

HP OpenView Data Protector IDB(Internal Database) Management

PART 1

SYSWILL EMS TEAM

JAN 2004

문서 개요

HP OpenView Data Protector 를 운영 하는데 있어서 매우 중요한 역할을 하는 IDB (Internal Database) 에 대한 개념과 주요 특징 및 기능 에 대한 이해를 통해서 보다 안정적이고 편리한 백업 시스템 정책을 구현 하고자 합니다.

본 문서는 Data Protector 5.1 을 기준으로 작성 되었으므로 일부 내용과 파일 경로 등에서 기존 버전의 내용과 약간의 차이가 있을 수 있습니다.

목차

- PART 1 -

1장 IDB 주요 기능 및 특징

2장 Architecture

3장 IDB Maintenance

- PART 2 -

4장 IDB Command

5장 Troubleshooting

6장 기타 :문서 보완

1장. IDB 주요 기능 및 특징

Data Protector Internal Database (IDB) 는 Cell Manager 에 위치 하며 DATA 백업 작업 내역과 미디어 정보를 관리 합니다.

1.1 Scalability

IDB는 소규모의 관리 Point 로 백업 시스템 전반에 걸친 Management 를 가능 하게 합니다.

1.2 Higher Performance

IDB 는 백업서버의 CPU 나 DISK I/O 에 적은 부하만으로 작업 정보에 대한 빠른 입력 속도를 보장 하며 여러대의 백업 대상 혹은 Restore 대상 에 대해서 병렬 작업이 가능 하도록 탁월한 파일시스템 브라우징 기능을 제공 합니다.

1.3 Low Maintenance Requirements

IDB 는 내부 에서 관리되는 모든 백업 정보 에 대해서 효과적인 관리 방안을 제시하며 Report 및 알람 기능을 통해 IDB 관리의 효율성을 제공합니다.

1.4 Backup management

백업이나 복구 시 해당 작업(sessions) 에 대한 내역 들을 저장하여 관리 합니다.

1.5 Media management

백업 작업 시 이용되는 백업 Device 및 Media Pool, Media 속성, Media 순서 등에 대한 정보를 저장 하여 관리 합니다.

1.6 빠르고 편리한 Data Restore

IDB에 백업작업 시 저장된 directory 들이나 나 file 정보를 이용하여 장애발생시 media 안의 restore 대상 DATA 를 신속하고 정확하게 찾아내어 궁극적으로는 보다 빠른 DATA restore 를 제공 합니다.

1.7 IDB 장애 발생시 쉽고 간편한 복구 방법 제공

D:\Womniback\Wbin>omnidbrestore -autorecover
* 기존 IDB 백업 본이 있을 경우에 한해서 실시 가능.

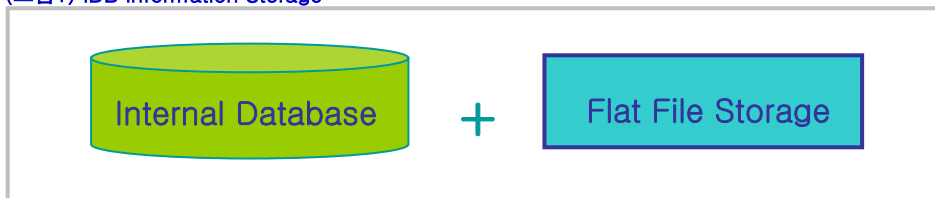
1.8 Automated "online" Migration

OmniBack Version Upgrade 시 /omnidbupgrade utility 를 통해서 DB Migration 기능을 제공.

2장. Architecture

Data Protector 구성 및 운영에 있어서의 주요 정보는 크게 두가지 형태로 저장 되어 지며 그 첫번째가 본 문서에서 주로 설명 하고 있는 IDB 이며 두번째는 일반 파일 형태의 configuration 파일 입니다.

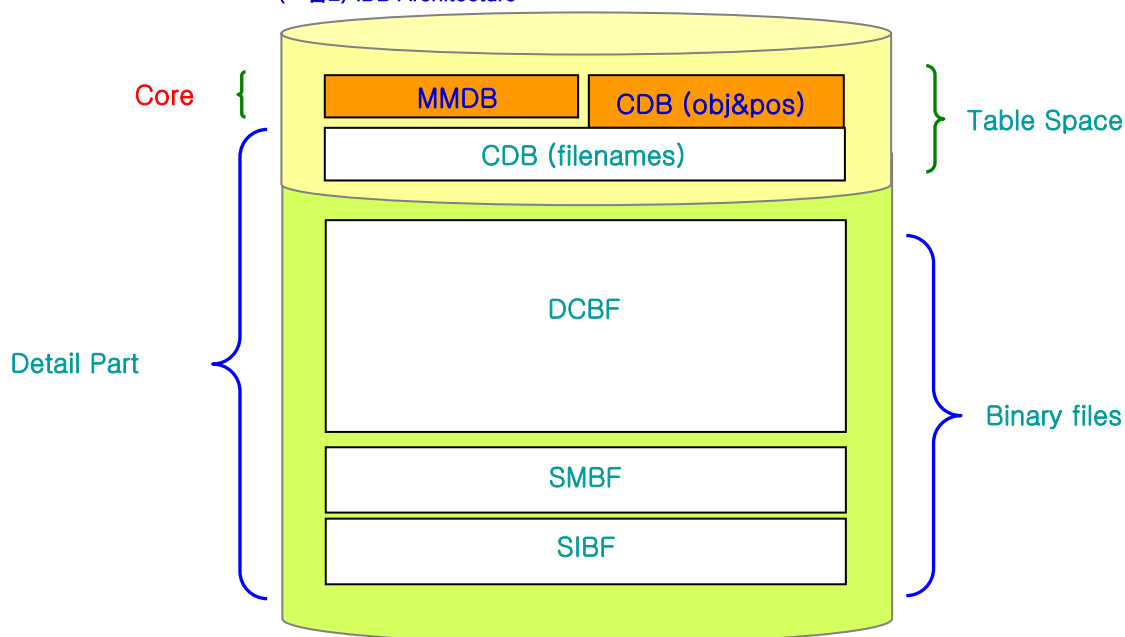
(그림1) IDB Information Storage



(표1) IDB 와 Flat File Storage 비교

구분	IDB	Flat File Storage
TYPE	Raima Velocis	FILE (ASCII)
UNIX 경로	/var/opt/omni/db40	/etc/opt/omni
WIN 경로	Data Protector HomeWdb40	Data Protector HomeWconfig
운영정보	<ul style="list-style-type: none"> • Media management data • Device configuration data • Backup & Restore session data • File catalog data 	<ul style="list-style-type: none"> • User configuration • Backup specifications • Schedules • Cell environment • Report groups • Report schedules • Notifications

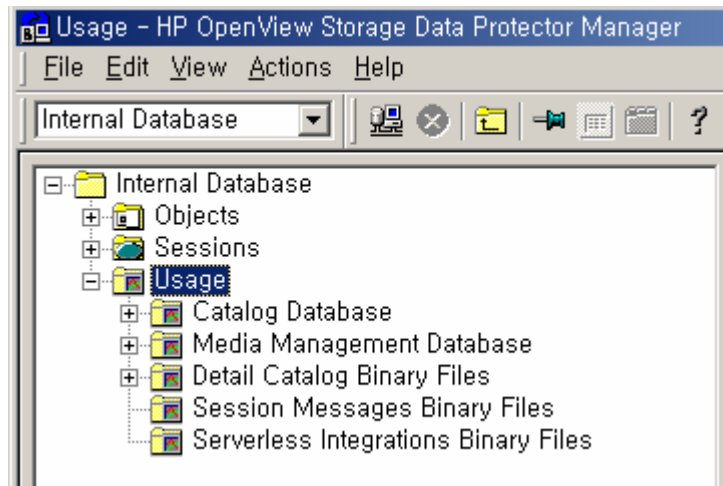
(그림2) IDB Architecture



2.1 IDB 구성

IDB 는 Raima Velocis 타입의 내부 DBMS 에 의해서 콘트롤 되며
 앞 page 의 그림 2 에서 보듯이 **Tablespace** 에 해당 하는 **MMDB, CDB** 와
Binary files 형태로 저장되는 **DCBF, SMBF, SIBF** 영역으로 나뉘어져 있습니다.
 (Tablespace 영역은 RDS(Raima Database Server) service 에 의해서 작업 진행)
 또한 해당 영역은 IDB CORE 부분의 **MMDB** 와 **CDB** (catalog DB) **Detail Part** 의 **CDB(filename)** 와
DCBF, SMBF, SIBF 로 분류 되기도 합니다.

(그림 3)
 Data Protector GUI 에서
 IDB 구성 Display



- **CDB (Catalog Database) :**

백업 작업 시 수반되는 관련 정보를 저장 합니다.
 CDB는 내부적으로는 IDB Core part 에 해당하는 부분과 (objects & positions)
 백업된 DATA 의 개별 Filename 이 저장 되는 부분으로 나뉘어져 있습니다.
 또한 Filename 들에 대한 Table 영역으로 사용되는 물리적인 경로는
 해당 CDB 디렉토리안의 “fnames.dat “ 파일을 이용하며 **최초 2GB** 크기로 설정 돼있습니다.
 fnames.dat 파일은 1회 최소 1M ~ 최대 2GB 씩 추가 할 수 있으며 **TOTAL 32GB 까지**
확장이 가능(solraris CM 은 30 GB 까지) 합니다.
 (IDB maintenance part 에서 상세 설명)

Unix - /var/opt/omni/db40/datafiles/cdb

Windows - <Data Protector Home>Wdb40Wdatafiles/cdb

- Objects (filesystem, DBMS & Application DATA , rawdata ...)
- Object Versions (백업 작업에 따른 시간대별 내역)
- Sessions (백업 & Restore)
- Media positions (media 에 백업된 DATA 의 위치 정보)
- Directory names

- **MMDB** (Media Management Database) :

백업 시스템 운영자는 실제 존재 하는 물리적인 백업 Device (Library & Drive)를 Data Protector 를 이용한 논리적 Device 구성을 통해서 해당 Device 를 제어 하고 사용 하게 되는데 이때 구성되어지는 정보들이 MMDB 영역에 저장 됩니다.

마찬 가지로 Media 와 Media Pool 구성 정보 또한 함께 저장 됩니다.

Unix - /var/opt/omni/db40/datafiles/mmdb

Windows - <Data Protector Home>Wdb40Wdatafiles/mmdb

- **DCBF** (Detail Catalog Binary Files) :

IDB 내에서 DCBF 의 역할은 DATA 백업시의 모든 file Version 및 속성을 보유 하게 됩니다.

file size, modification time, permissions, attributes, etc

Unix - /var/opt/omni/db40/dcbf

Windows - <Data Protector Home>Wdb40Wdcbf

- **SMBF** (Session Messages Binary Files)

Backup & Restore 작업에 대한 Session message 뿐만 아니라 Media format 작업 시에 발생 되는 session message 를 저장 하게 됩니다.

각각의 작업 Session 에서는 그 상황이나 결과에 따라 여러가지 형태로 다양한 message 들이 발생되며 기본값은 “warning” 등급 즉, Data Protector 자체 기준으로 볼때 “warning” 이상의 상황에 대한 모든 메시지를 Dsisplay 하도록 설정 돼있습니다.

해당 메시지 등급은 “Normal”, “Warning”, “Minor”, “Major”, “Critical” 등으로 나누어 지며 “Warning” 이상의 level 에 대해서 선택 설정이 가능 합니다.

Unix - /var/opt/omni/db40/msg

Windows - <Data Protector Home>Wdb40Wmsg

- **SIBF** (Serverless Integrations Binary Files)

Data protector 는 Server-less 형태의 백업 작업을 지원합니다.

즉 별도의 Disk Agent 없이 Network 에서 바로 백업 작업이나 Restore 가 가능한데

대표적으로 NDMP(Network Data Management Protocol) data나 EMC Fastrix data 등에 대한 작업이 해당되며 이때의 Data Protector와의 구성 내용(Intergraton 관계) 를 저장 합니다.

<기타 주요 파일 >

IDB configuration 파일 : Velocis.ini

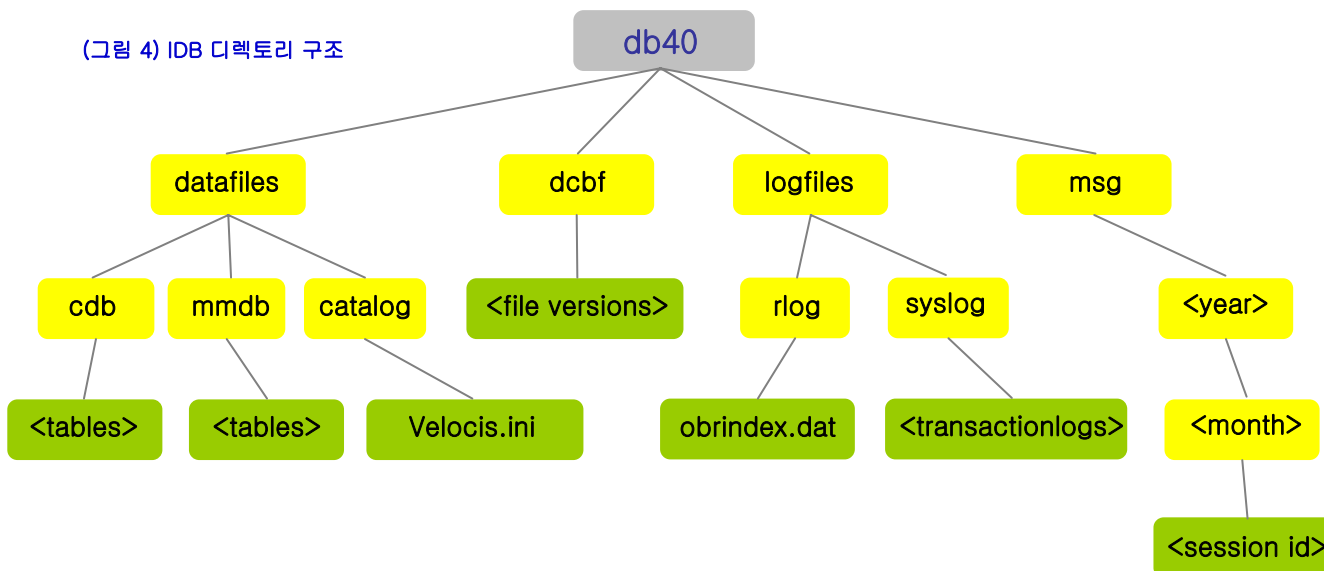
IDB recovery data 파일 : obrindex.dat

IDB transaction log 파일 : 이후 Page 에서 상세 설명

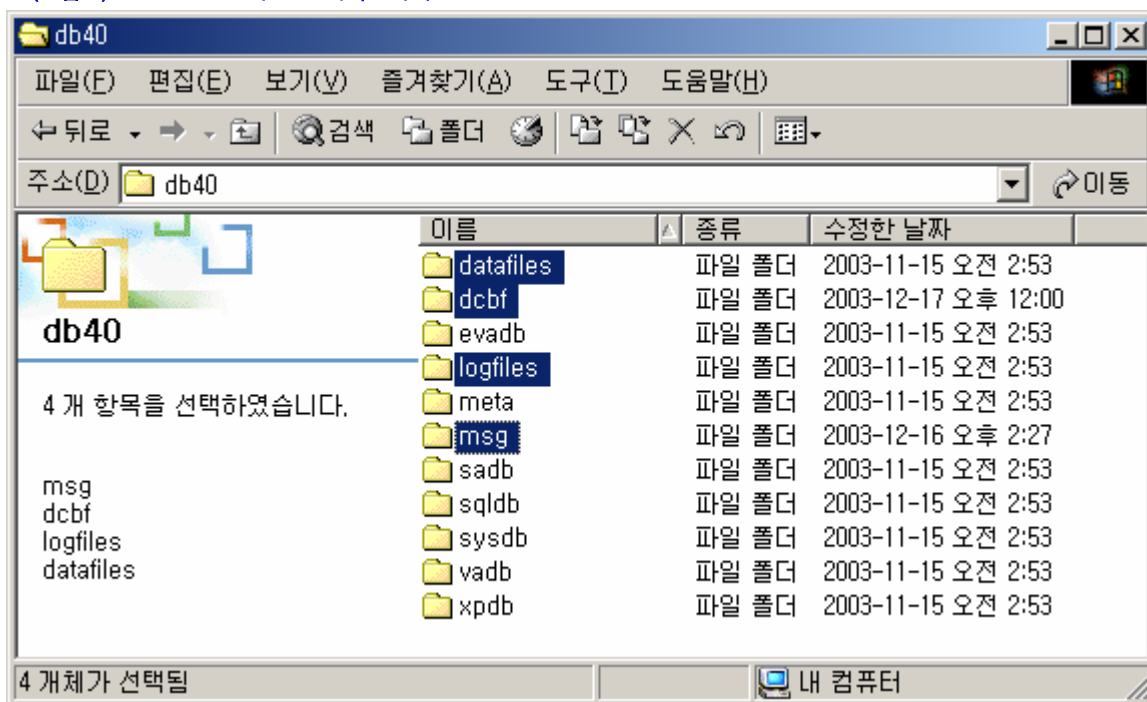
2.2.1 IDB Directory Structure

백업 서버에 위치하고 있는 IDB 는 기본적으로 아래 그림4 와 같은 Directory 구조를 가지고 있습니다. 또한 “db40” 디렉토리 밑에는 그림에는 표시 되지 않았지만 evadb, meta, sadb, sysdb, xpdb, sqldb, vadb 등의 하위 디렉토리가 준비 되어 있으며 NDMP 혹은 ZDB(Zero Downtime Backup) 백업 시 필요한 정보들을 위해 사용되어 집니다.

(그림 4) IDB 디렉토리 구조



(그림 5) windows CM 의 IDB 디렉토리 구조



2.2.2 IDB SIZE Limitations

Data Protector IDB 는 아래 표의 내용에서처럼 각각의 항목별 SIZE 를 적용 합니다.

IDB 에서의 SIZE “제한” 의 의미는 DP 작업 시 (Session) 발생되는 상황들에 대해서 (작업 LOG) IDB 에 얼마만큼 저장 할 수 있는지에 대한 제한 입니다.

아래 예를 들 경우 “최대 concurrent drives 수” 에 대한 내용은 동 시간대에 사용하는 Drive 숫자가 50대 (LTO) 를 초과 하면 해당 작업에 대한 LOG 정보를 저장 할 수 없다는 의미로 보시면 됩니다.

(표2) IDB Size Limitations 현황

항목	Size Limitations	비고
Filenames	700 million (UNIX) 450 million (Windows)	최대 32GB
file versions	10 x No of filenames	Filename 수량의 10배수 까지 Version 관리 가능
최대 DCBF directories	50	DCBF 확장 시 Directory 경로 수
DCBF directory SIZE	4 GB	
DCBF directory 당 최대 파일 개수	10000	
최대 concurrent drives 수 (DLT7000 and lower performing)	100	동일 시간대에 사용 DRIVE
최대 concurrent drives 수 (DLT8000/SDLT/LTO)	50	동일 시간대에 사용 DRIVE

2.2.3 기타 DP SPEC SIZE Limitatons

가) Backup Specification 의 Object 수 :

하나의 백업 작업 (spec) 당 500개의 Object (Mount Point / File System)를 처리 할 수 있습니다.

나) Media Pool 1개당 Media 수 :

Media Pool 1개에는 최대 40,000 Media 를 포함(연결) 할 수 있으며 total 500,000개 media 를 관리 할 수 있습니다.

다) IDB 최대 session (Backup, Restore , Media) :

작업 Session 에 대해서 IDB는 최대 1,000,000 session 을 저장 할 수 있으며

(물론 IDB 전체 FILE 사이즈를 초과 할 수 없습니다.)

1일 최대 2,000 개의 backup session을 저장 할 수 있습니다.

라) Concurrent Activities:

백업 작업 시 동일 session 에서 기본 5 대의 Drive 를 사용 가능 하며 최대 32 개의 Drive 사용이 가능 합니다.

(해당 Device(Drive) 사용 가능 수량은 global option 의 ” MaxMAperSM “ 항목에서 조정.)

마) Number of Cells in a MoM Environment :

MoM(Manager of Managerment) 환경에서 최대 50 개의 CELL 을 관리 할 수 있습니다.

2.3 Flat File Storage

Data Protector 는 IDB 와 함께 주요 구성 내용을 저장하는 FILE (ASCII) 형태의 Information Storage 를 가지고 있습니다.

이는 Data Protector 를 이용한 백업 시스템 운영에 매우 중요한 정보들로서 해당 내용은 Data Protector를 통한 IDB 백업 시 자동 저장 됩니다.

<경로> UX : /etc/opt/omni , WIN :Data Protector Home\config

2.3.1 User configuration

Data Protector 는 User interface Agent 가 설치된 시스템이 중앙의 Cell Manager 에 연결하여 Data Protector 를 관리할 수 있는 작업 범위에 대해서 users 디렉토리의 3가지 파일 (ClassSpec,UserList, WebAccess) 을 이용 하여 정의 합니다.

ClassSpec : user 들에 대한 그룹을 관리 합니다.

CLASS admin (Administrator 권한을 가진 유저들에 대한 그룹)
PERMISSION -1
DESCRIPTION "Administrator Class"

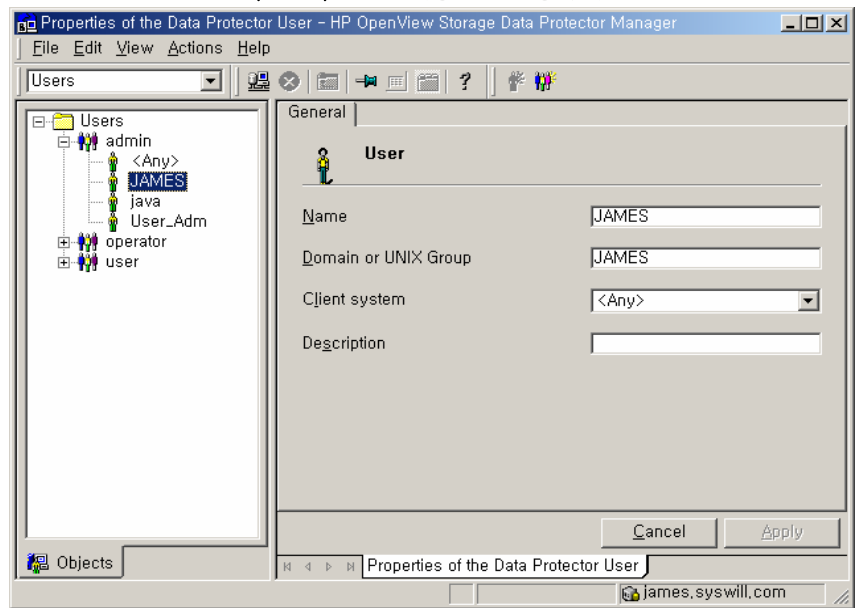
CLASS operator
PERMISSION 550911
DESCRIPTION "Operator"

CLASS user
PERMISSION 32
DESCRIPTION "Simple User Class"

UserList: user 별 등록 현황 입니다. 아래 파일의 내용 들은 Data Protector GUI 를 통해서 구성된 내용들이 반영되는 것이며 해당 파일을 통해서 직접입력(수정) 하실수도 있습니다.

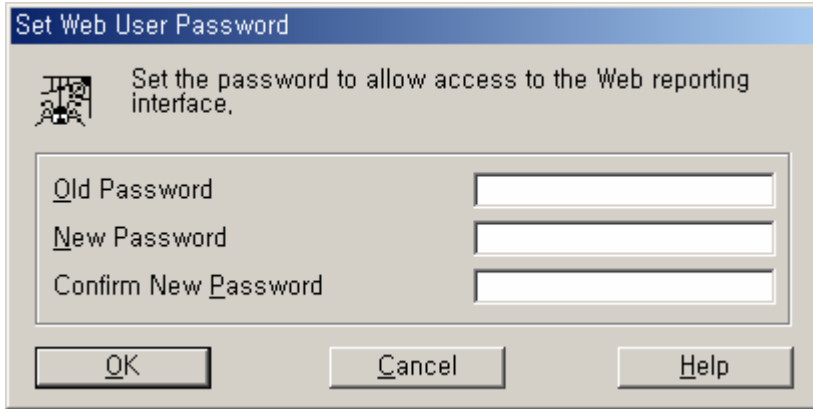
```
"" "*" "*" * "admin"  
"" "JAMES" "JAMES" * "admin"  
"WebReporting" "java" "applet" webreporting "admin"  
"" "User_1" "*" * "user"  
"" "User_2" "*" * "user"  
"" "User_3" "*" * "user"  
"" "User_4" "*" * "user"  
"" "User_Adm" "*" * "admin"  
"" "User_Op_1" "*" * "operator"  
"" "User_op_2" "*" * "operator"
```

(그림 6) GUI 를 이용한 User 등록 화면



WebAccess: Data Protector 에서 제공 하는 Web Reporting 사용시 필요한 password 를 정의 합니다.
 Data Protector 최초 설치 시에는 password 비 설정 상태 입니다.
 Password 설정은 Context List → Users → Actions → Set Web User Password 스텝을 통해서 설정을 하게 되며 해당 적용 값은 암호화 되어 반영 됩니다.

(그림 7) Web User (Report)Password 변경 화면



2.3.2 Backup specifications

Data Protector 에서 사용되는 일반 파일시스템 백업 및 DBMS 나 Application 등을 Intergration 하여 생성되는 백업 Specifications 을 관리 및 저장 합니다.

Datalists 디렉토리 : 일반 파일시스템 백업 Specification

BarLists 디렉토리 : DBMS 및 Application 대상 Intergration 백업 Specifications

2.3.3 Schedules

앞서 설명한 백업 specifications 들에 대한 작업 스케줄을 저장 관리 합니다.

Schedules 디렉토리 : 일반 파일시스템 백업 Specification 대상 작업 스케줄

Barschedules 디렉토리 : DBMS 및 Application 대상 Intergration 백업 Specifications 의 작업 스케줄.

2.3.4 Cell environment

Data Protector 의 핵심 요소인 Cell 의 구성 내역을 저장 관리 합니다.

cell_server : Cell Manager Server 의 시스템 명 (hostname)이 등록 되어 있습니다.

각각의 Data Protector Agent (Cell Client)시스템의 동일한 위치에도 해당 파일이 존재 합니다.

cell_format : Data Protector Cell Manager 가 사용하는 환경변수 및 설치 정보가 저장 되어 있습니다.

cell_info: Cell 에 구성 되어 있는 시스템 (CM + Cell Client) 들의 설치 정보가 저장 되어 있습니다.

installation_servers : 현재 구성되어 있는 Installation Server들의 정보가 저장 되어 있습니다.

omni_info : Cell 내의 각각의 SYSTEM 에 설치 되어 있는 Data Protector Agent 의 설치 내역 정보를 저장 합니다.

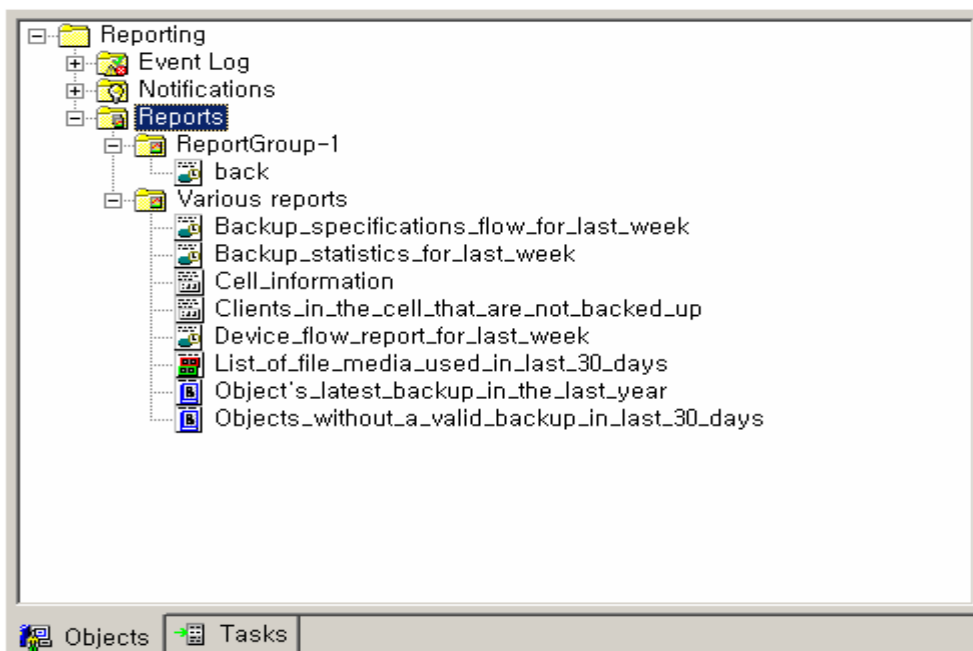
lic.dat : Data Protector 설치 후 GUI 를 통해서 라이선스 를 입력 하면 해당 파일이 생성되며 라이선스가 적용 됩니다.

사용자가 라이선스 Key 값을 잘못 입력 하였거나 Cell Manager 시스템의 IP 변경 등의 이유로 갱신 할 필요가 있을 때에는 해당 파일을 편집 하면 됩니다.

2.3.5 Report groups (rptgroups)

Data Protector는 백업 시스템 구성 내용이나 작업 내역에 대한 내용을 Report 서비스를 이용하여 다양한 형태로 제공 하며, 보고 범위나 사용 목적에 맞게 Index 를 가능 하게 합니다.

(그림 8) GUI 에서의 Reporting 그룹



2.3.6 Report schedules (rptschedules)

보고 목적에 맞게 분류된 Reporting group 들에 대해서 작업 스케줄을 설정 합니다. 그룹 안의 해당 Report 들은 설정된 스케줄에 의해 각각의 SEND 방식으로 발송 되게 됩니다.

2.3.7 Notifications

Data Protector는 백업 시스템 운영 시 특정 event 들 ("DeviceError", "EndOfSession", "MountRequest", "DatabaseSpaceLow", "NotEnoughFreeMedia", "DatabaseCorrupted", "BackupError", "UnexpectedEvents", "HealthCheckFailed", "MailSlotsFull", "DatabasePurgeNeeded", "LicenseWillExpire" ...) 이 발생 하면 EVENT 별 발생 상황에 대해 알려 주며 기본적으로 해당 내용은 Event Log 에 쌓이게 됩니다.

3장. IDB Maintenance

Data Protector IDB 운영 방법이나 정책에 대해 설명을 하며 장애 발생시 효과적으로 대처 할 수 있는 방안을 모색 하도록 합니다.

3.1 IDB Maintenance

IDB 운영시 Disk 공간 부족에 의한 IDB SIZE 축소, 불필요한 작업 LOG 삭제, 예기치 않은 IDB 장애발생 등으로 인해 IDB 는 여러가지 형태의 관리를 필요로 하게 됩니다.

3.1.1 Managing IDB Growth

IDB size 는 앞서 설명 했듯이 32GB 이상까지 확장이 가능 하지만 운영자는 백업서버의 DISK 크기나 백업 시스템 운영에 관한 효율적인 기준을 고려 하여 적절한 IDB size 를 유지 해야만 합니다.

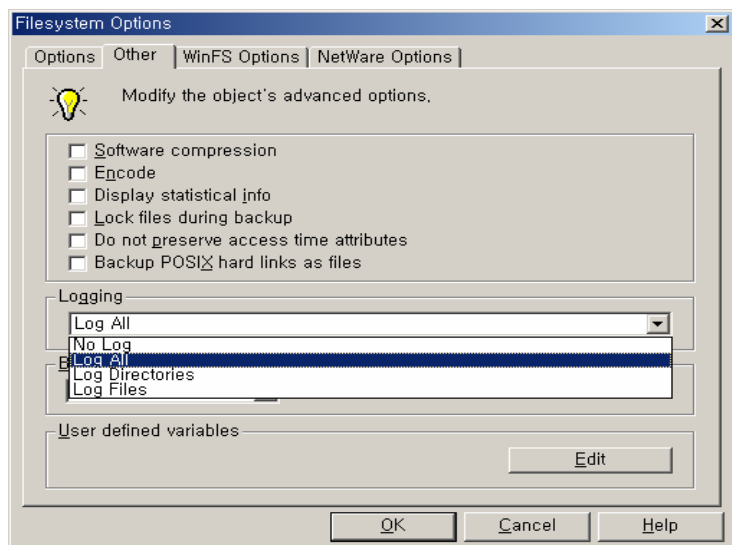
가) LOG LEVEL 차등 적용

백업 작업 시 IDB에 저장되는 상세 directory 및 파일 정보를 차등 적용 함으로서 백업 속도 개선 효과와 IDB SIZE 증가 억제 효과를 얻을 수 있으며 Restore 시 파일 브라우징 속도에 영향을 주게 됩니다.

- **Log All** : default logging level 로서 백업작업 시 Directory 나 File 에 대한 모든 상세 정보 (names, versions, attributes) 들을 IDB 에 저장 합니다. Data Restore 시 운영자는 백업된 DATA 의 상세 정보를 확인 할 수 있으며 미디어에 저장된 DATA 의 Postion 을 보다 빠르게 찾을 수 있습니다.
- **Log Files** : 백업 시 file 과 directory 에 대해서 속성 부분을 제외 한 상세 log 정보를 기록 합니다.
- **Log Directories**: 백업 Data 중에서 directory 에 대한 상세 정보 (names, versions, and attributes) 만을 기록 합니다. 본 log Level은 자동 생성 파일 기반의 Application DATA, 즉 News 그룹이나 Mail 시스템을 운영하는 경우에 적합한 백업 log 방식 입니다. 단 restore 시에 directory 레벨 까지만 브라우징 하며 복구가 가능 합니다.
- **No Log**: 백업 DATA 의 directory 나 file 의 정보를 저장 하지 않으므로 복구시에는 백업 DATA 최 상위 point 에서만 restore 가능.

(그림 1) Logging Level

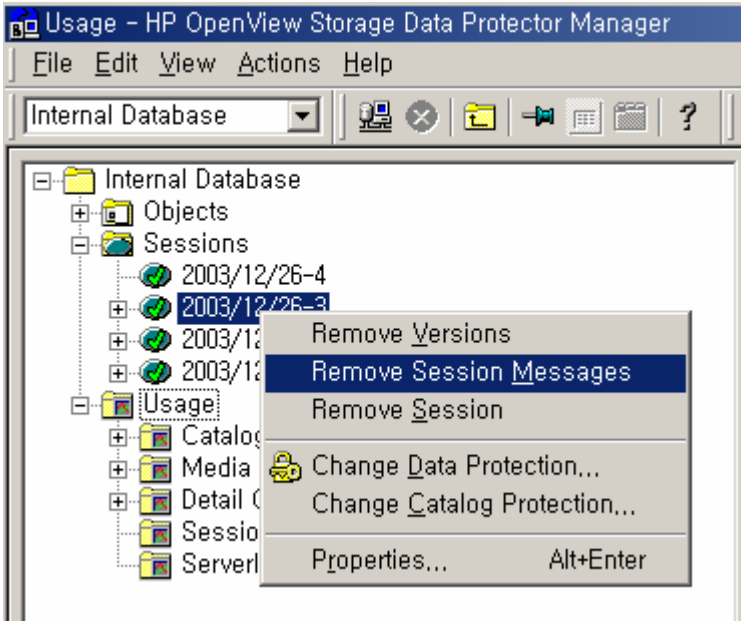
일반 파일시스템 백업시 log 레벨은 백업 Specification 의 Filesystem Options 에서 적용이 가능함.



나) IDB record 폐기

- 미디어에 저장된 백업 DATA를 Overwrite 하게 되면 자동으로 해당 Record 가 삭제 됩니다.
- DATA retention policy (보관 정책) 가 만료 되었을 경우에 자동으로 해당 Record 가 삭제 됩니다.
- Data Protector GUI 나 CLI 를 통해서 수동으로 삭제 할 수 있습니다.

(그림 2) Manually remove sessions



Remove Versions :

백업된 Data 내의 Directory 와 File 별 Version 을 삭제 합니다.
(DB Purge 후 반영)

Remove Session Messages:

해당 session 이 가지고 있는 작업 Message 를 삭제 합니다.

Remove Session:

Session 자체를 삭제 합니다.

<참고>

Change Data protection:

백업된 DATA에 대한 보존 기한을 변경합니다.

Change Catalog Protection:

IDB 내에서 저장하고 있는 catalog 보존 기한을 변경 합니다.

자동 삭제

IDB 내에서 보관주기가 만료되었거나 Version 정보를 삭제한 경우 혹은 여러 가지 이유로 백업 시스템 운영에 불필요한 정보들은 ASM(Admin Session Manager) 에 의해서 DCBF, SMBF 영역의 내용을 대상으로 삭제 됩니다.

해당 설정은 global option 의 “DailyMaintenanceTime” 에서 사전에 정의 되어 있으며 매일 정오(12:00) 에 진행 되도록 스케줄 되어 있습니다.

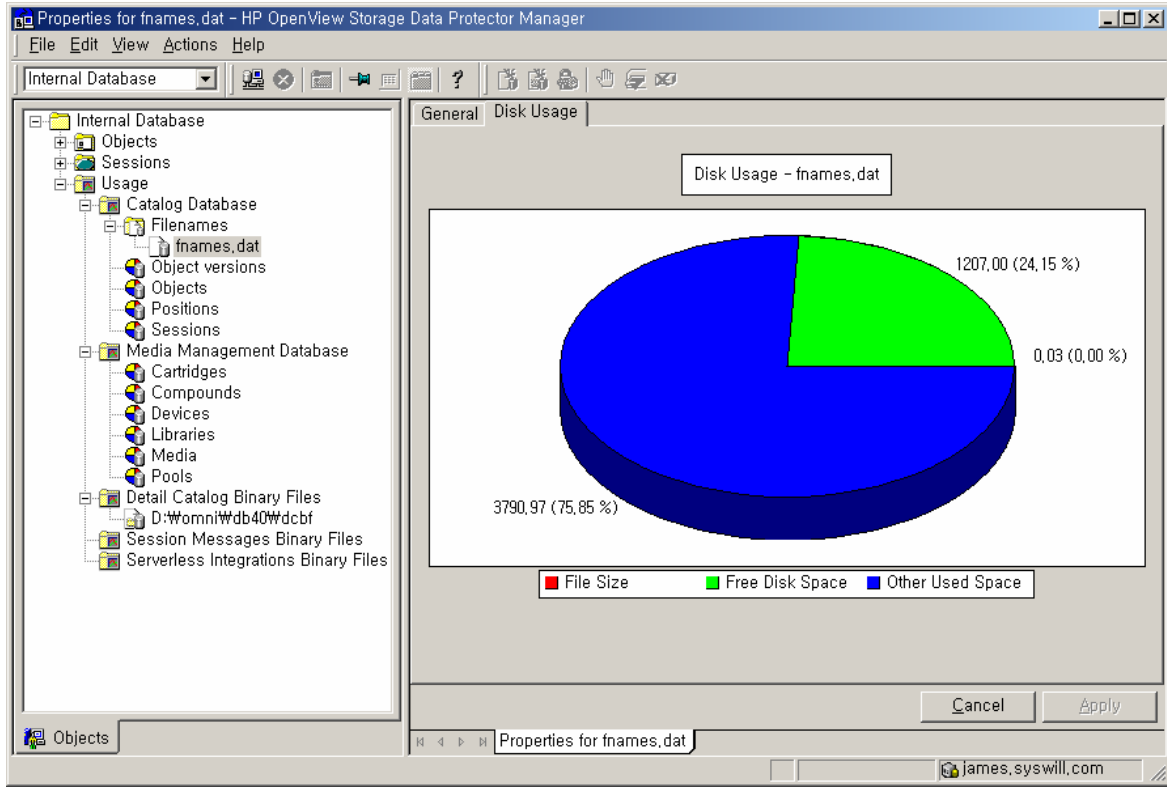
수동 삭제

운영자는 Command 를 이용하여 IDB 에 대한 효과적인 Purge 를 실시 할 수 있습니다.
/opt/omni/bin/omnidbutil (IDB Command 파트에서 상세 설명)

3.1.2 IDB GUI & Extensions

Data Protector IDB 에 대한 정보는 GUI 를 통해서 확인 할 수 있으며 다양한 Display 형태를 통해서 보다 손쉽게 세부 내용을 관리 할 수 있습니다.

(그림 3) GUI 를 통한 IDB Monitoring 화면



- 위 (그림3) 은 CDB(Catalog Database) 영역 중에서 filename 들을 저장하는 fnames.dat 파일에 대한 Monitoring 화면 입니다. Data Protector 초기 설치 시 “fnames.dat” 파일은 1개 존재하며 최대 2GB 까지의 filename 들에 대한 Data 를 저장 할 수 있습니다.

기본 PATH : D:\WDP 설치 홈 디렉토리\wdb40\datafiles\cdb\w\fnames.dat

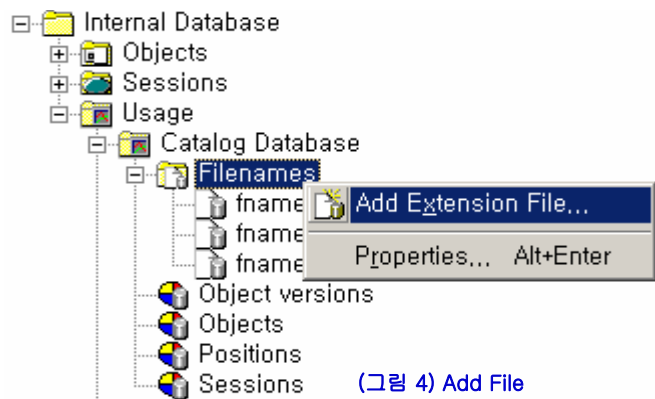
화면 우측의 PIE 차트는 전체 Disk 사용량 대비 “filenames”영역의 사용량을 나타낸것으로서 현재 “D” drive 내에서 청색은 이미 사용중인 Disk 영역, 녹색은 사용 가능한 Disk 영역으로서 위와 같은 경우엔 DISK 에 남은 공간이 얼마 없으므로 “filename”을 위한 확장 공간이 필요 할 수 있습니다. 적색은 filenames SIZE 를 의미함.

만일 해당 영역을 확장 하시고자 할 때는 옆의 (그림4)처럼 “Add Extension File” 기능을 이용 하시면 됩니다.

디렉토리 경로까지만 설정 한 후 (파일이름은 자동으로 생성) 해당 파일의 최대 SIZE 를 설정 합니다.

< 파일 추가 시 이름 생성 순차 >

fnames.dat1, fnames.dat2, fnames.dat3 ...



(그림 4) Add File

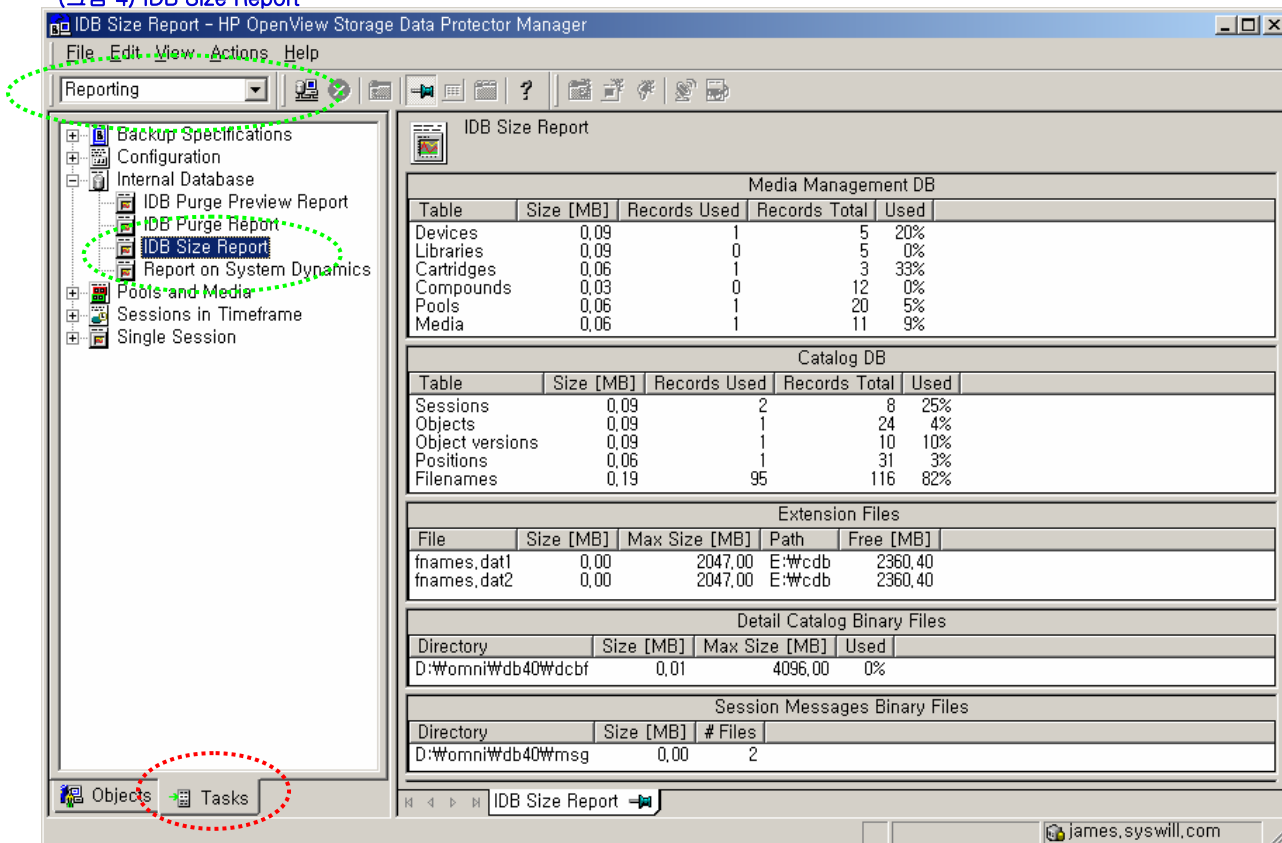
3.1.3 IDB SIZE Report

Data protector GUI Context List 에서 “Reporting” 을 선택한 후 화면 아래의 “Tasks” TAB 을 선택 하면 Data Protector 운영에 관한 주요 Report 를 확인 할 수 있습니다.

아래 (그림5) 는 IDB 전체 구성내역에 대한 상세 SIZE 로서

화면 좌측의 [Internal Database → IDB Size Report](#) 를 선택하면 Display 됩니다.

(그림 4) IDB Size Report



아래 표는 IDB Size Report 내역 중에서 catalog 부분만 발췌한 것으로 위 GUI 의 전체 내용을 별도의 HTML 형식으로 LOCAL 폴더에 logging 한 파일 (Ex: IDB_SIZE_RPT.htm) 을 편집 한 것입니다. (Report 작성 부분 매뉴얼 참조 Data Protector CD /docs/admin.pdf)

(표1) Catalog DB SIZE Report

Table	Size [MB]	Records Used	Records Total	Used
Sessions	0.09	2	8	
Objects	0.09	1	24	
Object versions	0.09	1	10	
Positions	0.06	1	31	
Filenames	0.19	95	116	

3.1.4 Adding DCBF(Detail Catalog Binary File) Locations

앞서 언급한 CDB 영역의 “filenames” 부분 확장과 마찬가지로 DCBF directory 경로를 최대 50개 까지 추가할 수 있습니다.

Global 파일에서 정의 하고 있는 초기 값은 기본 10 개까지 확장이 가능 하며 추가 확장은 해당 파일 편집을 통해 적용 하시면 됩니다.

[/Data Portector Home/config/Options/global](#)

```
# MaxDCDirs=NumberOfDirectories
```

```
# default: 10
```

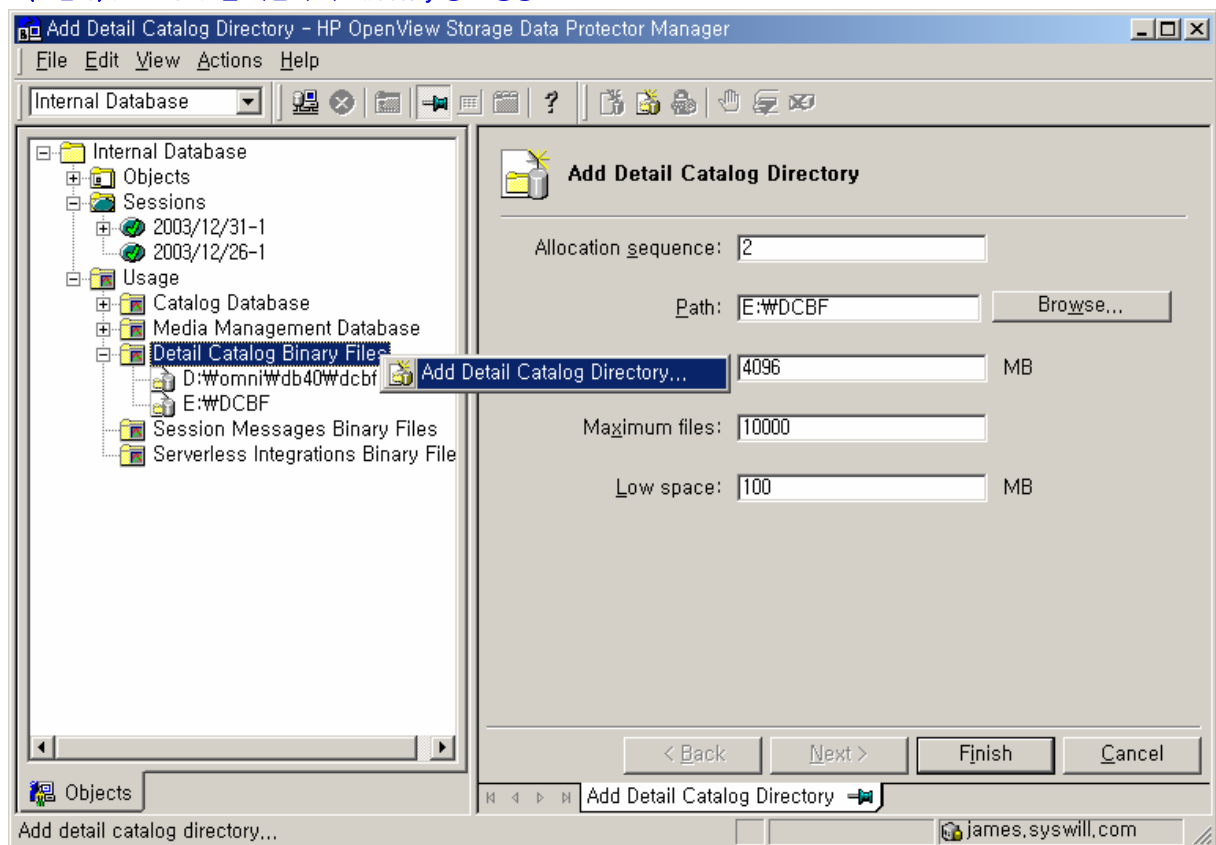
```
# minimum: 1
```

```
# maximum: 50
```

```
# This option specifies maximum number of configured DCBF
```

```
# Directories.
```

(그림 5) IDB DCBF 를 위한 추가 Directory 경로 생성



- DCBF 경로 확장은 위 (그림5) 에서 처럼 GUI 를 통해서도 가능 하며
“omnidbutil -add_dcbf <Path>” 명령을 통해서도 생성 이 가능 합니다.

3.2 IDB Backup

IDB 는 효율적인 구성을 바탕으로한 운영정책이 뒷바침 되어야 하며 근본적으로는 IDB 자체 백업작업이 효과적으로 이루어 져야 합니다.

IDB 백업은 Data Protector 자체 IDB Hot Backup 기능을 통해서 작업이 가능 하며 Data Protector 가 예기치 않은 장애로 인해 정상적인 기능을 수행 할 수 없을 때를 대비 하여 Data Protector Management 와 무관하게 일반 파일 COPY 방식으로 백업을 실시할 필요가 있습니다.

3.2.1 IDB Backup Media

IDB 백업 시 사용되는 Media 는 가급적 Main Backup Device 보다는 DAT Drive 를 이용 하거나 원격지 시스템의 File 영역을 이용하는 것을 권장 합니다.

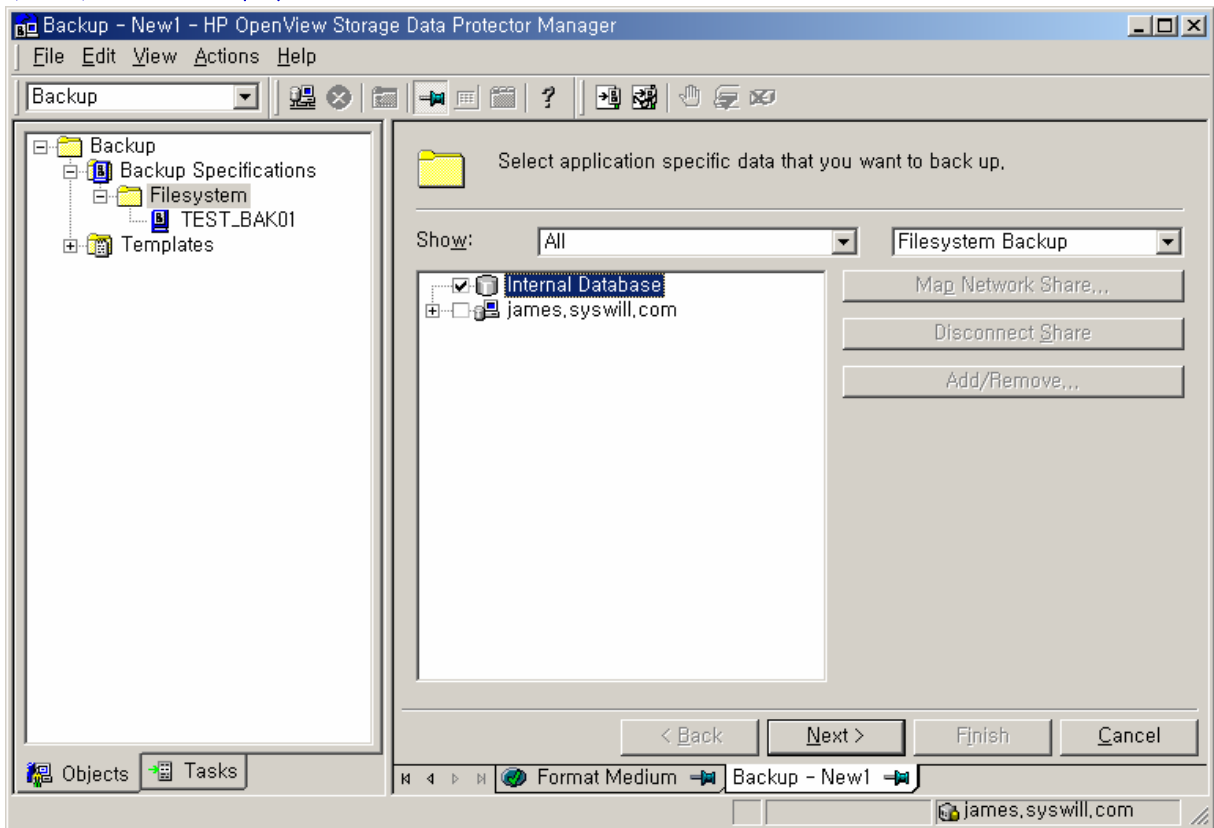
3.2.2 IDB 백업 시기

통상적으로 대부분의 주요 백업 작업이 야간 혹은 새벽 시간대에 이루어지는 경우가 많으므로 오전 시간대에 적절한 시점을 선정하여 스케줄링 하는 것이 좋습니다. 작업에 큰 무리가 없다면 일일 2회(오전/야간) 이상의 백업 작업을 시행 하는 것도 권장 하는 바 입니다.

3.2.3 Data Protector IDB HOT 백업 절차

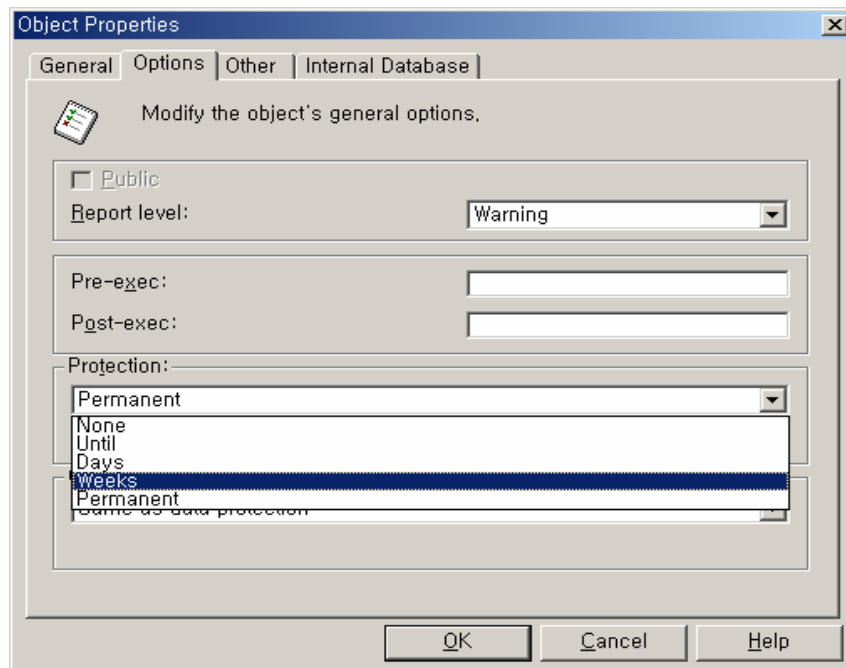
- 가) 우선 GUI 를 통해서 Filesystem 형태의 IDB 백업 SPEC 을 생성 합니다.
 - 아래 (그림6) 에서와 같이 Internal Database 부분을 백업 대상으로 선택하여 Spec 을 생성 합니다. 기본적으로 IDB Hot backup Spec 의 Protection 은 Permanent 로 설정되어 있습니다.

(그림 6) IDB Hot Backup Spec 생성



나) 만일 IDB HOT Backup DATA 의 보관주기를 변경 하고 싶은 경우에는 해당 IDB 백업 spec 의 Object Property 의 Protection 을 변경 하면 됩니다.

(그림 7) IDB Backup Spec 의 Object Property



다) GUI 를 통해 생성된 IDB Hot Backup Spec 작업을 실시 하게 되면 Data Protector 는 백업 작업 실시전에 IDB consistency check 작업을 하게 됩니다.

<Ex: IDB Hot Backup 작업 Message>

[Normal] From: BMA@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 3:07:39
STARTING Media Agent "IDB_BACK"

[Normal] From: DBBDA@james.syswill.com "[Database]: james.syswill.com" Time: 2003-12-29 오후 3:07:45
STARTING Database HotBackup Disk Agent on james.syswill.com "[Database]: james.syswill.com".

[Normal] From: DBBDA@james.syswill.com "[Database]: james.syswill.com" Time: 2003-12-29 오후 3:07:47
[Consistency check of Media Management Database...](#)

[Normal] From: DBBDA@james.syswill.com "[Database]: james.syswill.com" Time: 2003-12-29 오후 3:07:52
[Consistency check of Catalog Database...](#)

[Normal] From: DBBDA@james.syswill.com "[Database]: james.syswill.com" Time: 2003-12-29 오후 3:07:57
[Databases are consistent.](#)

** IDB 백업은 반드시 IDB 운영 상황이 정상적인 경우일 때에만 의미가 있습니다.

만일 IDB 백업 전 DB check 시 문제가 있을 때 에는 문제 해결 후 작업을 실시 하시기 바랍니다.

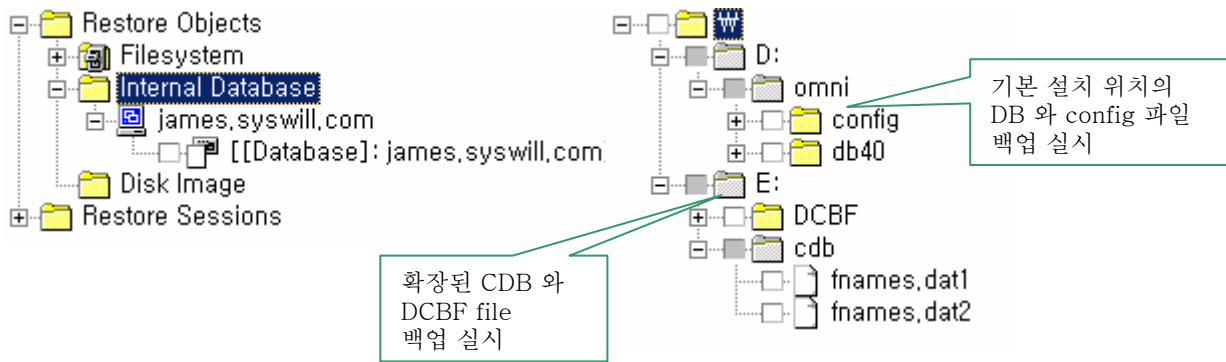
3.2.4 IDB & configuration 파일 COPY

IDB 백업은 Data Protector 에서의 HOT Backup 뿐만이 아니라 간단한 File Copy 형태로도 진행 할 수 있습니다.

운영자는 몇 가지 Check 조건을 확인한 후에 IDB 파일과 함께 Flat File 형태로 보관 되어지는 주요 환경 파일들을 함께 백업 하도록 합니다.

아래 (그림8) 은 IDB Hot Backup시 저장 되는 DATA 들을 **Restore** STEP 에서 확인한 내용 입니다. 현재 Data Protector 는 “ D” Drive 에 설치된 IDB 파일과 Config 파일의 기본 구조 외에도 “E” 드라이브 내에 확장된 DCBF 와 CDB 영역들까지도 포함해서 백업이 실시된 상태 입니다. 즉 수작업으로 IDB 관련 파일들을 COPY 하고자 할 때는 반드시 아래 경우 처럼 해당 내용 전체를 COPY 해야만 합니다.

(그림 8) Hot Backup 된 IDB 의 Restore 시 선택 경로와 백업된 DATA 내역



가) 백업 (COPY) 전에 반드시 IDB 상태 체크를 합니다.

```
D:\WomniWbin>omnidbcheck
Check Level          Mode          Status
=====
Core                 -core        OK
Filenames            -filenames   OK
DCBF(presence and size) -bf          OK

DONE!
```

만일 위에서 처럼 “OK” 싸인이 떨어지지 않고 에러가 발생 한다면 IDB 백업 이전에 먼저 장애 상황을 조치 하고 백업을 해야 합니다.

(물론 장애 상황에서 IDB 작업을 하기 위한 COPY는 필요 하다고 생각 합니다.)

나) IDB Check 가 잘 진행 되었다면 작업중인 다른 Session 있는지 확인한 후에 Data Protector Service 를 종료한 후 COPY 작업을 실시하기 바랍니다.

**** IDB Hot Backup 은 기타 작업이 진행 중이더라도 문제가 되지 않습니다.**

3.3 IDB Restore & Recovery

IDB 장애 발생시나 혹은 예전의 백업 시스템 설정으로 복원 하고자 할 때는 백업 되 있는 IDB 관련 DATA Restore & Recovery 작업을 실시 합니다.

3.3.1 Manual Restore of the IDB 개요

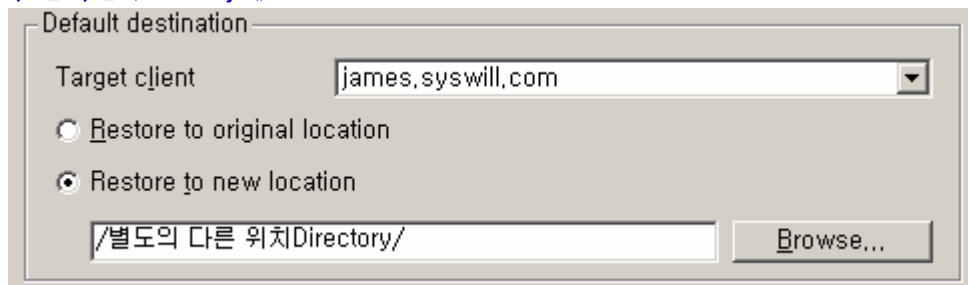
Hot Backup 된 IDB DATA 를 Manual 방식으로 Restore 할 때는

반드시 Original 위치에 아닌 별도의 다른 위치에 해당 파일을 Restore 한 후에 작업을 진행 하시기 바랍니다.

Data Protector 서비스가 운영중인 상황에서 Original 위치에 IDB DATA 를 Restore 하게 되면 현재 운영중인 IDB 및 서비스에 장애를 초래 합니다.

1) HOT Backup 된 IDB DATA 를 원래 위치가 아닌 별도의 공간에 Restore 합니다.

(그림 9) 임시 Directory 에 Restore



2) Restore 가 잘 종료 되었으면 Data Protector Service 를 종료 합니다.

`/omnisv stop`

3) 오리지날 위치의 IDB 관련 내용은 만일을 위해서 COPY 해 놓습니다.

4) Restore 된 파일들을 필요에 따라 원래 위치에 Overwrite 합니다.

`mv 임시 폴더/db40 /var/opt/omni/db40`

5) Data Protector 서비스를 재 가동 합니다.

`/omnisv start`

6) IDB check 를 통해서 IDB 이상 유무를 확인 합니다.

`/omnidbcheck`

(그림 10) IDB Restore 개요





<참고 : 백업 시스템 전체 Recovery >

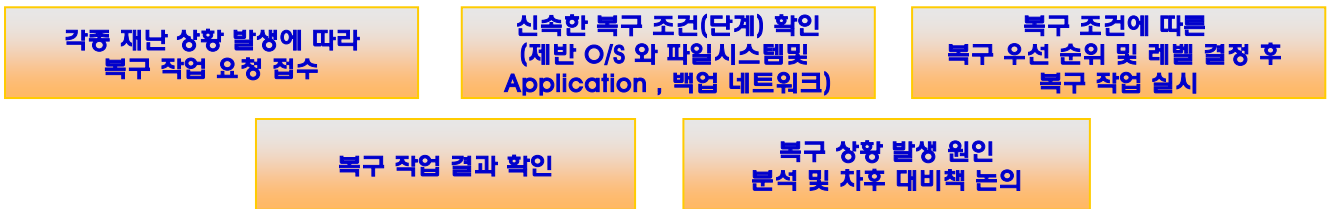
Data Protector 를 사용 하는 중에 DP Cell Manager 가 장착된 시스템이 완전히 붕괴 되었을 경우 어떻게 할 것인가?

정상적인 IDB 에 대한 백업 본이 있을 때에는 문제가 없지만 그렇지 않을 경우엔 Media 에서 모든 DATA 를 Import 받아야 하므로 시간도 많이 걸릴뿐더러 복구 수준도 만족스럽지 못할 수 있습니다. 그러기 때문에 반드시 어떤 형태로든 **IDB 백업은 매일 매일 받아 놓는 것이 좋습니다.**

Data Protector 운영자는 유사시 신속하고 정확한 백업 시스템 복구를 위해 평상시 복구 STEP 숙지와 더불어 체계적인 사전 훈련이 필요 합니다.

현업에서 운영 중인 백업 시스템을 대상으로 작업 하기가 곤란하면 개인 PC나 유틸 시스템을 이용하여 주기적인 연습과 모의 훈련 을 실시 하여 장애 발생시 백업 시스템 정상화 뿐만이 아니라 궁극적으로 주요 DATA 에 대한 완벽한 Recovery 체계를 유지할 수 있어야 하겠습니까.

< 시스템 장애 시 복구 단계 >

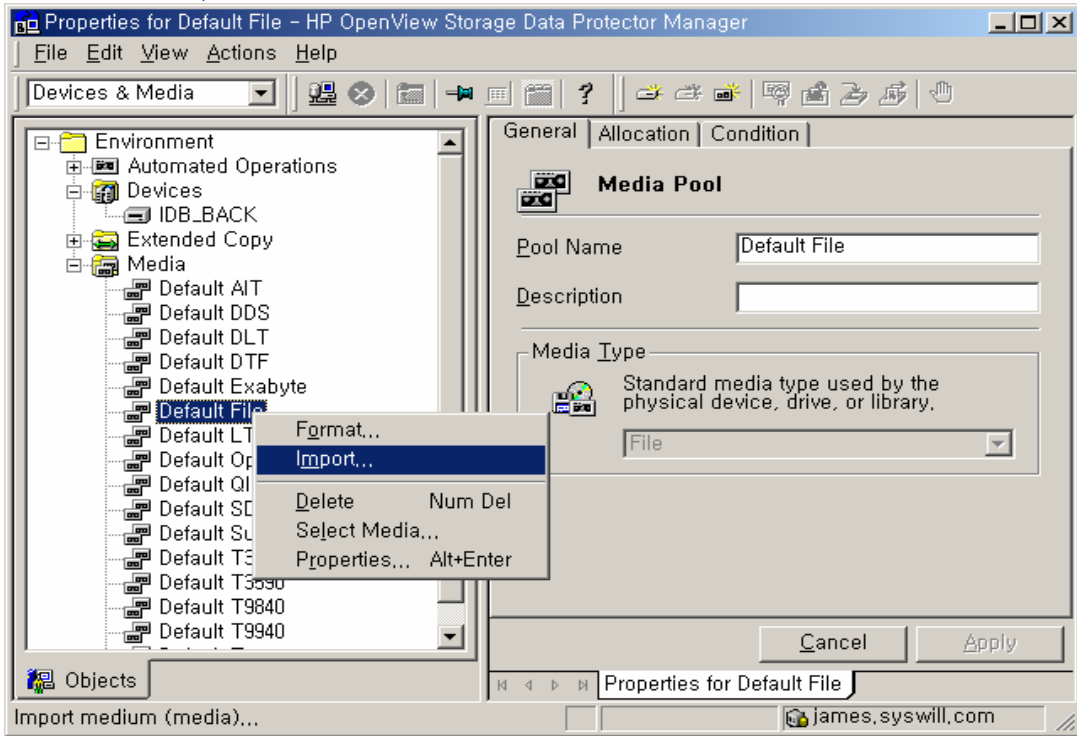


- 1) 시스템 하드웨어 문제 해결 :
장애 사실 통보 및 접수 후 신속한 시스템 하드웨어 복구 및 교체
- 2) Operating System 문제 해결 :
최악의 경우, 중요한 데이터를 보관하는 시스템 디스크나 혹은 모든 디스크가 손상되는 경우 발생. 이러한 경우는 기존에 수행되던 O/S를 최소 설정을 지닌 채로 다시 설치하여 복구.
- 3) 기존 네트워크 정보 값 설정 :
백업 소프트웨어의 기본적인 백업 네트워크 설정 복원.
- 4) Logical Volume 및 파일 시스템 설정:
O/S 재 설치 후 모든 Logical Volume 및 파일 시스템 재 생성 , 기존 Mount Point 복원
- 5) 백업 S/W(Data Protector) 운영 상황 복구 (Manager or Agent):
기존 운영중인 백업 시스템을 원상태로 복구 합니다.
만일 Cell Manager (백업 매니저 서버 탑재) 서버가 복구 대상일 경우에는 백업 S/W 자체 DB 복구 작업을 실시토록 합니다
- 단순 백업 Agent 시스템일 경우 에는 장애 발생 전에 운영하던 Agent 만 복원 시키면 됨.
- 6) DATA RESTORE :
- 백업 S/W 의 모든 기능이 정상화 됐을 경우 해당 DATA 를 RESTORE 합니다.
- 7) Recovery :
- Application , DBMS 별 recovery 작업을 실시 합니다.

3.3.2 Manual Restore/Recovery of the IDB 절차

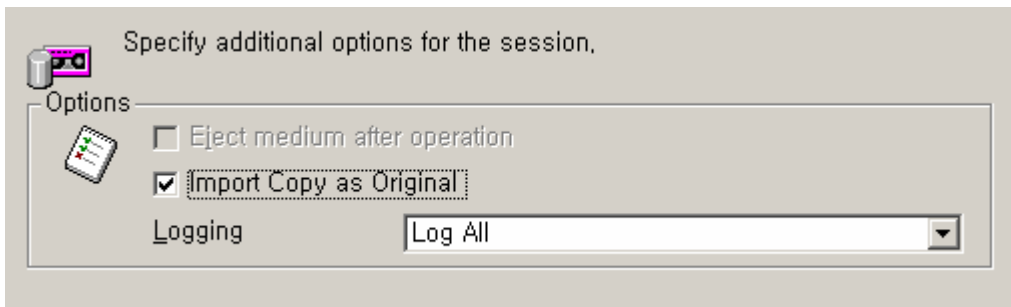
- 1) 백업 시스템 정상화:
백업시스템이 운영중인 서버에 문제가 발생 했다면 해당 서버의 O/S 및 File System 을 최 우선으로 정상화 시킵니다.
- 2) Data Protector 재설치 :
사용하던 Version 에 맞게 Data Protector 를 재설치 하며 필요한 Patch 도 모두 적용 합니다.
(평상시 패치 정보 관리가 필요 하며 Patch 파일은 크기 문제로 인해 단시간에 다운 받기가 어려울 수도 있으니 필요한 Patch 파일은 Down 받아 별도 보관 하는것을 권장 합니다.)
- 3) IDB 백업 본을 위한 Device & Media 를 설정 한 후 해당 Media 정보를 Import 합니다.

(그림 11) Media import



- 4) IDB Data 가 백업된 Media Import 시에는 Logging mode 선택을 “Log All” 로 합니다.

(그림 12) Import 시 Logging Level Setting



5) IDB DATA 가 백업된 Media 로 부터 import 를 실시하면 아래처럼 IDB 백업 작업 내역을 인지 하며 IDB DATA Restore 가 가능 해 집니다.

[Normal] From: MMA@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 7:03:27
STARTING Media Agent "IDB_BACK"

[Normal] From: MSM@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 7:03:28
Data Protector foreign medium "6b74eecb:3fefbfc0:0604:0001" found.

[Normal] From: MSM@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 7:03:28
Importing session into database:

SessionID: 2003/12/29-2
Owner: JAMESWJAMES@james.syswill.com
Start time: 2003-12-29 오후 2:48:59

[Normal] From: MSM@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 7:03:29
Importing session into database:

SessionID: 2003/12/29-3
Owner: JAMESWJAMES@james.syswill.com
Start time: 2003-12-29 오후 3:07:39

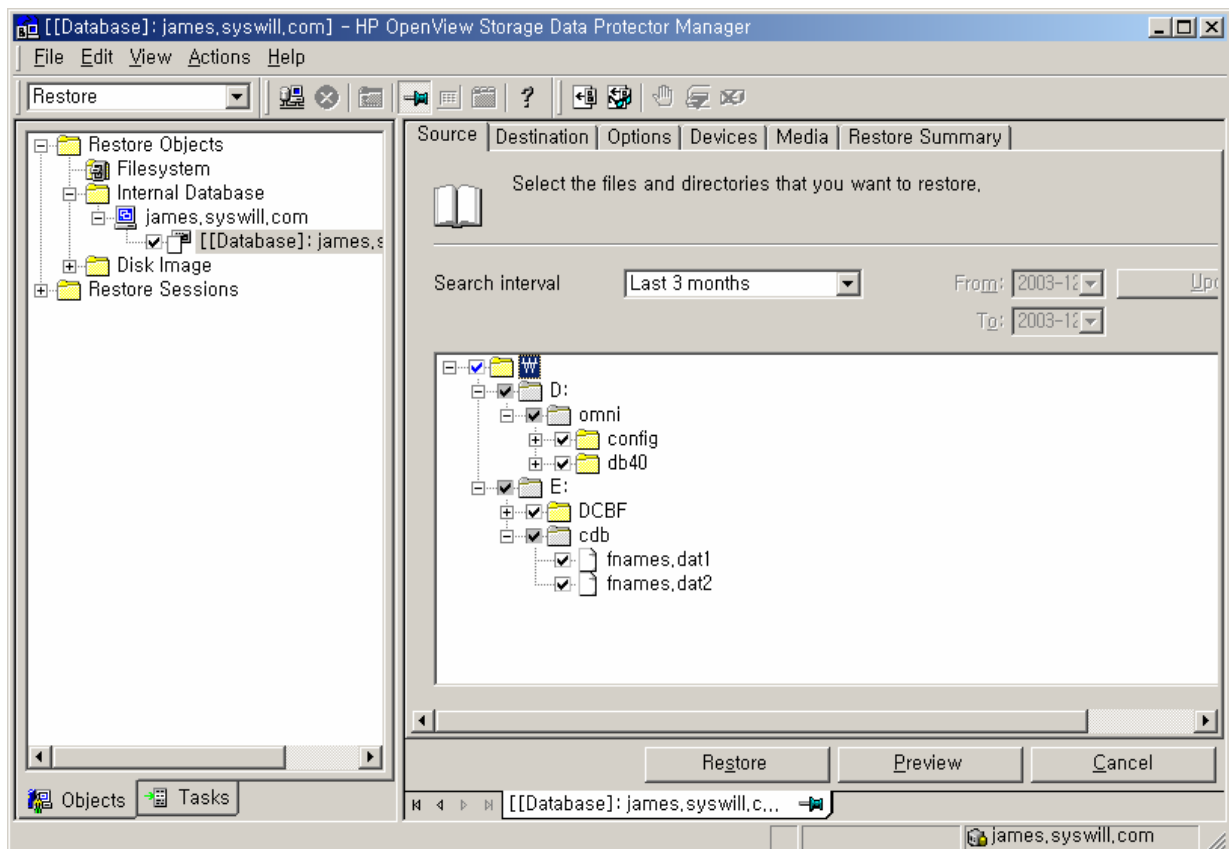
[Normal] From: MMA@james.syswill.com "IDB_BACK" Time: 2003-12-29 오후 7:03:29
COMPLETED Media Agent "IDB_BACK"

=====

1 media out of 1 successfully imported.

=====

(그림 13) 복원된 IDB DATA 백업 내역



6) 다른위치에 IDB DATA 를 Restore 합니다.

(그림 14) 임시 디렉토리에 IDB DATA Restore



7) Restore 가 잘 끝나고 나면

실행중인 Data Protector 를 종료 한 다음 Data Protector 서비스를 중지 합니다.

```
D:\WomniWbin>omnisv stop
```

```
HP OpenView Storage Data Protector services successfully stopped.
```

8) 다른위치에 Restore 된 IDB 및 Flat file 들을 Original 위치에 COPY 합니다.

9) 서비스를 재 시작 합니다.

```
D:\WomniWbin>omnisv start
```

```
HP OpenView Storage Data Protector services successfully started.
```

10) IDB Check 를 실시 합니다.

```
D:\WomniWbin>omnidbcheck
```

```
Check Level      Mode      Status
```

```
=====
```

```
Core             -core     OK
```

```
Filenames       -filenames OK
```

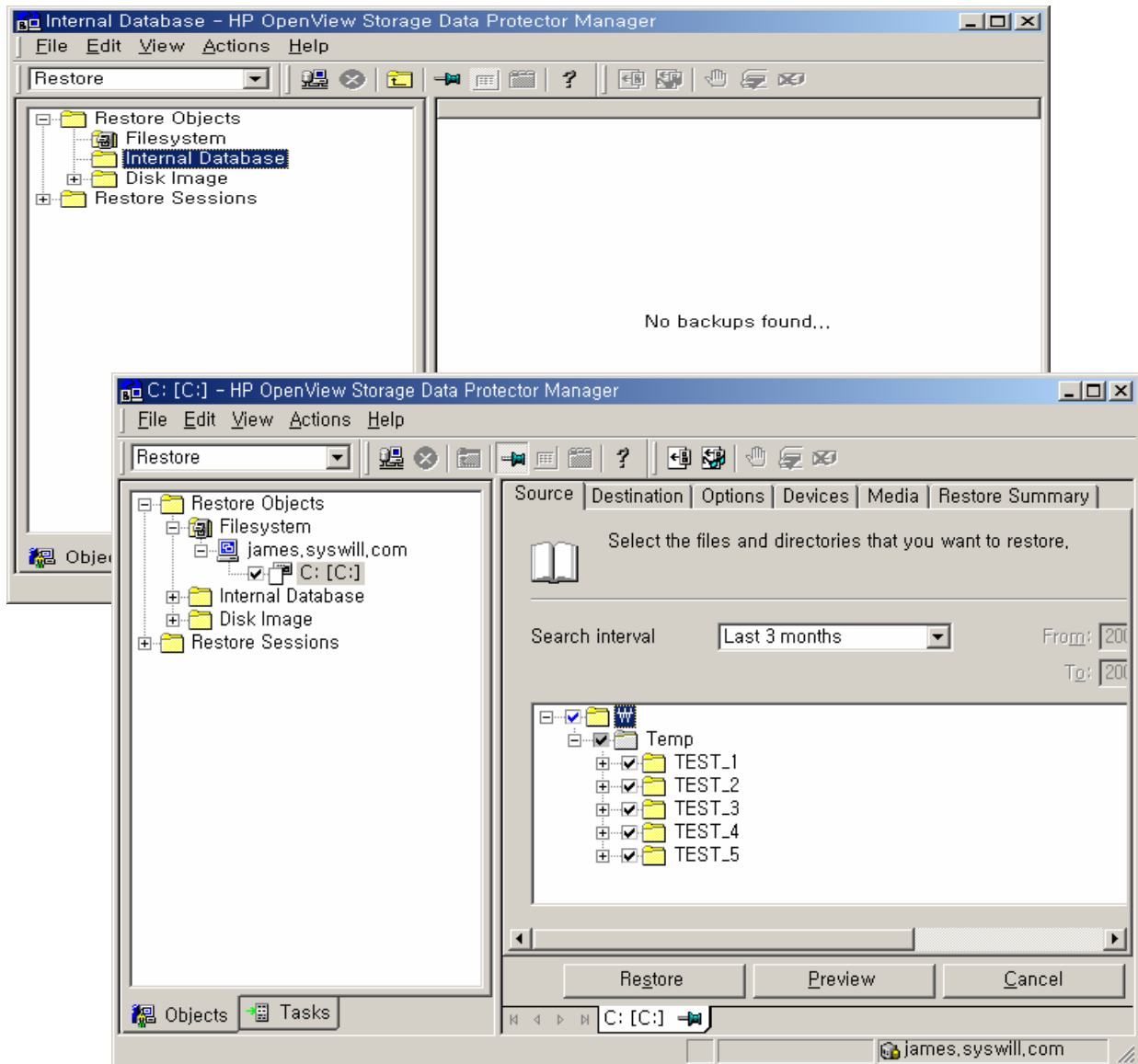
```
DCBF(presence and size) -bf      OK
```

```
DONE!
```

11)복원이 잘 되었는지 기존 구성을 확인 합니다.

12) 기존 구성이 잘 복원 되었다면 필요한 시스템의 파일을 복원 합니다.

(그림 15) IDB 복원 전 과 후의 GUI Rstore Step



** Data Protector 초기 설치 시에는 GUI Restore Part 에서 백업 정보를 확인 할 수 없었으나 IDB 복원이 정상적으로 종료 되게되면 위 (그림15)와 같이 IDB 나 Filesystem, DBMS 등에서 백업 받았던 작업 log 확인이 가능 하며 시스템 별 정상적인 DATA Restore 가 가능하게 됩니다.

** IDB 복원작업 에는 Cell 구성 정보(CM 과 client 관계) 에 관한 확인도 반드시 필요 합니다. 즉 백업 시스템이 정상적으로 구성, 운영되고 있는가에 대해서 확인을 해야 합니다.

3.3.3 Automated Restore/Recovery of the IDB

Data protector 에서 IDB Hot Backup 을 하게 되면

```
/var/opt/omni/db40/logfiles/rlog  
/omni_home/db40/logfiles/rlog
```

위 디렉토리의 **obrindex.dat** 파일에 IDB 백업 정보가 저장 됩니다.

(해당 파일은 최초 IDB Hot Backup 작업 시 생성 됩니다.)

Data protector 는 IDB Hot 백업에 이용된 device & Media 제어에 이상이 없는 경우 이 정보를 바탕으로 저장된 IDB Hot Backup Data 를 이용 하여 자동으로 IDB Restore & Recovery 를 수행 할 수 있습니다.

< Auto Recovery 절차 >

1) Service 종료 : 현재 작업중인 Session 이 없는지를 확인한 후 Service 종료
omnisv stop

2) omnidbrestore 명령어 실행

```
/opt/omni/sbin/omnidbrestore -autorecover ( 마지막 IDB 백업 version 을 이용 하여 복원 )  
WDP_HOME\bin\Womnidbrestore -autorecover
```

**** omnidbrestore 명령어는 help 를 참조 하세요 ****

PART 2 에서 계속 됩니다...