

Archive Backup System and Data Protector: Leading OpenVMS Backup Solutions

Deepa R Shenoy, OpenVMS Engineering



Archive Backup System and Data Protector: Leading OpenVMS Backup Solutions	1
Introduction	2
Product introduction	2
Product components	3
Product installation	4
Types of backup	5
Backup to disk	6
Backup to tape	6
Media and device management	6
Disaster situation handling	8
Product features compared	9
Reporting	11
For more information	11
References	11

Introduction

Backup strategy is a plan that aids the user to recognize the backup solution most suitable to the site. There is no particular backup strategy that can be termed as a solution for all the customer sites. Therefore, according to the site requirement, a backup strategy should be framed which would aid in choosing the best suitable backup solution.

Various Enterprise backup solutions are available for OpenVMS platform catering to wide spectrum of customer requirements/needs. HP Archive Backup System (ABS) is a backup software solution which is suitable for OpenVMS prominent environment. Whereas, HP Data Protector (DP) is a versatile product for the needs of today's heterogeneous enterprise environments including OpenVMS.

This paper will delve upon some of the useful features from both the products. The document does not compare the products to prove one solution better than the other, but merely lists the features of ABS and DP. The user needs to decide which solution best suits their environment and this feature listing may aid the user with the decision.

Product introduction

Archive Backup System

ABS is primarily developed for OpenVMS Operating System users. Apart from Open VMS files, ABS can be used to backup and restore TRU64 UNIX and Windows files. ABS supports HP devices that are qualified by OpenVMS Operating System. It also supports SUN libraries with the help of another product DCSC (Digital Cartridge Server Component). ABS manages small environments and can also be scaled to manage backups in enterprise environments.

The latest major version release of ABS is Version 4.5 (1200). After this, another patch or remedial release of ABS V4.5 (1201) was done which contains fixes to some of the problems reported in ABS. For more information about the latest release of ABS, see the ABS website:
<http://h71000.www7.hp.com/openvms/storage/abspage.html>

Data Protector (DP)

Data Protector is designed to backup or restore data for heterogeneous enterprise environment. DP supports backup of a multitude of file systems available in the market which includes OpenVMS files backup. DP works with both HP and non-HP hardware (Tape Libraries) available. DP offers easy central management via GUI, that is, from a single system; all DP client systems can be accessed.

The latest version of DP is A.06.11. For more information on this DP release, see the [DP Documents Page](#).

Product components

Archive Backup System

Following are some of the ABS components listed below:

1. *Media and Device Management System (MDMS)* is an integrated component of ABS. MDMS performs several functions for ABS:
 - Database Services: All ABS and MDMS objects are maintained by MDMS.
 - User Interface: MDMS manages both the Command-line Interface (CLI) and Graphical User Interface (GUI).
 - Security Service: MDMS manages access rights/privileges for both ABS and MDMS objects.
 - Media Management Services: MDMS takes care of Media Management for ABS. MDMS specifically supports a set of objects (termed as MDMS objects) for media management.
 - For Network backups, MDMS works in conjunction with RDF (remote Device Facility). RDF works only with Decnet and Decnet over IP. RDF does not work with TCPIP.
2. A *Catalog* is a set of files created to preserve the history information of backups done using ABS. Catalogs contain the records of data saved using ABS. Those records enable you to locate and restore data that was saved using ABS. ABS refers to the catalog for information during data restoration; this process is termed as “Catalog Lookup” in ABS.
3. *ABS objects* define physical locations of backed-up data on tape/disk, the criteria under which save and restore requests are performed that is the time and schedule of backups/restores.
MDMS Objects define physical resources such as node, jukebox, drives, tape (cartridge/volume). It also defines logical resources such as media type, pool, magazine, and group.
4. *MDMS Domain* – Each OpenVMS node participating runs a generic process called MDMS\$SERVER. A MDMS\$SERVER process which has access to the database is termed as the *DB server*. Any other MDMS\$SERVER process is served by the DBServer in the same MDMS domain, this is termed as MDMS client. All nodes communicating with the same database server belong to the same MDMS domain. Each MDMS domain has its own database. Typically you have only one MDMS domain in your network.
5. A *backup agent* is the utility that performs the actual data movement operation.
OpenVMS systems - the backup agents are the OpenVMS BACKUP Utility
RDB backup - backup agent is RMU Backup Utility
UNIX and Windows clients - backup agent is GTAR (tape archiver).

For more information on each of these components, see the ABS Guide to Operations:

http://h71000.www7.hp.com/doc/abs044_opr_gd.pdf

Data Protector (DP)

Following are some of the DP components explained below:

1. *DP Cell: Cell Manager* is a central control point where the Core Data Protector software is installed. The *Cell Manager* allows you to add systems to be backed up; these systems become DP Client systems to the *Cell Manager* and are considered a part of the Cell.

2. DP Client systems must have *Disk Agents* (or Backup Agents) installed. The Disk Agent reads or writes data from a disk on the system and sends or receives data from a *Media Agent*. The Disk Agent is also installed on the *Cell Manager*, thus allowing you to back up data on the *Cell Manager*, the DP configuration, and the IDB.
3. A *backup device* (Tape devices) can be connected to either the *Cell Manager* or any other client system. A system in the CELL which has a Backup device must have the Media Agent installed. The *Media Agent* reads or writes data from media on the backup device and sends or receives data from the disk agent.
4. The *IDB (DP Internal Database)* is a database located on the *Cell Manager*, which maintains history information regarding what data is backed up, on which media it resides, the result of backup, restore, object copy, object consolidation, object verification, and media management sessions, and what devices and libraries are configured IDB.
5. The *Manager of Managers (MoM)* allows a user to manage large enterprises with multiple cells. MoM is a single control point from which many cells can be managed. MoM facilitates sharing of devices between CELLS and aids in report generation starting from a single cell basis or for the entire enterprise (all CELLS under MoM).

Product installation

ABS Installation on OpenVMS

A single kit is provided for ABS installation on both OpenVMS Alpha and OpenVMS Integrity server Operating System. The ABS installation is done with the help of VMSINSTAL utility.

ABS needs to be manually installed on all OpenVMS systems identified as part of the backup strategy. Installation of ABS OpenVMS server or client software is determined by the OpenVMS node name that you enter during the installation procedure. There is no separate kit provided for an ABS OpenVMS client.

ABS allows a user to install the product in a standard mode, where ABS decides the host disk and product components to be installed. It also allows user to control the installation in the custom mode. The user can decide the disk, where ABS product must be installed. Along with this, the user can also choose the optional ABS components to be installed such as RDF, MDMS GUI, NT kits and so on. For information about ABS installation instructions, see the ABS Guide to Installation:

http://h71000.www7.hp.com/doc/abs044_ins_gd.pdf

ABS Installation on different OS

ABS GTAR component needs to be installed on TRU64 UNIX systems and on Windows an ABS service needs to be installed and started up so that ABS can include the systems as clients. Apart from this, the Windows and TRU64 UNIX clients will need to be authorized on the OpenVMS system. For information about ABS installation instructions, in the ABS Guide to Installation:

http://h71000.www7.hp.com/doc/abs044_ins_gd.pdf

DP Installation on OpenVMS

The cell manager can be installed on the Windows, HP-UX, Solaris, or Linux platform. However, on an OpenVMS system, only a DP client may be installed. This paper discusses about the DP installation on OpenVMS. For more information, see the DP Installation Guide:

<http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c01631236/c01631236.pdf>

DP OpenVMS client software needs to be manually installed on all OpenVMS systems identified as part of the backup strategy. You can install the Data Protector Disk Agent, General Media Agent, and the User Interface (command-line interface only) on systems running OpenVMS Alpha V7.3-2 or OpenVMS Integrity servers V8.2-1. You can also install the Oracle Integration component on systems running OpenVMS Alpha V7.3-2 or later. DP provides a PCSI file which needs to be installed manually on the OpenVMS system. The DP installation is done with the help of PCSI utility (PRODUCT INSTALL). The product can only be installed on the system disk in "SYS\$COMMON:[OMNI]".

DP allows the user to install the product in a default mode, where all the components get installed by default. DP allows the user to control the installation in the Custom mode. The user decides the DP components that should be installed on that OpenVMS system. A step by step procedure is available in the DP Installation Guide under the section "Local installation of HP OpenVMS clients".

DP Installation on different OS

The Installation Server (IS) is a separate system or a Cell Manager component that contains the Data Protector Software repository used for remote client installations. This Data Protector feature greatly simplifies the software installation process for remote clients. Installation Server cannot be used to install DP on OpenVMS systems. Installation Server is supported for UNIX and Windows Operating Systems. Client software can be installed remotely on HP-UX, Solaris, Sinix, Linux, AIX, and other supported UNIX operating systems from an installation server for UNIX. Client software can be distributed to any Windows system, except Windows XP HE, from an installation server for Windows.

Types of backup

Full/Incremental backups

A full backup saves all the files selected for backup in a file system.

During a full backup, ABS performs an image backup on OpenVMS file system. There is no extra step required to make the system disk bootable during a restore.

On OpenVMS, DP has no equivalent functionality like the native OpenVMS image backup using BACKUP/IMAGE or BACKUP/PHYSICAL. 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.

For ABS and DP, an incremental backup saves only those files that have changed since the last full or incremental backup.

Synthetic/Virtual full backup

This concept is unique to DP and ABS does not support these backup types. A synthetic full backup data set is consolidated from a full backup (residing on disk/tape) and incremental backups (residing on disk). This eliminates the need for the backup server to be involved during the backup hence speeding up the backup time.

If all the backups, full and incremental, are written to the same file library that uses distributed file media format, virtual full backups may be used. This solution uses pointers to consolidate data rather than copy the data. As a result, the consolidation takes less time and avoids unnecessary duplication of data.

DP does not support zero downtime backup (ZDB) or split mirror backups on OpenVMS.

Backup to disk

The resultant data-set of a backup operation needs to be stored on a separate medium that can be later transported to a different location or maintained as a near-line option. There are two types of media that the backup solutions use, they are disk medium (generally used as near-line option) and tape medium (best medium for maintaining offline data backups).

Both ABS and DP supports backups to disk. The user can specify the disk on which the data is to be stored. But ABS does not support disk-to-disk backups. DP, on the other hand, supports disk-to-disk backups. These disk-to-disk backups include:

- Disk Staging: Data from backup server is intermediately done to a STAGED DISK and later copied to a Tape device.
- Synthetic Full backup and Virtual Full Backups are examples of disk to disk backups

To aid disk-to-disk backups, DP has the following disk-based devices:

- Standalone file device - It consists of a single slot to which data can be backed up.
- File jukebox device - The file jukebox device consists of multiple slots to which data can be backed up. Each slot in the file jukebox device has a maximum capacity of 2 TB. This requires a 2-stages configuration.
- File library device - The file library device has multiple slots called file depots to which data can be backed up. Each file depot has a maximum capacity of up to 2 TB. This requires a single stage configuration.

Backup to tape

The traditional and highly used medium is tape or cartridge. Tapes are used as they are reliable, cheaper than disk and can be easily transported from one place to another.

Data format on Tape:

ABS and DP both support backup to tapes. ABS stores backed up data on a tape in a SAVESET format which is understandable to native VMS BACKUP utility. DP stores data on a tape in its own format understandable only to DP.

Media and device management

Tapes are a highly used medium for backups and tapes require media management to be done. Both products offer excellent media management facilities. These media managers provide common functionalities such as:

- Media pools: Logically grouping media to enable user to categorize media efficiently.
- Media details: Maintaining useful information about the media at all times, especially, expiration time of data on medium, availability of media etc.
- Media rotation policies: Automatically rotating tapes without need for manual intervention.
- Providing barcode support on large Libraries, and so on.

There are also other functionalities of media management where the products differ; some of them are explained below:

1. Device streaming

If the rate at which data is written by the drive to the tape is less than or equal to the rate at which data is being provided to the device by the application, then the device is said to be 'streaming'. Device streaming is also dependent on other factors, such as, network load and the

block size of the data written to the device. In DP, the device streaming is accomplished by starting multiple Disk Agents for each Media Agent that writes data to the device. If properly configured, this setup leads to increased backup performance.

ABS does not include a device streaming mechanism.

2. Load balancing

In both ABS and DP, multiple devices might be used for backup so that data is backed up in parallel to multiple devices (drives/media).

But DP also supports load balancing that is, DP automatically balances the load or usage of devices for evenly using the devices. Load balancing provides optimum performance:

- When large number of objects needs to be backed up
- A library with several drives are available
- Good network connection is available

ABS does not take up the responsibility of load balancing

3. Media condition maintenance

When ABS/MDMS encounters an error with media, it automatically avoids the usage of that media for further backups. The user can later query the MDMS database to know the media which are not in use due to media errors. The user now has to manually check the problem with media and fix the errors. MDMS does not explicitly maintain the media condition based on the usage or age of media.

DP calculates the state of the media using "Media Condition Factors". In DP, media is set to have any one of the three states: GOOD, FAIR, OR POOR. The state is calculated on the basis of:

- Number of Overwrites - Once the medium has more than the threshold number of overwrites, it is marked as poor.
- Media Age - The age of a medium is calculated as the number of months that have elapsed since you formatted, or initialized, the medium. Once a medium is older than the threshold number of months, it is marked as poor.
- Device Errors - If a device fails during a backup, the medium used for the backup in this device is marked as poor.

Data Protector fully supports TapeAlert 2.0 (a device monitoring utility that provides error/warning alerts and suggest a course of action), as long as the connected device also provides this functionality.

4. Cleaning tape handling

In ABS, the cleaning tapes have to be manually loaded, whereas DP provides automatic cleaning for most devices using a cleaning tape. This medium will be used automatically by DP if a dirty drive event from the device is detected. For devices without a cleaning tape, dirty drive detection will cause a cleaning request to be displayed on the session monitor window. The operator must clean the device manually.

5. Tape size

DP is capable of displaying the approximate size of tape that remains to be filled. ABS does not maintain any information on the size of tape.

6. Virtual tape libraries (VTL)

The Backup window is further reduced and managing the backups has become easier and faster with VTLs. ABS supports HP VLS (Virtual Library System) and HP D2D (Disk 2 Disk device) for OpenVMS files backup but DP supports only HP VLS for OpenVMS file systems.

The latest technology that these Virtual Tape Libraries have come up with is called “[deduplication](#)”. Currently (as on June 2010) VLS does not support deduplication of OpenVMS file systems. But D2D device supports deduplication of OpenVMS file system. ABS works well with deduplication of OpenVMS files along with the D2D device.

Disaster situation handling

Natural disaster

When a natural disaster occurs at the business data centre site, a remote data centre site needs to be setup immediately for business continuity. A disaster recovery from the last backed up data of business data centre needs to be performed at this stage.

Disaster Recovery of an OpenVMS system is an uncomplicated procedure in ABS and requires:

1. The image backup of the system disk on OpenVMS node.
2. Backup of important information such as, ABS Catalog files and MDMS database files.

Image backups create bootable disk at the time of restore. Image backups also automatically defragment the disk when a restore is attempted, which mostly results in improved performance. After the restore is complete, ABS and MDMS files are restored to make sure that the ABS/MDMS database is consistent and exact state is restored.

For more information, see Section 7 in the *ABS Guide to Operations*:

http://h71000.www7.hp.com/doc/abs044_opr_gd.pdf

Disaster Recovery of an OpenVMS system in DP requires:

1. A complete restore of files on disk (disk will be non-bootable).
2. The OpenVMS system needs to be booted from a different disk (another bootable disk).
3. With the help of WRITEBOOT, write the boot block on the disk to make the disk “bootable”.

User error

An uncommon situation where a user has accidentally deleted the history information (Catalog of ABS/ IDB of DP) of a backup solution.

For ABS, the following prevention and remedy techniques can be used:

Prevention: ABS recommends you to always backup the catalogs and also set appropriate VMS ACLs and MDMS ACLs to protect catalog data.

Remedy: ABS provides a mechanism to rebuild lost catalogs with a method called “Cataloging Existing Saveset”. Here the Customer can refer the backup logs and find out the tape name where the data is placed. ABS will rebuild the history data for all the SAVESETS present on this tape. ABS does not support this mechanism for encrypted SAVESETS.

For DP, the following prevention and remedy techniques can be used:

Prevention: The following features allow and restrict access to Data Protector Cells

- Data Protector user accounts
- Data Protector user groups
- Data Protector user rights

Remedy: DP provides a mechanism to rebuild the history information in IDB by a technique named "Importing catalog information from media".

Application server node crash

A common situation seen is when the Application server node crashes, there are several client nodes waiting to get serviced by the Application server. In ABS, a user can nominate more than one node (all nodes must have access to the DB disk to be the application Server (MDMS DB server). At a point in time, one node can act as application server. If the current Application Server (DB server) node crashes, automatically ABS takes care of the situation and fails over to the next nominated node in the list. When the crashed node comes up, it takes up the role of a client system getting serviced by the new Application Server.

In DP, all Cell Manager Operations are always available since Data Protector Services are defined as cluster resources within the cluster and are automatically restarted when a failover occurs.

Media hardware error

A common situation where the backup application has previously stored data on a tape, while using the tape for a subsequent backup, a media hardware error is encountered.

If the previously stored data is critical data and needs to be restored, ABS allows a user to restore data stored on tape till the point where tape allows access (until the failure point).

DP maintains media state and places the tape in POOR state after it experiences problems with the hardware. DP does not restore any data from media in POOR state.

Product features compared

Sl. No.	Features	Archive Backup System (ABS)	Data Protector (DP)
1	GUI	GUI on Windows is provided.	GUI on Windows, HP-UX, SOLARIS, UNIX platforms is provided.
2	CLI	ABS/MDMS CLI on OVMS provided	DP CLI on OVMS provided
3	Backup technique	Uses the native BACKUP Utility to perform backups	Issues QIO call over a network to backup data
4	Archiving (After Backup, the original data on disk is deleted)	Supported	Not supported
5	Data specification details	Include Specification (VMS style File specification is supported by ABS)	Backup Specification (Any file specifications that are passed to the CLI must conform to a UNIX-style syntax: /disk/directory1/directory2/filename.ext.n)
6	Network Backups	ABS supports Network Backups via RDF (Remote Device facility). But RDF works with Decnet and Decnet over IP only.	DP supports network backups (TCPIP).

7	Frequency of Backups	User can choose from a predefined frequency sets or define a desired custom frequency.	User can choose from a predefined frequency sets or define a desired custom frequency.
8	Schedulers	ABS supports usage of 1. MDMS internal scheduler 2. External scheduler (CA Scheduler)	DP Scheduler
9	Track data backed-up using	Catalogs	IDB (Resides on Cell Manager)
10	Procedure for cleaning up the above mentioned catalog/IDB	Catalog cleanup (configurable)	Purging policies (configurable)
11	Centralized repository (catalog/IDB)	Catalogs are generally node-specific and not centralized. But this is configurable.	IDB is centralized and optimized.
12	Maximum size of catalogs/IDB	Generally if the catalog size grows beyond 5 GB, ABS performance problems may be seen.	Generally if the IDB size grows beyond 16 GB, DP performance problems may be seen.
13	Catalog Segment on Tape	ABS does not store a Catalog segment on Tape.	DP stores a Catalog segment on tape with every data segment.
14	RDB support for OpenVMS	RDB V7.2 supported	Not qualified to work with RDB
15	Oracle support for OpenVMS	Oracle 10gR2 supported	Oracle 10gR2 supported
16	Hardware Encryption for OpenVMS files	ABS V4.5 also has been qualified with the latest MSL LTO-4 encryption kit that provides key management functionality for LTO-4 drives in an MSL G3 library.	Hardware encryption is not supported for OpenVMS files. For Oracle integration backup/restore AES algorithm (256 bit) for encryption is supported.
17	Software Encryption for OpenVMS files	Software Encryption feature was introduced in ABS starting from ABS V4.5 and ABS supplies its own key management facility.	Software Encryption of OpenVMS files backup is currently not available on DP.
18	Compression of OpenVMS Files	This feature is currently not available	With DP, compression of OpenVMS files is achievable.
19	Tape to tape copy	This feature is currently not available	With DP, tape to tape copy is supported which in turn helps in tape consolidation. I.e. copying discrete data on different tapes to a single tape.

20	ODS 2 and ODS 5 file system Support	Both are supported	Both are supported
21	Network	ABS can be configured to work with DECNET or TCPIP or both.	DP works with TCPIP alone for OpenVMS Clients
22	Multiple NIC card support	ABS does not support Multiple NIC card configuration.	DP supports a Multiple NIC card configuration.
23	Hardware Support details	Link for Device Matrix	Link for Device Support Matrix
24	Hard Links On Open VMS	ABS takes care of the hard links.	The Backup POSIX hard links as files option is not available on OpenVMS.
25	XFC Cache thrashing	ABS takes care not to thrash the XFC cache on OpenVMS	DP does not take care of avoiding the XFC cache and thus thrashes the XFC cache when a backup is performed.

Reporting

If the backup or restore occurs in a lights-off mode, for any backup solution, you can generate a report. These reports help you or the administrators to verify the status of backups. Both ABS and DP generates report and sends the notification.

In ABS, event notifications can be set for

1. Backup/restore status
2. Media (if number of usable media < threshold defined by user)

DP provides a highly customizable and flexible tool which provides a rich set of built-in reports. A user can choose from pre-configured reports and specify desired parameters for these reports. You can also select report formats (for example, ASCII, HTML). Some of the reports are as follows:

- Inventory/Status Reports
- Capacity Utilization Reports
- Problem Reports
- Event Based Reports

For more information

- [ABS Document Set](#)
- [DP Document Set](#)

References

- [ABS Document Set](#)
- [DP Document Set](#)
- Article on "[abs-dataprotector_differences](#)" by Ted Saul