Enterprise Backup and Restore technology and solutions

LESSON VII

HP Data Protector
Overview and Concepts
Part III

Veselin Petrunov
Backup and Restore team / Deep Technical Support

HP Bulgaria Global Delivery Hub
Global Operations Center
November, 2013

HP Data Protector

Overview and Concepts

Part III

Veselin Petrunov / November 2013

Contents

Part III

4. The Data Protector internal database

1. About the IDB / The IDB on the Windows/Unix Cell manger and in the MOM environment
2. IDB architecture
3. IDB operation
    1. During backup/restore/object copying or object consolidation/object verification
    2. Exporting media/Removing the detail catalog
    3. Filenames/File versions purge
4. Overview of IDB management
5. IDB growth and performance
    1. Key IDB growth and performance factors
    2. IDB growth and performance: key tunable parameters
    3. IDB size estimation

5. Service management

1. Overview
2. Data Protector and service management
3. Native Data Protector functionality
4. Integration with HP Operations Manager software
5. SNMP traps
6. The monitor
7. Reporting and notification
8. Event logging and notification/Data Protector log files/Windows application log
9. Java-based online reporting
10. Data Protector checking and maintenance mechanism
11. Central management, distributed environment
12. Using the data provided by Data Protector

HP Data Protector

About the IDB

What is the Data Protector Internal Database (IDB)?

The IDB is an embedded database, located on the Cell Manager, which keeps 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.

Why is the IDB used?

The information stored in the IDB enables the following:

- Fast and convenient restore: The information stored in the IDB enables you to quickly find the media required for a restore, and therefore makes the restore much faster. It also offers you the convenience of being able to browse for files and directories to be restored.
- Backup management: The information stored in the IDB enables you to verify how backups were done. You can also configure various reports using the Data Protector reporting functionality.
- Media management: The information stored in the IDB enables to allocate media during backup, object copy, and object consolidation sessions, track media attributes, group media in different media pools, and track media locations in tape libraries.
- Encryption/decryption management: The information stored in the IDB enables Data Protector to allocate encryption keys for encrypted backup or object copy sessions, and to supply the decryption key required for the restore of encrypted backup objects.

HP Data Protector

The IDB on the Windows Cell Manager

IDB location

The IDB on the Windows Cell Manager is located in the directory

*Data_Protector_program_data**db40* (Windows Server 2008 and later) or

*Data_Protector_home**db40* (older Windows systems).

IDB format

The IDB on the Windows Cell Manager stores all text information in Unicode, double-byte format. Therefore, the IDB grows slightly faster than the IDB on the UNIX Cell Manager, which stores information in the ASCII format.

The Unicode format allows for full support of filenames and messages localized to other languages.

HP Data Protector

The IDB on the UNIX Cell Manager

IDB location

The IDB on the UNIX Cell Manager is located in the */var/opt/omni/server/db40* directory.

IDB format

The IDB on the HP-UX and Solaris Cell Manager stores all text information in ASCII single- and multi-byte formats.

The ASCII format limits the support of filenames and messages localized to other languages. When backing up files with filenames in a double-byte format, such as Unicode, the filenames are converted to the ASCII format and may not appear correctly in the Data Protector user interface. However, the files and filenames will be restored correctly.

HP Data Protector

The IDB in the Manager-of-Managers environment

In the Manager-of-Managers (MoM) environment, you can use the Centralized Media Management Database (CMMDB), which allows you to share devices and media across several cells.

HP Data Protector

IDB architecture

The IDB consists of the following parts:

- MMDB (Media Management Database)
- CDB (Catalog Database), divided into two parts: filenames and other CDB records
- DCBF (Detail Catalog Binary Files)
- SMBF (Session Messages Binary Files)
- SIBF (Serverless Integrations Binary Files for the NDMP integration)
- Encryption Keystore

Each of the IDB parts stores certain specific Data Protector information (records), influences IDB size and growth in different ways, and is located in a separate directory on the Cell Manager.

For robustness considerations and recommendations for optimizing robustness by relocating some IDB directories.

HP Data Protector

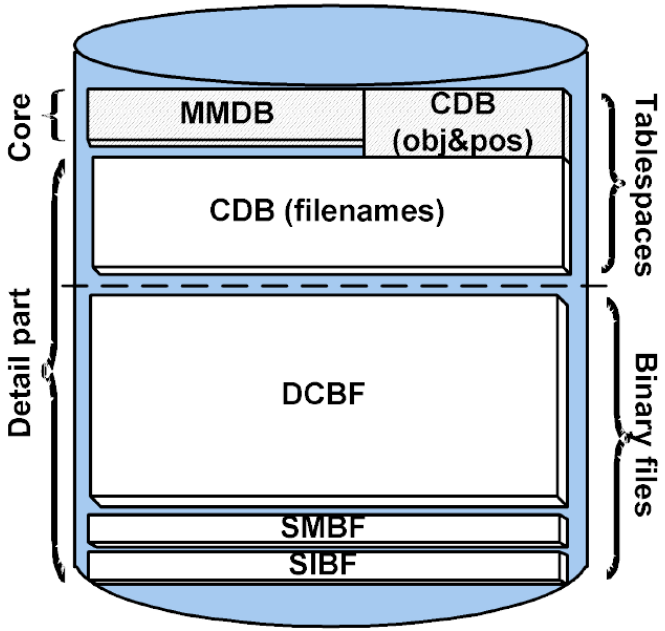
IDB architecture

Underlying technology

The MMDB and CDB parts are implemented using an embedded database consisting of tablespaces. This database is controlled by the RDS database server process. All changes to the MMDB and CDB are updated using transaction logs. The transaction logs are stored in the *db40\logfiles\syslog* directory. The CDB (objects and positions) and the MMDB parts represent the core part of the IDB.

The DCBF, SMBF and SIBF parts of the IDB consist of binary files. Updates are direct (no transactions).

IDB parts



HP Data Protector

Media Management Database (MMDB)

MMDB records

The Media Management Database stores information about the following:

- Configured devices, libraries, library drives, and slots
- Data Protector media
- Configured media pools and media magazines

MMDB size and growth

The MMDB does not grow very big in size. The largest portion of the MMDB is typically occupied by information about the Data Protector media. Space consumption is in the range of 30 MB.

MMDB location

The MMDB is located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\datafiles\mmdb*
- On older Windows systems: *Data_Protector_home\db40\datafiles\mmdb*
- On UNIX systems: */var/opt/omni/server/db40/datafiles/mmdb*

HP Data Protector

Catalog Database (CDB)

CDB records

The Catalog Database stores information about the following:

- Backup, restore, object copy, object consolidation, object verification, and media management sessions. This is a copy of the information sent to the Data Protector Monitor window.
- Backed up objects, their versions, and object copies. In the case of encrypted object versions, key identifiers (KeyID-StoreID) are also stored.
- Positions of backed up objects on media. For each backed up object, Data Protector stores information about the media and data segments used for the backup. The same is done for object copies and object mirrors.
- Pathnames of backed up files (filenames) together with client system names. Filenames are stored only once per client system. The filenames created between backups are added to the CDB.

HP Data Protector

Catalog Database (CDB)

Filename size and growth

The biggest and fastest growing part of the CDB is the filenames part. It typically occupies 20% of the entire database. The growth of the filenames part is proportional to the growth and dynamics of the backup environment, and not to the number of backups.

A file or directory on the HP-UX or Solaris Cell Manager occupies approximately 50-70 bytes, and a file or directory on the Windows Cell Manager occupies 70-100 bytes in the IDB.

Filenames are stored in the *fnames.dat* file and in some other files, depending on the filename length. The maximum size of each of these files is 2 GB. You are notified when one of these files starts running out of space, so that you can add new files to extend the size of the filenames part of the IDB.

Size and growth for CDB (objects and positions)

The CDB records other than filenames occupy a minor share of space in the IDB. Space consumption is in the range of 100 MB for a medium size backup environment.

CDB location

The CDB is located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\datafiles\cdb*
- On older Windows systems: *Data_Protector_home\db40\datafiles\cdb*
- On UNIX systems: */var/opt/omni/server/db40/datafiles/cdb*

HP Data Protector

Detail Catalog Binary Files (DCBF)

DCBF information - The Detail Catalog Binary Files part stores file version information. This is information about backed up files, such as file size, modification time, attributes/protection, and so on.

One DC (Detail Catalog) binary file is created for each Data Protector medium used for backup. When the medium is overwritten, the old binary file is removed and a new one is created.

DCBF size and growth - In an environment where filesystem backups using the Log all option are typical, the DCBF occupies the largest part (typically 80%) of the IDB. To calculate the size of DCBF, use the following formula: *dcbf_file_in_bytes* is approximately *num_of_files_on_tape x 30_bytes*. Logging level and catalog protection can be used to specify what is actually stored in the IDB and for how long.

By default, one DC directory, *db40\dcbf*, is configured for the DC binary files. Its default maximum size is 16 GB. You can create more DC directories and have them on different disks on the Cell Manager, thus extending IDB size. The maximum number of supported directories per cell is 50.

DCBF location - By default, the DCBF is located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\dcbf* and *Data_Protector_home\db40\dcbf* for older
- On UNIX systems: */var/opt/omni/server/db40/dcbf*

Consider the disk space on the Cell Manager and relocate the DC directory, if necessary. You can create more DC directories and locate them to different disks. Create several DC directories only if the number of media/DC binary files grows very large (several thousand) or if you have space problems.

HP Data Protector

Session Messages Binary Files (SMBF)

SMBF records

The Session Messages Binary Files stores session messages generated during any Data Protector sessions. One binary file is created per session. The files are grouped by year and month.

SMBF size and growth

The SMBF size depends on the following:

- The number of sessions performed, since one binary file is created per session.
- The number of messages in a session. One session message occupies approximately 200 bytes on Windows and 130 bytes on UNIX systems. You can change the amount of messages displayed when backup, restore, and media management operations are performed by specifying the Report level option. This also influences the amount of messages stored in the IDB.

SMBF location

The SMBF is located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\msg* and *Data_Protector_home\db40\msg* for older version
- On UNIX systems: */var/opt/omni/server/db40/msg*

You can relocate the directory by editing the SessionMessageDir global option.

HP Data Protector

Serverless Integrations Binary Files (SIBF)

SIBF records

The Serverless Integrations Binary Files stores raw NDMP restore data. This data is necessary for restore NDMP objects.

SIBF size and growth

The SIBF does not grow very big in size. For NDMP backups, the SMBF grows proportionally to the number of objects backed up.

Approximately 3 kB are used for each backed up object.

SIBF location

The SIBF is located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\meta*
- On older Windows systems: *Data_Protector_home\db40\meta*
- On UNIX systems: */var/opt/omni/server/db40/meta*

HP Data Protector

Encryption keystore and catalog files

All the keys created, either manually or automatically, during encrypted backups are stored in a keystore. The keys can also be used for object copy, object verification, and restore sessions. In the case of hardware encryption, they can also be used for object consolidation sessions.

In the case of software encryption, the key identifiers (each consisting of a KeyID and a StoreID) are mapped to the object versions encrypted. This mapping is stored in the catalog database. Every objects in a medium can have different (software) encryption keys.

For hardware encryption, the key identifiers are mapped to medium ID and these mappings are stored in a catalog file. This file contains the information required to allow an encrypted medium to be exported to another cell.

Keystore location

The keystore is located in the following directory:

• On Windows Server 2008 +: *Data_Protector_program_data\db40\keystore* and *Data_Protector_home\db40\keystore* for older

• On UNIX systems: */var/opt/omni/server/db40/keystore*

Catalog file location

The catalog files are located in the following directory:

- On Windows Server 2008 +: *Data_Protector_program_data\db40\keystore\catalog*
- On older Windows systems: *Data_Protector_home\db40\keystore\catalog*
- On UNIX systems: */var/opt/omni/server/db40/keystore/catalog*

HP Data Protector

IDB operation

During backup

When a backup session is started, a session record is created in the IDB. Also, for each object and each object mirror in the session, an object version record is created. All these records are stored in the CDB and have several attributes. If software encryption has been requested for the backup, the active encryption keys for the entities involved (hosts) are obtained from the keystore, used for the backup, and the key identifiers (KeyID-StoreID) is linked to the object versions and included in the CDB records. The mappings of the hosts to the KeyID-StoreIDs are also stored in a catalog in the keystore.

The Backup Session Manager updates media during a backup. All media records are stored in the MMDB and are allocated for a backup depending on policies. If the media involved are in drives for which hardware encryption has been requested, first the active encryption keys for the entities (media) are obtained from the keystore. The mappings of the media to the KeyID-StoreIDs

are recorded in a catalog in the keystore and also written to the media.

When a data segment is written to the tape and then to a catalog segment, then for each object version that was part of this data segment, a media position record is stored in the CDB. In addition, the catalog is stored in the DC (Detail Catalog) binary file. One DC binary file is maintained per Data Protector medium. A DC binary file is named MediumID_TimeStamp.dat. If a medium is overwritten during a backup, its old DC binary file is removed and a new one is created.

All session messages generated during backups are stored in session messages binary files (the SMBF part).

If transaction logging is enabled, an IDB backup removes old transaction logs and starts creating new ones, which are necessary for an IDB recovery.

HP Data Protector

IDB operation

During object copying or object consolidation

During an object copy or object consolidation session, the same run as during a backup and a restore session. Basically, data is read from source media as if it was restored and written to target media as if it was backed up. An object copy or object consolidation session has the same effect on the IDB operation as backup and restore. This does not apply for object consolidation with software encryption, since this is not supported.

During object verification

During an object verification session, the same database processes run as during a restore session. Basically, data is read from the source media, as if it were being restored, and is sent to the host disk agent(s) where the verification is performed. An object verification session has the same effect on the IDB operation as a restore session. All session messages generated during verification sessions are stored in session messages binary files.

HP Data Protector

IDB operation

Exporting media

When a medium is exported, if it contains encrypted information, the relevant keys are exported from the keystore to a .csv file on the Cell Manager. This file is required for successful import of the medium in another cell.

In addition, several items are removed.

Key-export directory location

The encryption key-export directory location is as follows:

- On Windows Server 2008 +: *Data_Protector_program_data\Config\Server\export\keys*
- On older Windows systems: *Data_Protector_home\Config\Server\export\keys*
- On UNIX systems: */var/opt/omni/server/export/keys*

Removed items - The following are removed:

- All the media position records from that medium are removed from the CDB.
- All objects and object copies that now have no positions on any other media are removed from the CDB part.
- Obsolete sessions (whose media have either been overwritten or exported) older than 30 days are removed (this can be modified using the KeepSession variable from the global option file). Session messages of such sessions are also removed.
- The medium record is removed from the MMDB part, and the DC binary file for that medium is removed from the DCBF.

HP Data Protector

IDB operation

Removing the detail catalog

When the detail catalog is removed for a specific medium, its DC binary file is removed. The same result is achieved by removing the catalog protection for all object versions and object copies on that medium (the next daily maintenance of DC binary files removes the binary file). All other records stay in the CDB and MMDB and it is possible to run a restore from such media (however, browsing is not possible).

Filenames purge

DC binary files show whether a given file is backed up on a related medium or not, but the filenames are actually stored in the CDB. A filename is considered “used” if it is marked as backed up in at least one DC binary file. Over time, it can happen that a large number of filenames are not used. To remove such filenames, Data Protector scans all DC binary files and then removes unused filenames.

File versions purge

When the catalog protection of all object versions stored on a specific medium expires, automatic daily maintenance of DC binary files removes the respective binary file.

HP Data Protector

Overview of IDB management

IDB configuration

One of the most important steps in setting up your Data Protector backup environment is to configure the IDB. The initial configuration enables you to set your internal policies regarding IDB size, the location of IDB directories, the IDB backup necessary in case of IDB corruption or a disaster, and the configuration of IDB reports and notifications.

IDB maintenance

Once you configure the IDB, its maintenance is reduced to a minimum, mainly acting on notifications and reports.

IDB recovery

An IDB recovery is needed if some of the IDB files are missing or corrupted. The recovery procedure depends on the level of corruption.

HP Data Protector

IDB growth and performance

For proper IDB configuration and maintenance it is necessary to understand the key factors that influence the IDB growth and performance, as well as the key tunable parameters that you can adapt to your needs, and thus handle the growth and performance of the IDB as efficiently as possible.

HP Data Protector

IDB growth and performance

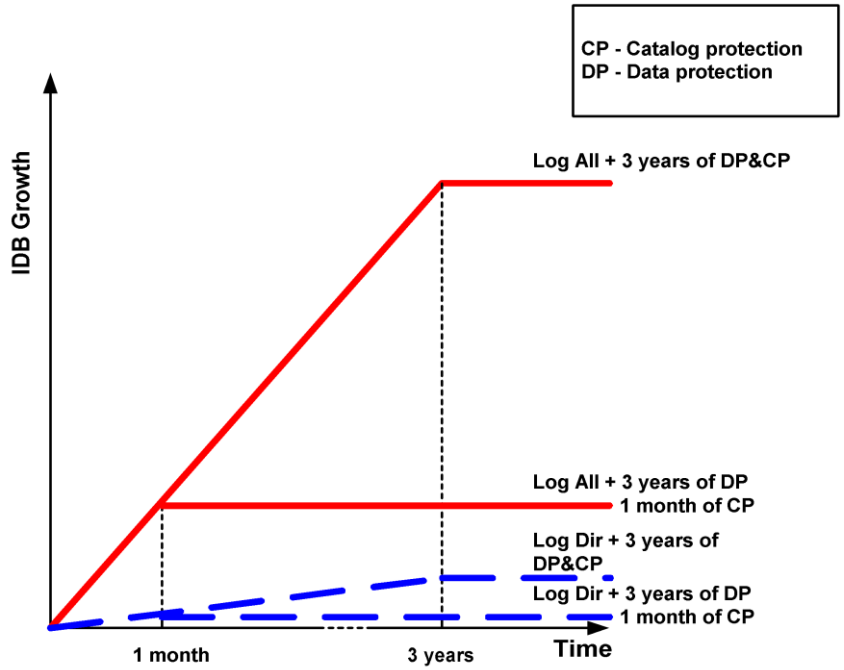
Key IDB growth and performance factors - The key factors for IDB growth and performance are the following:

- Logging level settings. Logging level defines the amount of detail written to the IDB during backup.
- Catalog protection settings. Catalog protection determines how long the information about backed up data is available in the IDB.
- Number of backed up files. Data Protector keeps track of each file and each version of that file. Different backup types impact the IDB differently.
- Number of backups - The more often you perform a backup, the more information is stored in the IDB.
- Filesystem dynamics - The number of files created and removed between backups can have a significant impact on the growth of the filenames part of the IDB. The *Report on System Dynamics* gives you information about the system dynamics.
- Growth of your backup environment. The number of systems being backed up in the cell influences the IDB growth.
- Character encoding used for your filenames (applicable for UNIX only). Depending on the filename encoding, a character in the filename can take up from one to three bytes in the IDB. Shift-JIS encoded filenames, for example, take up to three bytes in the IDB, while pure ASCII filenames take up only one byte. The character encoding is relevant for growth of filename part of IDB on UNIX (on Windows, all characters take up two bytes in the IDB).
- Number of object copies and object mirrors. The more object copies and object mirrors you create, the more information is stored in the IDB. For object copies and object mirrors, the IDB stores the same information as for backed up objects, except for filenames.

HP Data Protector

IDB growth and performance: key tunable parameters

The logging level and catalog protection are the main factors of the IDB growth and performance. Their impact on the IDB depends on the settings you use.



HP Data Protector

Logging level as an IDB key tunable parameter

What is logging level?

Logging level determines the amount of details about backed up files and directories written to the IDB. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels that control the amount of details about files and directories written to the IDB:

Log All	Logs all detailed information about backed up files and directories (names, versions, and attributes).
Log Files	Logs all detailed information about backed up files and directories (names and versions). This represents approximately 30% of all detailed information about backed up files and directories.
Log Directories	Logs all detailed information about backed up directories (names, versions, and attributes). This represents approximately 10% of all detailed information about backed up files and directories.
No Log	No information about backed up files and directories is logged to the IDB.

The different settings influence the IDB growth, the backup speed, and the convenience of browsing for data to be restored.

Impact on performance

The logging level defines the amount of data written to the IDB during a backup. This also influences the IDB speed, and therefore the backup process.

HP Data Protector

Logging level and restore

Logging level and browsing for restore

Changing the level of stored information affects your ability to browse files using the Data Protector GUI during a restore. If the *No Log* option is set, browsing is not possible; if the *Log Directories* option is set, browsing of directories is possible; if the *Log Files* option is set, full browsing is possible but file attributes (size, creation, and modification dates and so on) are not displayed.

Regardless of the logging level set, it is always possible to restore your data:

- Instead of browsing for your data, you can always manually select a file to restore (if you know the name of the file).
- You can retrieve information about backed up data from the media.

Logging level and restore speed

The restore speed is approximately the same when the *Log All*, *Log Directories*, or *Log Files* options are set.

If the *No Log* option is set, the restore speed can be slower when restoring single files. This is because Data Protector has to read all data from the beginning of an object before finding a file to be restored.

In case of a full system restore, the whole object should be read anyway, so the logging level settings do not play an important role.

HP Data Protector

Catalog protection as an IDB key tunable parameter

What is catalog protection?

Catalog protection determines how long the information about backed up data is available in the IDB. This is different from data protection, which determines how long the backed up data is available on the medium itself. If there is no catalog protection, you can still restore your data, but you cannot browse for it in the Data Protector GUI.

Catalog protection is based on the fact that the data stored last is most important and accessed most frequently. Old files are seldom searched for, and therefore it is allowable for their search to take more time.

Expired catalog protection

Once the catalog protection expires, the information is not immediately removed from the IDB. Data Protector removes it automatically once per day. Since the information in the IDB is organized on a per-medium basis, it is removed completely when catalog protection expires for all objects on the medium.

Impact on performance

Catalog protection settings do not have any impact on the backup performance.

Catalog protection and restore

When catalog protection expires, data is restored as if it were backed up using the *No Log* option.

HP Data Protector

IDB size estimation

If you mainly perform filesystem backups, the IDB may, under certain conditions, grow to a significant size (larger than 16 GB). If you perform disk image or online database backups, your IDB will probably not grow beyond 2 GB.

To estimate the size of the IDB use the Internal Database Capacity Planning Tool which is installed as a part of the English Documentation (Guides, Help) component. The installation places the tool to the following location:

- UNIX systems: */opt/omni/doc/C/IDB_capacity_planning.xls*
- Windows systems: *Data_Protector_home\docs\IDB_capacity_planning.xls*

You can also use this tool to estimate the size of the IDB in environments with online databases (Oracle, SAP R/3).

HP Data Protector

The Data Protector internal database

HP Data Protector

Service management

HP Data Protector

Data Protector and service management

Data Protector provides service management supports and can be integrated with service management applications, such as HP Operations Manager for Windows.

Data Protector service management falls into two categories: native (or out-of-the-box) and application integrations. The items in each category are described in more detail later in this chapter.

HP Data Protector

Native Data Protector functionality

- Built-in monitoring of running sessions allows you to instantly react to occurrences in your backup environment.
- The Data Protector built-in notification and reporting engine allows you to receive concise reports as well as immediate alerts in many different formats (such as ASCII, HTML, and spreadsheet compatible format) and delivered in various ways (such as e-mail, SNMP, broadcast (available on Windows only), write to file, and send to external command). As the Data Protector built-in notification engine can send alerts via SNMP, it is possible to integrate virtually any application that can receive SNMP traps.
- Data Protector backup session auditing stores information about all backup tasks that were performed over extended periods for the whole Data Protector cell, and provides this information on demand in an integral and printable fashion for auditing and administrative purposes.
- The integration of Data Protector with HP Operations Manager software allows you to receive alerts from Data Protector on the OM console and have automatic actions performed.
- The Data Protector capability to send major and critical events into the Windows Event Log opens up a variety of interesting integration possibilities.

HP Data Protector

Integration with HP Operations Manager software

Functionality of the HP OM integration

Data Protector integrates with HP Operations Manager software (OM). OM simplifies management of large networks by allowing the operator to monitor and administer the network and the applications from a single point. Once Data Protector is integrated in the OM environment, the network administrator can immediately see if anything is wrong during backup and react upon the information given. Data Protector messages can be displayed in the OM message window.

Functionality of the HP Operations Manager for Windows

The HP Operations Manager for Windows (OMW) provides the following functionality:

- Data Protector writes all major and critical messages that occur during backup, restore or any other operation to the Windows Event Log. HP Operations Manager for Windows (OMW) then uses these events and forwards them to the OMW console, so that an operator can react to them.
- Service monitoring - OMW monitors all Data Protector services running on the Cell Manager as well as any Data Protector client system. In case of failure of any of these services, OMW immediately alerts the operator. OMW can also be configured in such a way that it automatically attempts to restart the failed service.

HP Data Protector

Service management

SNMP traps

SNMP traps allow a Service Management application to receive and process an SNMP trap message when a Data Protector event occurs or when an SNMP trap is sent as a result of Data Protector's checking and maintenance mechanism.

The monitor

The Data Protector monitor is a part of the Data Protector user interface and allows you to supervise and to take corrective action on currently running backup, restore, and media management sessions. Monitoring lets you view all sessions in a cell and shows you detailed messages and the current status of these sessions. In a multi-cell environment, you can view the sessions that run on computer systems in other cells. From the monitor's user interface, you can abort a backup, restore, or media management session or respond to "mount" requests.

If you make use of the Manager-of-Managers, you can monitor sessions of multiple cells simultaneously from one user interface.

HP Data Protector

Reporting and notification

Data Protector reporting represents a powerful, customizable, and flexible tool for managing and planning your backup environment. Data Protector has always had a rich set of built-in reports that system administrators have relied upon to manage Cell Managers. IT Service Providers now can use these same reports to demonstrate data protection SLA compliance. Built-in reports that are especially relevant to service level management include:

- Inventory/Status Reports such as the Clients not Configured for Data Protector report, which contains information about unprotected systems, the Session Specification Schedule report, which lists all scheduled backups, object copy, and object consolidation as well as the List of Pools report, which is a media inventory report.
- Capacity Utilization Reports such as the Licensing report report, which is a Data Protector license utilization report, and the Configured Devices not Used by Data Protector report, which lists devices that are currently not used for backup, object copy, or object consolidation and are consequently available.
- Problem Reports such as the Session Statistics report, which consists of information about failed backup, copy, and consolidation sessions. An administrator can receive an hourly, daily, or weekly E-mail report on failed jobs and the reasons for failure.

HP Data Protector

Reporting and notification

The notification and reporting capabilities that have always been part of the Cell Manager (and that have been extended significantly from earlier versions) also allow you to:

- Choose from numerous pre-configured reports (including, but not limited to, reports such as sessions in a specific time frame, IDB reports, and device usage report)
- Specify your own parameters for those reports (such as time frames, backup, copy, and consolidation specifications, and groups of backups)
- Select from various different output formats (such as ASCII, HTML, and spreadsheet compatible formats)
- Schedule those reports with the Data Protector built-in scheduler
- Trigger report sending based on events (such as device failure, mount requests, and end of sessions)
- Select from many delivery methods used to deliver reports (such as e-mail, SNMP, broadcast (available on Windows only), write to file, and send to external command)

You can combine most of these different formats, delivery methods, schedules, and triggers.

HP Data Protector

Reporting and notification

Reporting and notification examples

- Every morning at 7:00, a report about all backup, copy, and consolidation sessions in the last 24 hours is created and sent by e-mail in the ASCII format to the backup administrator's mailbox. Additionally, the same report is written to a file on your Web server in the HTML format so that others can also access this information.
- In event of a device failure or a mount request, a broadcast message is immediately sent to the backup administrator's Windows workstation, and an external command is triggered, which activates the backup administrator's pager.
- At the end of a backup session, every end user whose system has been backed up receives an e-mail in ASCII format that contains a backup status report.

HP Data Protector

Event logging and notification

The Data Protector Event Log is a central repository of all Data Protector-related notifications. Events that are logged in the Data Protector Event Log are either process-triggered or user-triggered. The Data Protector built-in notification engine sends alerts or activates the Data Protector reporting mechanism based on the log entries. The event log is the information source for SLA-compliance reports in Data Protector or in HP software management applications.

Since the Data Protector built-in notification engine can send alerts via SNMP, virtually any application that can receive SNMP traps can integrate with Data Protector. Integration with HP Operations Manager is an example of SNMP trap-based implementation.

The Event Log is accessible only for Data Protector users in the Admin group and for Data Protector users that are granted the *Reporting and notifications* user rights. You can view or delete all events in the Data Protector Event Log using the Event Log Viewer.

Data Protector log files

Some Service Management applications, such as HP Operations Manager software, allow you to specify when and which log files should be monitored for a specific log entry. If the specified entry is detected in the file, an action can be specified. In OM this is called Log file encapsulation.

You can configure such a Service Management application to monitor Data Protector log files for specific log entries (Data Protector events) and define an action that is to be executed in case a particular Data Protector event is detected.

HP Data Protector

Event logging and notification

Windows application log

Some Service Management applications, such as HP Operations Manager for Windows (OMW), monitor the Windows Application Log.

To enable automatic forwarding of all Data Protector messages and messages about the Data Protector services (if they are stopped) to Windows Application Log, set the *EventLogMessages* variable in the Data Protector global options file to *1*. For more information on the Data Protector global options file, see the HP Data Protector Troubleshooting Guide.

Java-based online reporting

Data Protector comes with a Java-based online reporting capability that lets you configure, run, and print all Data Protector built-in reports, live and interactive. During reporting operations, Data Protector Java reporting directly accesses the Cell Manager to retrieve current data. You can make this Java applet available through a Web server, copy it to the client machine for direct access, or use it locally. Using this facility only requires a supported Web browser; there is no need to have the Data Protector GUI installed on the system. Not only can you use the Java reporting facility to get online access to your reports, but you can also configure your reporting structure through it, such as adding new reports to a schedule or changing a report's parameters.

HP Data Protector

Data Protector checking and maintenance mechanism

Data Protector has a rich automated daily self-check and maintenance mechanism, which improves its operational reliability and predictability. Data Protector's self-check and maintenance tasks include:

- "Not Enough Free Media" check
- "Data Protector License Expiration" check

HP Data Protector

Central management, distributed environment

The Data Protector MoM enables administrators to centrally manage an enterprise environment consisting of several Data Protector Cell Managers. The MoM system administrator performs configuration, media management, monitoring, and status reporting tasks for the whole enterprise from a single console. With MoM, managing many Data Protector Cell Managers is as convenient as managing just one. IT service providers can administer larger clients' environments without adding employees.

HP Data Protector

Using the data provided by Data Protector

Here are some examples of what you can do with the data that Data Protector provides:

- Regular e-mail reports to back up operators, end users, and management (Data Protector built-in reporting with the capability to send e-mails).
- Backup reports written to a Web server to make them available on an on-demand basis (built-in Data Protector reporting with the capability to write HTML).
- Sending major and critical Data Protector events to your network management solution, such as HP Network Node Manager (Data Protector built-in notification engine sending SNMP traps).

Q&A

Thank you