Pack 1 must be installed.
- 190 MB of disk space + approximately 2% of planned data to be backed up (for use by the IDB)
- `2 × size_of_the_biggest_package_to_be_installed + 5MB` of disk space needed on system drive

For viewing online Help on the Data Protector Cell Manager, Microsoft Internet Explorer 6.0 or newer version is required.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

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 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 A.06.10.

For viewing online Help on the Data Protector Cell Manager, Microsoft Internet Explorer 6.0 or newer version is required.

For the Java GUI Client on Windows Server 2003 systems, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

For the Java GUI Client on Windows Server 2008 systems, BEA JRockit 5.0 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

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.

- 300–425 MB of disk space + approximately 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.

Requirements for viewing online Help on the Data Protector Cell Manager are the same as on Data Protector clients. See "Client system requirements" on page 112.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

Operating systems supported by HP AutoPass

The following Windows operating systems are supported by HP AutoPass:

- Windows 2000
- Windows XP
- Windows Server 2003 (32–bit)
- Windows Vista (32–bit)
- Windows Server 2008 (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)

Solaris and 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

- 750 MB of disk space

Requirements for viewing online Help on the Data Protector Installation Server are the same as on Data Protector clients. See "Client system requirements" on page 112.

On systems running Solaris

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 750 MB of disk space

Requirements for viewing online Help on the Data Protector Installation Server are the same as on Data Protector clients. See "Client system requirements" on page 112.

On systems running Windows 2000 or Windows XP

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM (Windows 2000 Professional)
- 250 MB of disk space
- On Windows 2000 systems, Service Pack 3 or later must be installed.
- On Windows XP Professional systems, Service Pack 1 must be installed.

For viewing online Help on the Data Protector Installation Server, Microsoft Internet Explorer 6.0 or newer version is required.

On systems running Windows Server 2003 or Windows Server 2008

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 250 MB of disk space
- On Windows Server 2008 systems, administrative privileges are required to install Data Protector A.06.10.
- On Windows Server 2008 systems, you must configure the user whose credentials will be used during remote installation.

For viewing online Help on the Data Protector Installation Server, Microsoft Internet Explorer 6.0 or newer version is required.

For the Java GUI Client on Windows Server 2003 systems, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

For the Java GUI Client on Windows Server 2008 systems, BEA JRockit 5.0 1.5_06 or newer update (for example, 1.5_07) is required.

On systems running Linux

The Installation Server must meet the following minimum requirements:

- 64 MB of RAM
- 800 MB of disk space

Requirements for viewing online Help on the Data Protector Installation Server are the same as on Data Protector clients. See "Client system requirements" on page 112.

Client system requirements

On systems running UNIX

The prerequisite for remote installation of the Data Protector client is the following:

- The `inetd` daemon must be up and running on the remote client system.

The prerequisite for viewing online Help on the Data Protector client is the following:

- A web browser that is able to run under the same account as Data Protector must be installed on the client system:
  - On HP-UX, the Mozilla web browser is supported. HP recommends using Mozilla 1.7, but you can also use any other Mozilla version that is officially supported on this platform. For a list of supported Mozilla versions and their installation packages, see the web site http://www.hp.com/products1/unix/java/mozilla/index.html.
  - On Solaris, Mozilla 1.7, Netscape 7.0, and Netscape Navigator 4.7x are supported. HP recommends using Mozilla 1.7. You can download it at http://www.sun.com/software/solaris/browser/index.xml and http://www.mozilla.org/releases/#1.7.12.
  - On Linux, Mozilla 1.7 is supported. You can download it at http://www.mozilla.org/releases/#1.7.12.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

Disk space and RAM requirements for Data Protector UNIX clients

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

Client system component	RAM (MB)	Disk space (MB)
Java GUI	512 (1,000 recommended)	40 (60 recommended)
Disk Agent	64 (recommended 128)	10
Media Agent	64 (recommended 128)	20
Integration modules	64 (recommended 128)	20
English Documentation & 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, page 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.

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 systems running Windows

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

- On Microsoft Windows 2000 systems, Service Pack 2 must be installed.
- On Microsoft Windows XP Professional systems, Service Pack 1 must be installed.
- On Microsoft Windows 2003 systems, Service Pack 1 must be installed.

For viewing online Help on the Data Protector client, Microsoft Internet Explorer 6.0 or newer version is required.

For Java GUI Client, Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) is required.

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

Client system component	**RAM (MB)**	**Disk space (MB)**
Original GUI	256[1]	150[2]
Java GUI[3]	512 (1,000 recommended)	40 (60 recommended)
Disk Agent	64 (recommended 128)	10
Media Agent	64 (recommended 128)	20
Integration modules	64 (recommended 128)	20

Client system component	RAM (MB)	Disk space (MB)
English Documentation & 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 1,000 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, page file or other applications.

Newer Windows operating systems and service packs

Windows XP Service Pack 2, Windows Server 2003 Service Pack 1, Windows Vista, 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 web reporting

Java Runtime Environment (JRE) 1.5.0_06 or newer update (for example, 1.5.0_07) must be installed on the system and enabled in the Web browser. The supported browsers are Netscape Navigator 4.7.x, Netscape 7.x, Mozilla 1.7 and Microsoft Internet Explorer 6.0 or later.

You can download a JRE plug-in for Internet Explorer and Netscape Navigator browsers at http://java.sun.com/products/plugin/.

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 HP-UX DVD-ROM or Installation Server installation CD-ROM and import it to the Cell Manager using automated procedure.

For the installation procedure see the *HP Data Protector installation and licensing guide*.

MPE/iX, Novell NetWare, and HP OpenVMS clients can be installed locally. Remote installation is not supported.

Upgrade

The procedures for upgrading to Data Protector A.06.10 from Data Protector A.05.10, A.05.50, and A.06.00 are 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.05.10, and then upgrade to Data Protector A.06.10 following the procedures in the *HP Data Protector installation and licensing guide*.

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

UI-Proxy — 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 or http://www.software.hp.com/SUPPORT_PLUS/qpk.html 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
SP0312-11.11 (or later)	GOLDQPK11i	Current patch bundle for HP-UX 11.11
SP0312-11.11 (or later)	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
PHSS_32864 or PHSS_37516	s700, s800	ld(1) and linker tools cumulative patch
PHKL_33390	s700, s800	LVM Cumulative Patch; LVM OLR; SLVM 16 Node
PHKL_34534	s700, s800	vPar, callout, abstime, sync perf, wakeup

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

Patch name	Hardware platform	Description
PHCO_27408	s700, s800	LVM commands cumulative patch
PHKL_26785	s700, s800	SCSI Tape (stape) cumulative patch
Use latest	s700, s800	MC/ServiceGuard patches for the version you use
PHSS_33033	s700, s800	ld(1) and linker tools cumulative 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.

[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	QPKBASE	Current patch bundle for HP-UX 11.31

MPE/iX system patches required by Data Protector

Operating system	Description
MPE/iX 6.5 system	PowerPatch I, TurboSTORE/iX's patch MPELXG2A (C.65.13)
MPE/iX 7.0 system	PowerPatch I

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

Operating system version	Patch	Description
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

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.

Patches required by Data Protector for using the HP Integrated Archive Platform (IAP) integration

Before using the integration, check for the latest available patches.

SUSE Linux Enterprise Server system patches required by Data Protector

Use the latest recommended system patches provided by SUSE.

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 in Data Protector A.06.10

The relevant version information regarding supported platforms is in the support matrices. The information in this chapter is provided for your convenience but may be not 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 A.06.10:

- HP-UX 11.0

Obsolete client platforms

The following Data Protector client platforms are no longer supported in Data Protector A.06.10:

- Solaris 7.0
- Tru64 5.0A, 5.1, 5.1A
- SCO OpenServer 5.0.6, 5.0.7

Obsolete integrations

The following integrations are no longer supported in Data Protector A.06.10

- Lotus Notes/Domino Server R5
- VMware ESX Server 2.x (scripting solution)

Obsolete original Data Protector GUI

The original Data Protector GUI is no longer supported on UNIX and Solaris systems. It remains supported on Windows systems.

8 Data Protector documentation

Documentation set

Other documents and online Help provide related information.

Guides

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

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

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

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

- *HP Data Protector concepts guide*

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

- *HP Data Protector installation and licensing guide*

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

- *HP Data Protector troubleshooting guide*

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

- *HP Data Protector disaster recovery guide*

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

- *HP Data Protector integration guides*

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

  - *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*

    This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server, Microsoft SQL Server, and Volume Shadow Copy Service.

  - *HP Data Protector integration guide for Oracle and SAP*

    This guide describes the integrations of Data Protector with Oracle, SAP R3, and SAP DB/MaxDB.

  - *HP Data Protector integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino*

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

  - *HP Data Protector integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server*

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

- *HP Data Protector integration guide for HP Service Information Portal*

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

- *HP Data Protector integration guide for HP Reporter*

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

- *HP Data Protector integration guide for HP Operations Manager for UNIX*

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

- *HP Data Protector integration guide for HP Operations Manager for Windows*

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

- *HP Data Protector integration guide for HP Performance Manager and HP Performance Agent*

  This guide provides information about how to monitor and manage the health and performance of the Data Protector environment with HP Performance Manager (PM) and HP Performance Agent (PA) on Windows, HP-UX, Solaris, and Linux.

- *HP Data Protector zero downtime backup concepts guide*

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

- *HP Data Protector zero downtime backup administrator's guide*

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

- *HP Data Protector zero downtime backup integration guide*

  This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases. The guide also describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.

- *HP Data Protector MPE/iX system user guide*

  This guide describes how to configure MPE/iX clients and how to back up and restore MPE/iX data.

- *HP Data Protector Media Operations user's guide*

  This guide provides tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.

- *HP Data Protector product announcements, software notes, and references*

  This guide gives a description of new features of HP Data Protector A.06.10. It also provides information on supported configurations (devices, platforms and online database integrations, SAN, and ZDB), required patches, and limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at http://www.hp.com/support/manuals.

- *HP Data Protector product announcements, software notes, and references for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal*

  This guide fulfills a similar function for the listed integrations.

- *HP Data Protector Media Operations product announcements, software notes, and references*

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector command line interface reference*

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

Online Help

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

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

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

Documentation map

Abbreviations

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

Abbreviation	Guide
CLI	Command line interface reference

Abbreviation	Guide
Concepts	Concepts guide
DR	Disaster recovery guide
GS	Getting started guide
Help	Online Help
IG-IBM	Integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service
IG-O/S	Integration guide for Oracle and SAP
IG-OMU	Integration guide for HP Operations Manager for UNIX
IG-OMW	Integration guide for HP Operations Manager for Windows
IG-PM/PA	Integration guide for HP Performance Manager and HP Performance Agent
IG-Report	Integration guide for HP Reporter
IG-SIP	Integration guide for HP Service Information Portal
IG-Var	Integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server
Install	Installation and licensing guide
MO GS	Media Operations getting started guide
MO RN	Media Operations product announcements, software notes, and references
MO UG	Media Operations user guide
MPE/iX	MPE/iX system user guide

Abbreviation	Guide
PA	Product announcements, software notes, and references
Trouble	Troubleshooting guide
ZDB Admin	ZDB administrator's guide
ZDB Concept	ZDB concepts guide
ZDB IG	ZDB integration guide

Map

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

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

Integrations

Look in these guides for details of the following integrations:

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

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

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

Localization

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

- *HP Data Protector getting started guide*
- *HP Data Protector product announcements, software notes, and references*
- *HP Data Protector installation and licensing guide*
- *HP Data Protector concepts guide*
- *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*
- *HP Data Protector integration guide for Oracle and SAP*
- *HP Data Protector zero downtime backup concepts guide*
- *HP Data Protector troubleshooting guide*
- *HP Data Protector disaster recovery guide*
- *online Help*

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

- *HP Data Protector getting started guide*
- *HP Data Protector installation and licensing guide*
- *HP Data Protector concepts guide*
- *HP Data Protector zero downtime backup concepts guide*
- *online Help*

Errata

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

- The Data Protector documentation at the time of the release. See General errata.
- The localized versions of the documents. See Localization specific errata.

General errata

This section contains updates to the Data Protector documentation not included in the Data Protector documentation at the time of the release.

Disaster recovery guide

The Microsoft Windows Automated Installation Kit 1.1. is properly listed as a prerequisite for both, the Enhance Automated Disaster Recover (EADR) and One Button Disaster Recovery (OBDR). However, the link to the Microsoft download page is missing:

http://www.microsoft.com/downloads/details.aspx?FamilyID=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=en

Localization specific errata

This section includes updates of the Data Protector documentation that are not included in the localized versions of the documents.

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, such as new recognized issues and workarounds, or limitations that were not included in the localized versions of the documents.

Important updates include among others:

- Updated DCBF limitations.
- Updated VMware Virtual Infrastructure limitations.
- Updated known Data Protector issues with the disk array integrations (HP StorageWorks Disk Array XP agent).
- A known issue when restarting a failed remote UNIX client installation.
- A known issue when starting interactive backup in the Data Protector Java GUI.
- A limitation for upgrading from 32-bit Windows to 64-bit Windows Server 2008 was removed and a workaround for the migration procedure was added.

Additional minor last minute updates may be included in the version of the document that is published on the DVD or Web.

Data Protector Backup to HP Integrated Archiving Platform (IAP)

In the Japanese *HP Data Protector product announcements, software notes, and references*, the section "Data Protector Backup to HP Integrated Archiving Platform (IAP)" describing the new IAP feature is missing from the chapter "Product features and benefits".

The section is available in the Japanese online Help.

Improved description of backup session ownership

Details about backup session ownership were updated in the *HP Data Protector concepts guide* and online Help to resolve an ambiguous definition.

Updates in the HP Data Protector installation and licensing guide

- A note about required licenses for the VSS integration was updated in Appendix A to resolve ambiguous wording.
- The prerequisites for installing the Microsoft SQL Server 2005 client were updated, including a corrected Web address.
- Prerequisites for installing the cluster-aware Cell Manager from a shared disk were updated.
- A note about installing Cell Manager on Solaris 10 was updated in the chapter "Installing Data Protector on your network", section "Installing a UNIX Cell Manager", "Installation procedure".

Updated Microsoft SQL Server 2000/2005 documentation

Microsoft SQL Server 2000/2005 backup and restore specifics were updated in the *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service* guide.

Updated online Help

- The task topic "Testing the Drive Cleaning Configuration" was updated with a new directory structure on other UNIX systems.
- The topic "F1 Help: Lotus Notes/Domino Server Restore Devices" was updated with new name of the GUI option **Save device mapping**.

- The navigation topic “Standard Object Copy Tasks” was updated with a new limitation regarding backup sessions that are run interactively from the Backup wizard in the GUI.

A List of enhancements and issues fixed in Data Protector A.06.10

The list of enhancements and fixed defects can be found on any Data Protector installation DVD-ROM in the `\DOCS` directory, in the file `DP61_Enhancements_Resolved_Defects.pdf`.

B Filename conversion performance

This appendix shows the impact of file name conversion in the IDB on backup performance.

HP Data Protector installation and licensing guide provides more information on conversion of file names in the IDB. Among other aspects, it covers the following:

- Which cell configurations require file name conversion in the IDB.
- How to skip the conversion and what are the consequences.
- Which other conversion options are available and what is their purpose.

Filename conversion performance on a UNIX Cell Manager

The following table presents the results of the backup performance measurements during conversion and non-conversion backups. The figures help you estimate the time needed for the first full backup of Windows clients after the upgrade to Data Protector A.06.10.

Filesystem conditions on the Windows client			Data Protector A.05.10		Data Protector A.06.10			
Total no. of files (in 1,000)	No. of files per dir.	% of non-ASCII file names	1st backup duration	2nd backup duration	Conversion backup			2nd backup duration
					Duration	Time per 1,000 files	Ratio to the 1st Data Protector A.05.10 backup (%)	
150	10	100	09:01	06:58	08:46	3.51	97	05:05
		50	09:51	07:08	06:43	2.68	68	05:27
		10	09:42	06:59	05:26	2.17	56	05:17
		0	10:11	07:06	05:23	2.15	53	05:24
150	1,000	100	06:08	03:46	51:09	20.46	835	02:39
		50	05:01	03:44	25:11	10.08	501	02:32
		10	05:02	03:48	07:39	3.06	152	02:39
		0	05:25	03:50	02:35	1.03	48	02:40
2,000	100,000	50	1:46:38	1:35:10	16:30:10	29.01	929	1:09:19
		10	2:10:03	1:40:59	14:19:27	25.18	661	1:10:23
		0	2:18:29	1:47:17	2:03:28	3.62	89	1:40:44

The tests were performed on systems with the following hardware and operating system configuration:

	Hardware model	CPU	RAM	Operating system
Cell Manager	HP 9000/800/ A500-5X	PA 8600 CPU Module 3.1, 550 MHz	1024 MB	HP-UX B.11.11 U
Client	PC	Intel Pentium III, 1266 MHz	1024 MB	Windows 2000 with SP4 (Japanese)

The client and Cell Manager were the only systems connected in an isolated 100 Mb network.

The time needed to perform the conversion, which is done during the first full client backup (**conversion backup**) on a client per client basis, depends on several factors. Typical directory structures on clients (less than 200 directories), should not significantly extend the conversion backup time. However, the conversion backup of large directories and numerous file names containing non-ASCII characters can take considerably more time than a subsequent full backup of the same client.

The impact on the duration of the conversion backup depends on the following factors:

- The percentage of file names in the IDB originating from Windows clients. Bigger percentage means longer conversion backup. File names from non-Windows clients do not need a conversion and thus do not prolong the conversion backup time.
- The number of files in directories:
  - Medium size directories (containing more than 200 files): the impact depends on the number of files in a directory and the percentage of file names that need to be converted. The conversion backup will take longer than a normal full backup with Data Protector A.05.10 if there are many files in a directory with more than 10% of the file names containing non-ASCII characters.
  - Large directories (containing more than 10.000 files): the conversion backup takes significantly longer than a normal full backup with Data Protector A.05.10 if there are large directories on the system containing non-ASCII characters.

NOTE:

After the conversion backup all subsequent backups are faster than comparable backups performed with Data Protector A.05.10.

Filename conversion performance on a Windows Cell Manager

Raw estimates for the duration of IDB conversion of file names for your specific configuration is displayed at the end of the upgrade process on a Windows Cell Manager. The impact on duration of the IDB conversion mainly depends on the number of file names in the IDB originating from non-Windows clients.