

HP OpenView Storage Data Protector Integration Guide

**for IBM Applications:
Informix
DB2
Lotus Notes/Domino**

Manual Edition: October 2004



Manufacturing Part Number: B6960-90110

Release A.05.50

© Copyright Hewlett-Packard Development Company, L.P.2004.

Legal Notices

©Copyright 2004 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

UNIX® is a registered trademark of The Open Group.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

ARM® is a registered trademark of ARM Limited.

1. Integrating Informix and Data Protector

In This Chapter	2
Overview	3
Prerequisites and Limitations	6
Integration Concepts	7
Data Protector Informix Configuration File	9
Setting, Retrieving, and Listing Data Protector Informix Configuration File Parameters Using the CLI	10
Configuring the Integration	13
Before You Begin Configuring	13
Configuring an Informix User in Data Protector	16
Configuring an OnLine Server	19
Configuring an Informix Backup	31
Testing the Integration	47
Using the Data Protector GUI	47
Using the Data Protector CLI	48
What Happens During the Testing?	50
Backing Up an Informix Database	51
Scheduling an Existing Backup Specification	54
Running an Interactive Backup	56
On-Demand and Continuous Backups	63
Restoring an Informix Database	65
Finding Information for Restore Using the Data Protector CLI	66
Finding Information for Restore Using the Data Protector GUI	68
Restore Using the Data Protector GUI	69
Restore Using Informix Commands	73
To Another OnLine Server	76
Using Another Device	77
Disaster Recovery	78
Monitoring an Informix Backup and Restore	79
Monitoring Current Sessions	79
Viewing Previous Sessions	80
Troubleshooting	81
Before You Begin	81
Troubleshooting on Windows Systems	81
Troubleshooting on UNIX Systems	89

Contents

2. Integrating IBM DB2 UDB and Data Protector

In This Chapter	104
Overview	105
Prerequisites and Limitations	107
Integration Concept	109
Configuring the Integration	115
Configuring a DB2 User	115
Configuring a DB2 Instance	116
Configuring a DB2 Backup	117
DB2 Specific Backup Options	124
Testing the Integration	126
Backing Up a DB2 Database	128
Scheduling an Existing Backup Specification	129
Running an Interactive Backup Using the Data Protector GUI	131
Running an Interactive Backup Using the Data Protector CLI	132
Restoring a DB2 Database	134
Restoring a DB2 Object Using the Data Protector GUI	135
Restore Options	140
Restoring a DB2 Object Using the Data Protector CLI	141
Monitoring a DB2 Backup and Restore	146
Monitoring Current Sessions	146
Viewing Previous Sessions	147
Troubleshooting	149
General Troubleshooting	149
Backup Problems	150
Restore Problems	152

3. Integrating Lotus Notes/Domino Server and Data Protector

In This Chapter	156
Overview	157
Prerequisites and Limitations	160
Integration Concepts	161
Configuring the Integration	164
Configuring the Lotus Notes/Domino Server	164
Configuring the Data Protector Lotus Integration	167
Testing the Integration	173
Backing Up Lotus Notes/Domino Server	176
Configuring a Lotus Notes/Domino Server Backup	177

Contents

Running an Online Backup	185
Restoring Lotus Notes/Domino Server Data	188
Restore Procedure	188
Restore Options	192
Monitoring a Lotus Notes/Domino Server Backup and Restore	195
Monitoring Current Sessions	195
Viewing Previous Sessions	196
Troubleshooting	198
General Troubleshooting	198
Checking Prerequisites Related to the Lotus Notes/Domino Server Side of the Integration	199
Configuration Problems	202
Backup Problems	204
Restore Problems	209
Recovery Problems	210
Before You Call Support	212

Glossary

Index

Contents

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Table 1

Edition History

Part Number	Manual Edition	Product
B6960-90110	October 2004	Data Protector Release A.05.50

Conventions

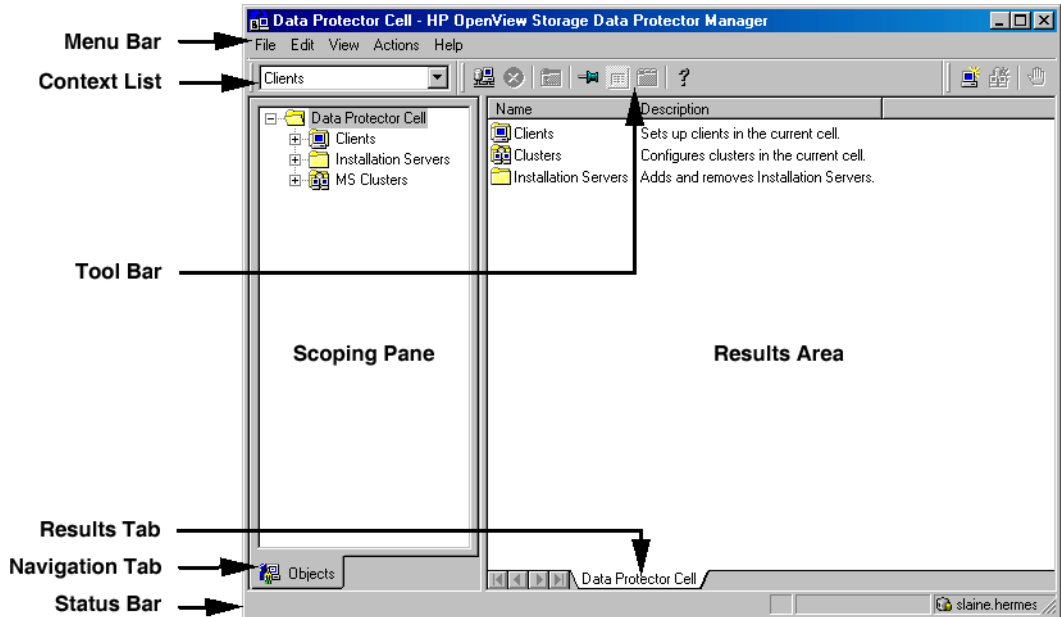
The following typographical conventions are used in this manual.

Table 2

Convention	Meaning	Example
<i>Italic</i>	Book or manual titles, and manual page names	Refer to the <i>HP OpenView Storage Data Protector Integration Guide</i> for more information.
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: rlogin <i>your_name</i> where you supply your login name.
Bold	New terms	The Data Protector Cell Manager is the main ...
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the grep command ...
	File and directory names	/usr/bin/X11
	Process names	Check to see if Data Protector Inet is running.
	Window/dialog box names	In the Backup Options dialog box...
	Text that you must enter	At the prompt, type: ls -l
Keycap	Keyboard keys	Press Return .

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information about the Data Protector graphical user interface.

Figure 1 Data Protector Graphical User Interface



Contact Information

General Information

General information about Data Protector can be found at

<http://www.hp.com/go/dataprotector>

Technical Support

Technical support information can be found at the HP Electronic Support Centers at

<http://support.openview.hp.com/support.jsp>

<http://www.hp.com/support>

Information about the latest Data Protector patches can be found at

http://support.openview.hp.com/patches/patch_index.jsp

For information on the Data Protector required patches, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

HP does not support third-party hardware and software. Contact the respective vendor for support.

Documentation Feedback

Your comments on the documentation help us to understand and meet your needs. You can provide feedback at

http://ovweb.external.hp.com/lpe/doc_serv/

Training Information

For information on currently available HP OpenView training, see the HP OpenView World Wide Web site at

<http://www.openview.hp.com/training/>

Follow the links to obtain information about scheduled classes, training at customer sites, and class registration.

Data Protector Documentation

Data Protector documentation comes in the form of manuals and online Help.

Manuals

Data Protector manuals are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `User Interface` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the manuals reside in the `<Data_Protector_home>\docs` directory on Windows and in the `/opt/omni/doc/C/` directory on UNIX. You can also find the manuals in PDF format at http://ovweb.external.hp.com/lpe/doc_serv/

HP OpenView Storage Data Protector Concepts Guide

This manual describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented *HP OpenView Storage Data Protector Administrator's Guide*.

HP OpenView Storage Data Protector Administrator's Guide

This manual describes typical configuration and administration tasks performed by a backup administrator, such as device configuration, media management, configuring a backup, and restoring data.

HP OpenView Storage Data Protector Installation and Licensing Guide

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

HP OpenView Storage Data Protector Integration Guide

This manual describes how to configure and use Data Protector to back up and restore various databases and applications. It is intended for backup administrators or operators. There are four versions of this manual:

- *HP OpenView Storage Data Protector Integration Guide for Microsoft Applications: SQL Server 7/2000, Exchange Server 5.x, Exchange Server 2000/2003, and Volume Shadow Copy Service*

This manual describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server 2000/2003, Microsoft Exchange Server 5.x, Microsoft SQL Server 7/2000, and Volume Shadow Copy Service.

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

This manual describes the integrations of Data Protector with Oracle, SAP R3, and SAP DB.

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

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

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

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

HP OpenView Storage Data Protector Integration Guide for HP OpenView

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

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for UNIX

This manual describes how to monitor and manage the health and performance of the Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and HP OpenView Performance (OVP) on UNIX.

HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations for Windows

This manual describes how to monitor and manage the health and performance of the Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and HP OpenView Performance (OVP) on Windows.

HP OpenView Storage Data Protector Zero Downtime Backup Concepts Guide

This manual 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 OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide* and the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*.

HP OpenView Storage Data Protector Zero Downtime Backup Administrator's Guide

This manual 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 OpenView Storage Data Protector Zero Downtime Backup Integration Guide

This manual 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 2000/2003, and Microsoft SQL Server 2000 databases. The manual also describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.

HP OpenView Storage Data Protector MPE/iX System User Guide

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

HP OpenView Storage Data Protector Media Operations User's Guide

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

HP OpenView Storage Data Protector Software Release Notes

This manual gives a description of new features of HP OpenView Storage Data Protector A.05.50. 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.openview.hp.com/products/datapro/spec_0001.html.

Online Help

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

In This Book

The *HP OpenView Storage Data Protector Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino* describes how to configure and use Data Protector with IBM applications.

Audience

This manual is intended for backup administrators who are responsible for the planning, setup, and maintenance of network backups. It assumes that you are familiar with:

- Basic Data Protector functionality
- Database administration

Conceptual information can be found in the *HP OpenView Storage Data Protector Concepts Guide*, which is recommended to fully understand the fundamentals and the model of Data Protector.

Organization

The manual is organized as follows:

- Chapter 1** “Integrating Informix and Data Protector” on page 1.
- Chapter 2** “Integrating Lotus Notes/Domino Server and Data Protector” on page 155.
- Chapter 3** “Integrating IBM DB2 UDB and Data Protector” on page 103.
- Glossary** Definition of terms used in this manual.

The integrations of Data Protector with the following database applications are described in the *HP OpenView Storage Data Protector Integration Guide for Microsoft Applications: SQL Server 7/2000, Exchange Server 5.x, Exchange Server 2000/2003, and Volume Shadow Copy Service*:

- Microsoft SQL Server 7.0/2000
- Microsoft Exchange Server 5.x
- Microsoft Exchange Server 2000/2003
- Microsoft Volume Shadow Copy Service

The integrations of Data Protector with the following database applications are described in the *HP OpenView Storage Data Protector Integration Guide for Oracle and SAP*:

- Oracle
- SAP R/3
- SAP DB

The integrations of Data Protector with the following database applications are described in the *HP OpenView Storage Data Protector Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol*:

- Sybase
- Network Node Manager
- Network Data Management Protocol

The integrations of Data Protector ZDB integrations with the following applications or operating system services are described in the *HP OpenView Storage Data Protector Zero Downtime Backup Integration Guide*:

- Oracle
- SAP R/3
- Microsoft SQL Server 7.0/2000
- Microsoft Volume Shadow Copy Service
- Microsoft Exchange Server 2000/2003

1**Integrating Informix and Data Protector**

In This Chapter

This chapter explains how to configure and use the Data Protector Informix integration. It explains the concepts and methods that you need to understand to back up and restore Informix **dbobjects**. Information pertaining to Informix refers to OnLine Dynamic Server.

The chapter is organized into the following sections:

“Overview” on page 3

“Prerequisites and Limitations” on page 6

“Integration Concepts” on page 7

“Data Protector Informix Configuration File” on page 9

“Configuring the Integration” on page 13

“Testing the Integration” on page 47

“Backing Up an Informix Database” on page 51

“Restoring an Informix Database” on page 65

“Monitoring an Informix Backup and Restore” on page 79

“Troubleshooting” on page 81

Overview

Data Protector integrates with OnLine Server to offer the online backup of your Informix database objects, hereinafter referred to as dbobjects.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for up-to-date information about platforms supported by the integration.

The online backup concept is now widely accepted because it addresses the business requirement of high application availability. During the backup, OnLine Server is online and actively used. The backup is performed quickly and efficiently, with least impact on OnLine Server performance.

Backup Types

You can perform the following types of backups of your Informix dbobjects using the Data Protector User Interface:

- Interactive backup using any of the following backup types:
 - **Full**, at which a baseline (level-0) backup of the selected dbobjects is made
 - **Incr1**, which backs up all changes since the last full (level-0) backup
 - **Incr2**, which backs up all changes since the last incremental (level-1) backup

NOTE

The Informix terms level-0, level-1, and level-2 backup are equivalent to Data Protector terms full, incr1, and incr2 backup, respectively.

-
- Scheduled backup of selected Informix dbobjects. You can schedule the same backup types as for interactive backups. Data Protector allows you to define the date and time for your unattended backup to start. You can also use predefined backup schedules to simplify your configuration.

NOTE

You can also back up Informix dobjects using the Informix `onbar` command.

A backup is always executed on OnLine Server via the Informix **ON-Bar** system. The **onbar utility** communicates backup and restore requests to OnLine Server.

You can restore your Informix dobjects using the Data Protector GUI or the Informix `onbar` command. Data Protector allows you to perform various types of restores, giving you all the flexibility you need to recover your mission-critical data.

Why Use the Data Protector User Interface?

Backing up and restoring using the integration offers various advantages over backing up using OnLine Server alone:

- Central Management for all backup operations

You can manage backup operations from a central point. This is especially important in large business environments.

- Media Management

Data Protector has an advanced media management system, which allows you to keep track of all media and the status of each medium, set protection for stored data, fully automate operation, as well as organize and manage devices and media.

- Backup Management

Backed up data can be duplicated during or after the backup to increase fault tolerance of backups, to improve data security and availability, or for vaulting purposes.

- Scheduling

Data Protector has a built-in scheduler that allows you to automate backups to run periodically. With the Data Protector Scheduler, the backups you set will run unattended at the times you specify.

- Device Support

Data Protector supports a wide range of devices; from standalone drives to complex multiple drive libraries. Refer to the *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported devices and other information.

- Reporting

Data Protector has reporting capabilities that allow you to receive information about your backup environment. You can schedule reports to be issued at a specific time or attached to a predefined set of events, such as the end of a backup session or a mount request.

- Monitoring

Data Protector has a feature that allows you to monitor currently running sessions and view finished sessions from any system that has the Data Protector User Interface installed.

All backup sessions are logged in the built-in IDB, providing you with a history of activities that can be queried at a later time.

Prerequisites and Limitations

Prerequisite

Before you begin, ensure that you have correctly installed and configured OnLine Server and Data Protector. For additional information, refer to the:

- *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, devices, and other information.
- *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions on how to install Data Protector on various architectures.
- *HP OpenView Storage Data Protector Administrator's Guide* for instructions on how to configure and run backups
- *INFORMIX-OnLine Dynamic Server: Backup and Restore Guide* for more information on configuring and using INFORMIX-OnLine Dynamic Server

Audience

The primary audience of this chapter is the administrator who must backup and restore OnLine data using the Data Protector Informix integration. This chapter assumes that you are familiar with OnLine Server, the UNIX or Windows operating system, and basic Data Protector functionality. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for Data Protector details.

Limitations

Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a list of general Data Protector limitations. This section describes limitations specific to this integration.

- Do not use double quotes for object-specific pre-exec and post-exec commands. These commands are optionally entered as integration-specific options during the creation of backup specifications.
- On Windows, due to an Informix bug, you cannot perform an Informix restore by a logical log number on Windows with the Informix version 7.31.TC2.
- On Windows, cold restore of non-critical dbspaces is not possible.

Integration Concepts

Data Protector integrates with Informix through the Data Protector Database Library based on a common library called Data Protector BAR (**B**ackup **A**nd **R**estore). The Data Protector Database Library channels communication between the Data Protector Session Manager (SM), and, via the **XBSA interface**, the Informix onbar utility. See Figure 1-1 for the architecture of the Data Protector Informix integration.

Figure 1-1

Informix Backup Concept

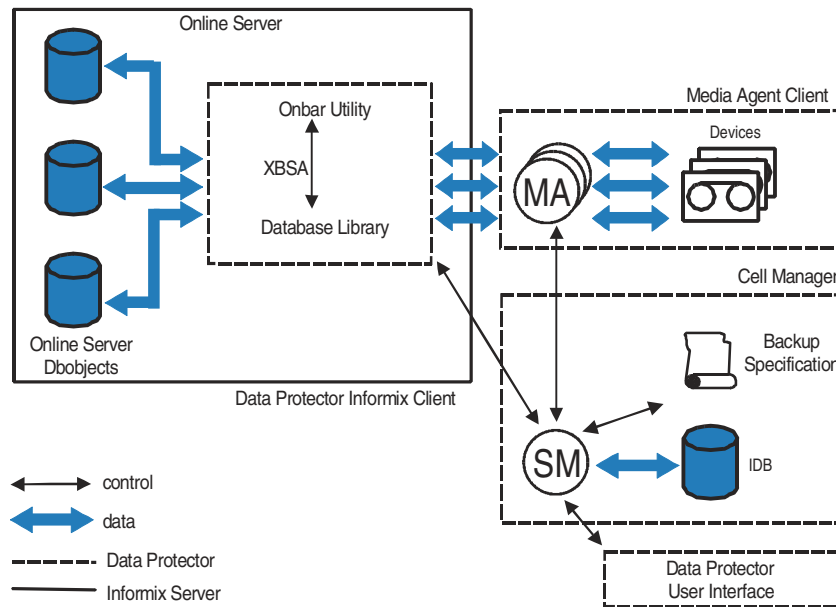


Table 1-1

Legend

SM	Data Protector Session Manager: Backup Session Manager during backup and Restore Session Manager during restore.
XBSA	X/Open Backup Services Application Programmer's Interface

Table 1-1

Legend

Database Library	The Data Protector set of routines that enables the data transfer between the OnLine Server and Data Protector.
MA	The Data Protector General Media Agent

Backup Specification

The onbar utility executes backup and restore requests coming from the Informix command-line and from Data Protector. The list of objects to be backed up, together with backup options and the set of devices to be used are kept in the Data Protector backup specification.

XBSA

The onbar utility and Data Protector exchange control as well as backup and restore data via the X/Open Backup Services Application Programmer's Interface (XBSA). When a request to execute a backup or restore is received, the onbar utility initiates a session with both OnLine Server and Data Protector.

Backup Flow

For a backup, the onbar utility requests dbobjects from OnLine Server and passes them to Data Protector. Data Protector then writes the data to devices.

Restore Flow

For a restore, Data Protector retrieves the requested dbobjects from media and sends them through the XBSA interface to the onbar utility, which sends the data to OnLine Server for writing to disk.

While OnLine Server is responsible for read/write operations to disk, Data Protector manages devices and media used for backup and restore sessions, and provides other powerful media management features before, during, and after backup sessions.

Data Protector Informix Configuration File

Data Protector stores the Informix integration parameters for every configured Informix *instance* in the following file on the Cell Manager:

- `/etc/opt/omni/server/integ/config/Informix/<client_name>%<instance_name>` (HP-UX and Solaris systems)
- `<Data_Protector_home>\Config\Server\Integ\Config\Informix\<client_name>%<instance_name>` (Windows systems).

The parameters stored in the configuration file are those entered during the configuration of this integration, as described in “Configuring an OnLine Server” on page 19. These parameters are:

- the Informix home directory.
- the full pathname of the OnLine Server `sqlhosts` file
- the filename of the OnLine Server `ONCONFIG` file

The Data Protector Informix configuration file is generated and parameters are written to it during the following events:

- configuration of the integration (using the `util_informix.exe` command or the Data Protector GUI)
- creation of a backup specification if the configuration parameters are changed
- when the configuration parameters are changed (using the `util_informix.exe` command, the `util_cmd` command, or the Data Protector GUI)

See “Configuring an OnLine Server” on page 19 for more information on configuring the integration using the `util_informix.exe` command or the Data Protector GUI. See “Setting, Retrieving, and Listing Data Protector Informix Configuration File Parameters Using the CLI” on page 10 for more information using the `util_cmd` command.

Configuration File Syntax The syntax of the file is as follows:

IMPORTANT To avoid problems with your backups, ensure that the syntax of your configuration file matches the examples by using the `util_informix.exe` command, the `util_cmd` command, or the Data Protector GUI. Do not edit the file manually.

```
HomeDir="<INFORMIXDIR>" //homedir path
SQLHosts="<sql_hosts>" //path of sqlhosts file
OnConfig="<ONCONFIG>" //path of onconfig file
Environment="{ }
```

Example of Configuration File This is an example of the Data Protector Informix configuration file:

```
HomeDir="/applications/informix73"
SQLHosts="/applications/informix73/etc/sqlhosts"
OnConfig="onconfig"
Environment="{ }
```

Setting, Retrieving, and Listing Data Protector Informix Configuration File Parameters Using the CLI

Data Protector Informix configuration file parameters are normally written to the Data Protector Informix configuration files after the completed configuration of the Informix instance in Data Protector using the `util_informix.exe` command or the Data Protector GUI.

The `util_cmd` Command

You can set, retrieve, or list the Data Protector Informix configuration file parameters using the `util_cmd -putopt` (setting a parameter), `util_cmd -getopt` (retrieving a parameter), or `util_cmd -getconf` (listing all parameters) command on the Data Protector Informix client. The command resides in the `/opt/omni/lbin` (HP-UX and Solaris systems), `/usr/omni/bin/` (other UNIX systems), or in the `<Data_Protector_home>\bin` (Windows systems) directory.

Cluster-Aware Clients

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before running the `util_cmd` command from the command line (on the client). The `OB2BARHOSTNAME` variable is set as follows:

- On UNIX: `export OB2BARHOSTNAME=<virtual_hostname>`
- On Windows: `set OB2BARHOSTNAME=<virtual_hostname>`

The `util_cmd` Synopsis

The syntax of the `util_cmd` command is as follows:

```
util_cmd -getconf[ig] Informix <Informix_instance> [-local \ <filename>]
```

```
util_cmd -getopt[ion] [Informix <Informix_instance>] \ <option_name> [-sub[list] <sublist_name>] [-local \ <filename>]
```

```
util_cmd -putopt[ion] [Informix <Informix_instance>] \ <option_name> [<option_value>] [-sub[list] <sublist_name>] \ [-local <filename>]
```

where:

`<option_name>` is the name of the parameter

`<option_value>` is the value for the parameter

`[-sub[list] <sublist_name>]` specifies the sublist in the configuration file which a parameter is written to or taken from.

`[-local <filename>]` specifies one of the following:

- When used with the `-getconf[ig]` option, it specifies a filename that the command output is written to. If the `-local` option is not specified, the output is written to the standard output.
- When used with the `-getopt[ion]`, it specifies a filename of the file from which the parameter and its value are to be retrieved from and then written to the standard output. If the `-local` option is not specified, the parameter and its value are retrieved from the Data Protector Informix configuration file and then written to the standard output.
- When use with the `-putopt[ion]` option, it specifies a filename for the output of the command to be written to. If the `-local` option is not specified, the output is written to the Data Protector Informix configuration file.

Return Values

The `util_cmd` command displays a short status message after each operation (written to the standard error):

- Configuration read/write operation successful.

This message is displayed when all the requested operations have been completed successfully

- Configuration option/file not found.

This message is displayed when either an option with the specified name does not exist in the configuration, or the file specified as the `-local` parameter does not exist.

- Configuration read/write operation failed.

This message is displayed if any fatal errors occurred, for example: the Cell Manager is unavailable or one of the Data Protector Informix configuration files is missing on the Cell Manager.

Configuring the Integration

After the installation, the integration is not yet ready for use. The following subsections provide instructions for configuring the integration.

To configure the integration, follow these steps:

Configuration Overview

1. Configure an Informix user.

This is a user with appropriate rights in both Data Protector and Informix environments as shown in “Configuring an Informix User in Data Protector” on page 16.

2. Configure an OnLine Server.

This is a client running OnLine Server. See “Configuring an OnLine Server” on page 19.

3. Configure an Informix backup.

Configure the devices and media needed for your backup, and create a Data Protector backup specification. See “Configuring an Informix Backup” on page 31.

Before You Begin Configuring

Check the following before you start configuring:

- ✓ OnLine Server is up and running

Before you start installing your integration software, ensure that your OnLine Server is running:

1. Log on to your OnLine Server. On UNIX, log on as the UNIX user `informix`.
2. Type in the following command:

UNIX

```
<INFORMIXDIR>/bin/onstat -d
```

Windows

```
<INFORMIXDIR>\bin\onstat -d
```

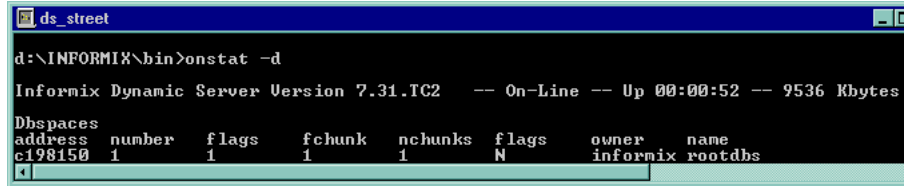
where `<INFORMIXDIR>` is the home directory of OnLine Server.

Integrating Informix and Data Protector

Configuring the Integration

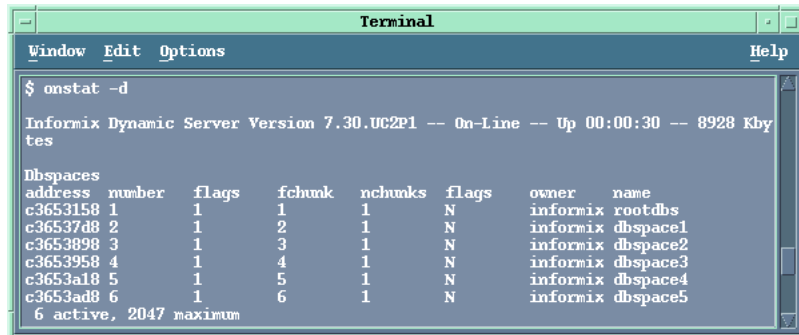
If OnLine Server is up and running, the `-- On-Line --` message is displayed as shown in Figure 1-2 and Figure 1-3.

Figure 1-2 Checking if OnLine Server Is Up (Windows Example)



```
ds_street
d:\INFORMIX\bin>onstat -d
Informix Dynamic Server Version 7.31.TC2 -- On-Line -- Up 00:00:52 -- 9536 Kbytes
Dbspaces
address number flags fchunk nchunks flags owner name
c198150 1 1 1 1 N informix rootdbs
```

Figure 1-3 Checking if OnLine Server Is Up (UNIX Example)



```
Terminal
Window Edit Options Help
$ onstat -d
Informix Dynamic Server Version 7.30.UC2P1 -- On-Line -- Up 00:00:30 -- 8928 Kbytes
Dbspaces
address number flags fchunk nchunks flags owner name
c3653158 1 1 1 1 N informix rootdbs
c36537d8 2 1 2 1 N informix dbspace1
c3653898 3 1 3 1 N informix dbspace2
c3653958 4 1 4 1 N informix dbspace3
c3653a18 5 1 5 1 N informix dbspace4
c3653ad8 6 1 6 1 N informix dbspace5
6 active, 2047 maximum
```

3. If OnLine Server is not up and running, proceed as follows to run it:
 - a. Log on to your OnLine Server. On UNIX, log on as the UNIX user `informix`.
 - b. Type in the following command:

UNIX

```
<INFORMIXDIR>/bin/oninit
```

Windows

```
<INFORMIXDIR>\bin\oninit
```

where `<INFORMIXDIR>` is the home directory of OnLine Server.

- ✓ You can successfully run a test backup of any filesystem on the system where the OnLine Server is running.

Configure and run a Data Protector backup of any filesystem on the system where the OnLine Server is running for test purposes. By doing this, you check whether OnLine Server and the Data Protector Cell Manager can communicate properly. In case of errors, this type of backup is much easier to troubleshoot than the integration itself. The configuration procedure includes installing a Disk Agent on OnLine Server, configuring appropriate devices and media (use any device), creating a filesystem backup specification, starting the backup, and then restoring the data. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

- ✓ The Informix Integration Module has been installed on all OnLine Servers you want to back up.
- ✓ For each client running OnLine Server, you will need to provide the following information:

Information Needed to Configure a Backup

- The Informix home directory, `<INFORMIXDIR>`, for example, `/applications/informix` (UNIX systems), or `d:\informix` (Windows systems).
- Filename of OnLine Server ONCONFIG configuration file, for example, `onconfig`. The ONCONFIG file is located in the `<INFORMIXDIR>/etc/` (UNIX systems), or in the `<INFORMIXDIR>\etc\` (Windows systems) directory, where `<INFORMIXDIR>` is the Informix home directory.
- The full pathname of the OnLine Server sqlhosts configuration file, for example, `/applications/informix/etc/sqlhosts` (UNIX systems) or `c:\informix\etc\sqlhosts` (Windows systems). The sqlhosts file is located in the `<INFORMIXDIR>/etc/` directory, where `<INFORMIXDIR>` is the Informix home directory.
- Name of OnLine Server. This is stored in the `INFORMIXSERVER` shell variable.

Log on to OnLine Server as the user `informix` (on UNIX, the user must be in group `informix`) and type in the following:

UNIX

```
echo $INFORMIXSERVER
```

Windows

```
echo %INFORMIXSERVER%
```

You should get the name of OnLine Server returned. In Figure 1-4 and Figure 1-5, the server is called `ODS730` (UNIX example), or `ds_street` (Windows example).

Figure 1-4 Finding the Name of OnLine Server (Windows Example)

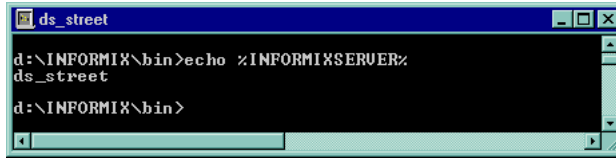


Figure 1-5 Finding the Name of OnLine Server (UNIX Example)



For more information, refer to the *INFORMIX-OnLine Dynamic Server: Backup and Restore Guide*.

Cluster-Aware Clients

- ✓ In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before running the configuration from the command line (on the client). When running the configuration from the GUI, this is not required. This is the command to be used:

- On UNIX: `export OB2BARHOSTNAME=<virtual_hostname>`
- On Windows: `set OB2BARHOSTNAME=<virtual_hostname>`

Configuring an Informix User in Data Protector

On UNIX, to start an Informix backup session, a user needs an operating system logon with sufficient privileges on the system where OnLine Server is running.

Who Is the Informix User?

To find an Informix user with sufficient backup and restore privileges, run the following command on OnLine Server:

```
$ ls -l <INFORMIXDIR>/bin/onbar
```

(for OnLine Server 7.2x)

or

```
$ ls -l <INFORMIXDIR>/bin/onbar_d
```

(for OnLine Server 7.3x)

where <INFORMIXDIR> is the home directory of OnLine Server.

OnLine Server returns the user, in this case the user root in the group informix with the following permissions:

```
-rwsr-sr-x 1 root informix 1569592 June 10 1999
/applications/informix73/bin/onbar_d
```

where <INFORMIXDIR> is /applications/informix73.

Owner of an Informix Backup Specification

Using that logon the user must be able to back up and restore Informix dbobjects. To start a backup of an Informix dbobject using Data Protector, the user must then become the owner of a Data Protector Informix backup specification.

This user (for example, the user root in the group informix) and the user informix in the group informix must be added to the Data Protector admin and operator groups.

Table 1-2 shows privileges of members of the Data Protector operator or admin groups. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for detailed information on user rights.

Table 1-2

Data Protector Admin and Operator User Groups and Their Access Rights

User Group	Access Rights
admin	Allowed to configure Data Protector and start backups, restores, and all other available operations. A member of this group has the rights of the root user on the UNIX or of the administrator on the Windows platform.
operator	Allowed to start backups and restores, and to respond to mount requests.

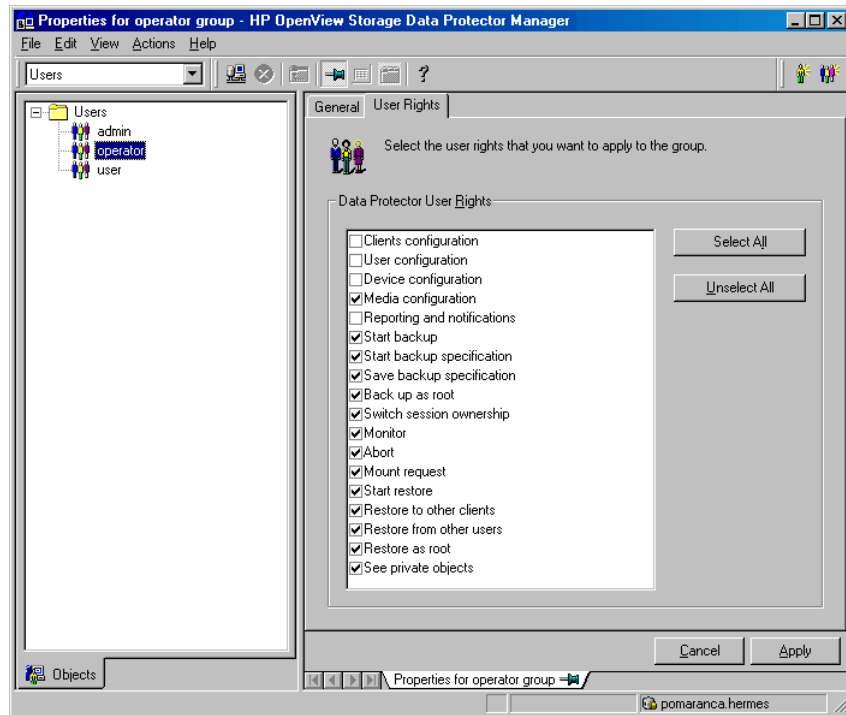
User Rights

Data Protector user rights are user configurable. Ensure that the See private objects user right of the Data Protector operator group is selected. This right allows a user to browse private objects. Note that this does not give the user permission to restore data. To configure this user right, proceed as follows:

Configuration Procedure

1. In the Context List, select Users.
2. In the Results Area, right-click Operator and click Properties.

Figure 1-6 Data Protector Operator Group User Rights



3. If the See private objects user right is selected, click Apply.

What's Next?

In this section you configured an Informix user, who has appropriate rights in both the Data Protector and Informix environments. You are now ready to configure your OnLine Server.

Configuring an OnLine Server

Each system running OnLine Server must be configured for proper integration with Data Protector.

Cluster-Aware Clients

When configuring the Data Protector Informix integration in a cluster environment, configure it only on one of the cluster nodes per one Informix server, because the configuration files reside on the Cell Manager. Use the cluster virtual hostname when configuring the integration.

IMPORTANT

On UNIX, *after* you have configured the Online Server, using either the CLI or GUI as described further on, make sure that the Informix user configured as described in the “Configuring an Informix User in Data Protector” on page 16 has permissions to read the Data Protector Informix configuration file. For more information on Data Protector Information configuration file, see “Data Protector Informix Configuration File” on page 9.

Before you configure an OnLine Server, ensure that OnLine Server is running. You can configure an OnLine Server using either the Data Protector CLI or the Data Protector GUI.

Using the Data Protector CLI

Cluster-Aware Clients

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before running the configuration from the command line (on the client). The `OB2BARHOSTNAME` variable is set as follows:

- On UNIX: `export OB2BARHOSTNAME=<virtual_hostname>`
- On Windows: `set OB2BARHOSTNAME=<virtual_hostname>`

Configuring an OnLine Server

To configure an OnLine Server, log in as user `root` (UNIX systems), or as user `informix` (Windows systems) on OnLine Server and execute the following command on the client you want to configure:

Windows

```
<Data_Protector_home>\bin\util_informix.exe -CONFIG  
<INFORMIXSERVER> <INFORMIXDIR> <SQL_HOSTS> <ONCONFIG>
```

Integrating Informix and Data Protector

Configuring the Integration

UNIX

```
/opt/omni/lbin/util_informix.exe -CONFIG <INFORMIXSERVER>  
<INFORMIXDIR> <SQL_HOSTS> <ONCONFIG> (HP-UX and Solaris systems)
```

```
/usr/omni/bin/util_informix.exe -CONFIG <INFORMIXSERVER>  
<INFORMIXDIR> <SQL_HOSTS> <ONCONFIG> (other UNIX systems)
```

where:

Informix Configuration Options

<INFORMIXSERVER> is the name of OnLine Server. If OnLine Server is configured in a cluster, this is the virtual hostname of the OnLine Server.

<INFORMIXDIR> is the Informix home directory.

<SQL_HOSTS> is the full pathname of the OnLine Server sqlhosts file.

<ONCONFIG> is the filename of the OnLine Server ONCONFIG file.

The following are example of the commands on various platforms:

Windows Example

```
<Data_Protector_home>\bin\util_informix.exe -CONFIG  
ds_street d:\informix \\STREET onconfig.ds_street
```

UNIX Example

```
/opt/omni/lbin/util_informix.exe -CONFIG  
ODS730 /applications/informix73  
/applications/informix73/etc/sqlhosts onconfig (HP-UX and  
Solaris systems)
```

```
/usr/omni/bin/util_informix.exe -CONFIG  
ODS730 /applications/informix73  
/applications/informix73/etc/sqlhosts onconfig (other UNIX  
systems)
```


Figure 1-7 OnLine Server CLI Configuration (Windows Example)

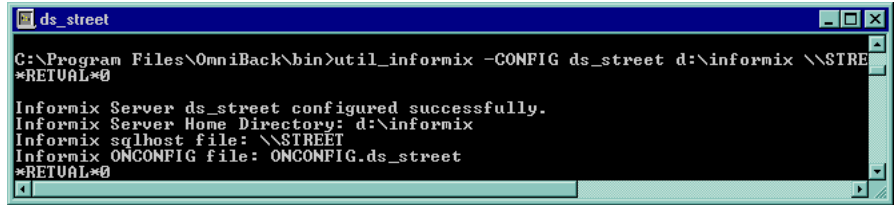
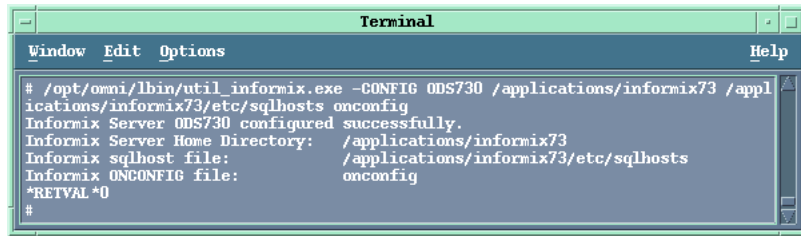


Figure 1-8 OnLine Server CLI Configuration (UNIX Example)



If the configuration is successful, the message, *RETNAL*0, is displayed. Otherwise, the error number is displayed in the form *RETNAL**<error number>*.

UNIX

To see more details about the error on UNIX, run the following command on OnLine Server:

```
/opt/omni/lbin/omnigetmsg 12 <error_number> (HP-UX and Solaris systems) or /usr/omni/bin/omnigetmsg 12 <error_number> (other UNIX systems).
```

or

Check the `/var/opt/omni/log/informix.log` file (HP-UX and Solaris systems) or `/usr/opt/omni/log/informix.log` file (other UNIX systems).

Windows

To see more details about the error on Windows, check the `<Data_Protector_home>\log\informix.log` and `<Data_Protector_home>\log\debug.log` files.

For more information, refer to the *INFORMIX-OnLine Dynamic Server: Backup and Restore Guide*.

What Happens? The following happens after saving the configuration.

1. The `util_informix.exe` saves the configuration parameters in the Data Protector Informix configuration file. For more information on Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
2. It verifies connections to OnLine Server.

What’s Next? Before you start configuring your Data Protector Informix backup specifications, check the configuration, as per instructions in “Checking the Informix Configuration” on page 28.

Using the Data Protector GUI

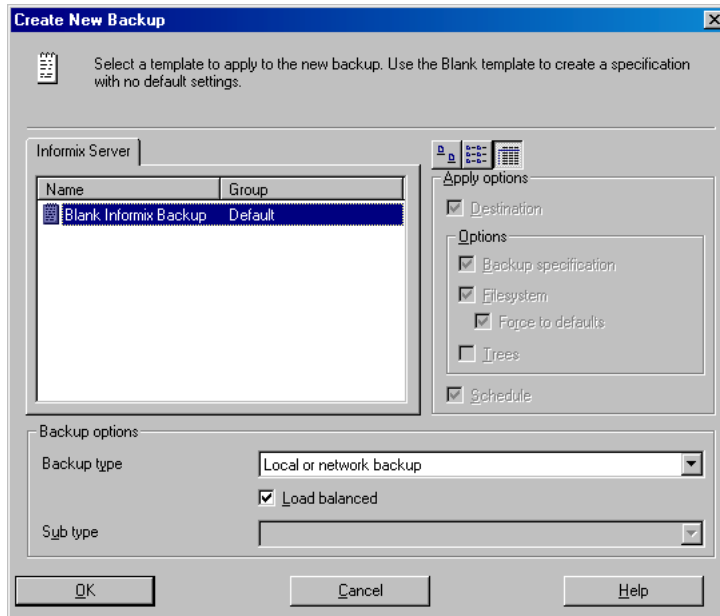
Log in as user `root` (UNIX systems), or `informix` (Windows systems) and perform the following steps in the HP OpenView Storage Data Protector Manager:

Configuring an OnLine Server

1. In the `Context List`, select `Backup`.
2. In the `Scoping Pane`, expand `Backup`, and then `Backup Specifications`. Right-click `Informix Server` and click `Add Backup`.

The `Create New Backup` dialog box is displayed.

Figure 1-9 **Selecting an Informix Backup Template**



Select the Load balanced option, which enables Data Protector to automatically balance the usage of devices that you select for the backup, thus ensuring equal usage of the devices. For more information about Data Protector load balancing, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

3. Click OK.

Figure 1-10

Configuring OnLine Server on UNIX Systems

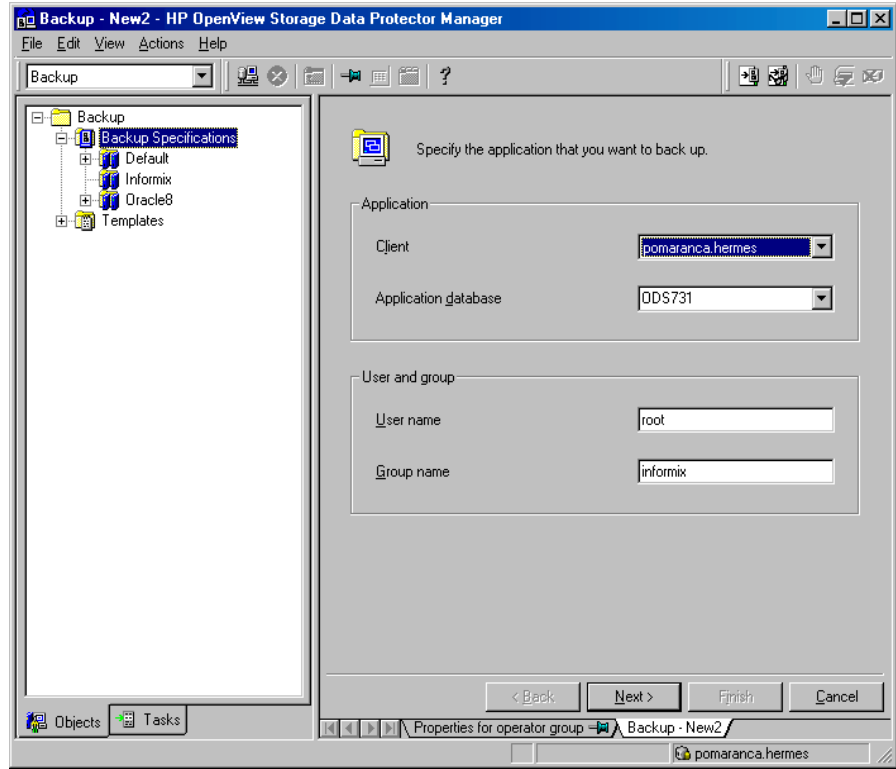
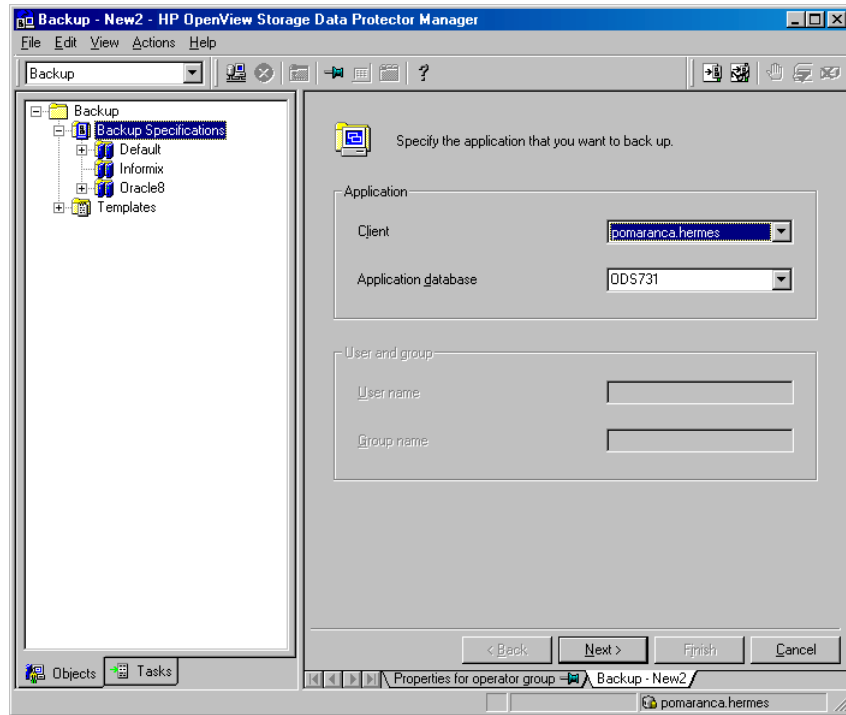


Figure 1-11 Configuring OnLine Server on Windows Systems



In the Results Area, enter the following information:

- The hostname of the OnLine Server you want to configure, for example, hase.hermes.
In a cluster environment, select the virtual hostname.
- The name of OnLine Server, for example, ODS731.
- On UNIX, the UNIX user name and user group of the Informix user, referred to in the section, “Configuring an Informix User in Data Protector” on page 16, for example, the user root in the group informix.

Click Next.

Integrating Informix and Data Protector Configuring the Integration

A message is displayed stating that the OnLine Server instance has not yet been configured.

Click OK.

The Configure Informix dialog box is displayed.

Figure 1-12 Configuring Informix on UNIX Systems

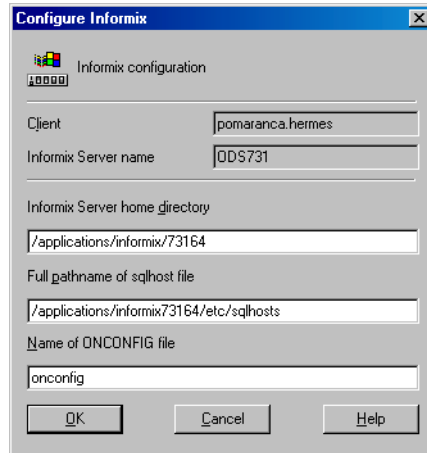
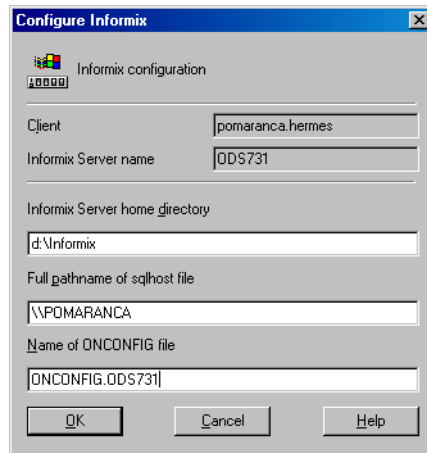


Figure 1-13 Configuring Informix on Windows Systems



4. In the Configure Informix window, enter the following information:

The Informix home directory, for example, /applications/informix73, full pathname of the sqlhosts file, and the name of the ONCONFIG file.

Click OK.

Upon successful configuration, a message like the one depicted in Figure 1-14 and Figure 1-15 is returned:

Figure 1-14 Success of the Configuration on Windows Systems

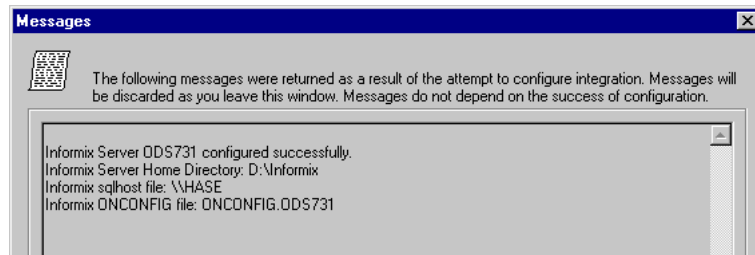
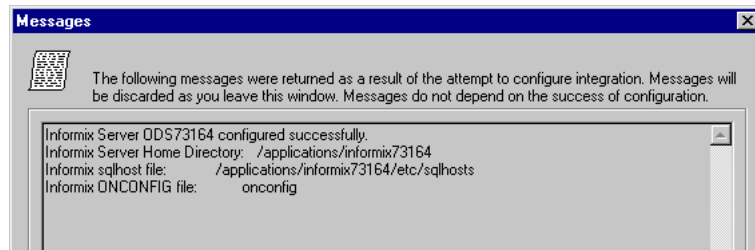


Figure 1-15 Success of the Configuration on UNIX Systems



The message states that the configuration was successful and also returns the name of the configured OnLine Server, the name of the OnLine Server home directory, the name of the Informix ONCONFIG file, and full pathname of the sqlhosts file.

Click OK.

Otherwise, an error number is displayed in the form *RETVAL**<error number>*.

Integrating Informix and Data Protector

Configuring the Integration

Windows

To see more details about the error on Windows, check the `<Data_Protector_home>\log\informix.log` and `<Data_Protector_home>\log\debug.log` files.

UNIX

To see more details about the error on UNIX, run the following command on OnLine Server:

```
opt/omni/sbin/omnigetmsg 12 <error_number> (HP-UX and Solaris systems) or /usr/omni/bin/omnigetmsg 12 <error_number> (other UNIX systems).
```

or

Check the `/var/opt/omni/log/informix.log` file (HP-UX and Solaris systems) or `/usr/omni/log/informix.log` file (other UNIX systems).

What Happens?

The following happens after saving the configuration.

Data Protector starts the file, `util_informix.exe`, on the OnLine Server, which performs the following:

1. The `util_informix.exe` saves the configuration parameters in the Data Protector Informix configuration file. For more information on Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
2. It verifies connections to OnLine Server.

What's Next?

Before you start configuring your Data Protector Informix backup specifications, check the configuration, as per instructions in “Checking the Informix Configuration” on page 28.

Checking the Informix Configuration

The Informix configuration can be checked either using the Data Protector CLI or using the Data Protector GUI.

Cluster-Aware Clients

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before checking the configuration from the command line (on the client). When checking the configuration from the GUI, this is not required. The `OB2BARHOSTNAME` variable is set as follows:

- On UNIX: `export OB2BARHOSTNAME=<virtual_hostname>`

- On Windows: set OB2BARHOSTNAME=<virtual_hostname>

Using the Data Protector CLI

To check the Informix configuration using the Data Protector CLI, start the following command:

Windows

```
<Data_Protector_home>\bin\util_informix.exe -CHKCONF  
<INFORMIXSERVER>
```

UNIX

```
/opt/omni/lbin/util_informix.exe -CHKCONF <INFORMIXSERVER>  
(HP-UX and Solaris systems)  
  
/usr/omni/bin/util_informix.exe -CHKCONF <INFORMIXSERVER>  
(other UNIX systems)
```

Figure 1-16

Checking the Informix Configuration Using the CLI (Windows Example)

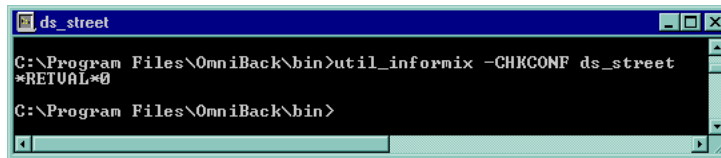


Figure 1-17

Checking the Informix Configuration Using the CLI (UNIX Example)



If the configuration is successful, the message, *RETVAL*0, is displayed.

Windows

On Windows, if an error occurs, the error number is displayed in the form *RETVAL*<error number>.

To see more details about the error, check the
<Data_Protector_home>\log\informix.log and
<Data_Protector_home>\log\debug.log files.

UNIX

On UNIX, if an error occurs, the error number is displayed in the form *RETVAL*<error number>.

To see more details about the error, run the following command on OnLine Server:

```
/opt/omni/sbin/omnigetmsg 12 <error_number> (HP-UX and Solaris systems) or /usr/omni/bin/omnigetmsg 12 <error_number> (other UNIX systems).
```

or

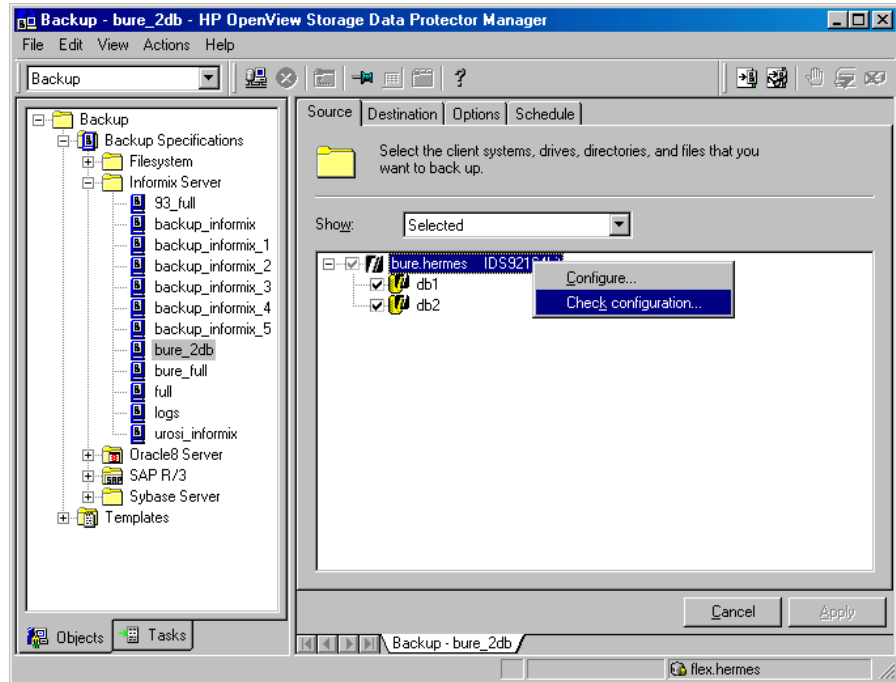
Check the `/var/opt/omni/log/informix.log` file (HP-UX and Solaris systems) or `/usr/omni/log/informix.log` file (other UNIX systems).

Using the Data Protector GUI

You can also check the configuration of your OnLine Server by performing the following steps in the HP OpenView Storage Data Protector Manager:

1. In the Context List, select Backup.
2. In the Scoping Pane, expand Backup, then Backup Specifications, and then Informix Server.
3. Go over the configuration procedure described in “Using the Data Protector GUI” on page 22.
Or, if you have already configured a backup specification, click it. The OnLine Server is displayed.
4. Right-click the client and then click Check Configuration.

Figure 1-18 Checking the Informix Configuration Using the Data Protector GUI



5. A message is returned confirming that the integration is properly configured.

What's Next?

Now that you have successfully configured your OnLine Server, you can configure your backup.

Configuring an Informix Backup

To run backups and restores of your Informix dbobjects, you need to configure Data Protector Informix backup specifications.

To configure the backup of Informix dbobjects, perform the following general steps:

Configuration Procedure

1. Configure devices, media, and media pools needed for the backup. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.
2. Create a Data Protector Informix backup specification specifying the data that you want to back up, the media and devices to which you want your data to be backed up, as well as Data Protector backup options that define the behavior of your backup or restore session.

Before You Begin

Perform the following preliminary tasks before creating your backup specification:

NOTE

Only general guidelines are given here. Refer to the *INFORMIX-Online Dynamic Server: Backup and Restore Guide* for detailed information about these tasks.

- ✓ Ensure that you have sufficient logical log space to create a backup.
If the total available space in the logical log (all the logical log files) is less than half of a single log file, OnLine Server does not create a backup.
- ✓ Print or keep a copy of your ONCONFIG file, the emergency boot file, and on UNIX, the sqlhosts file.
You need this information when you create a level-0 backup.
- ✓ Verify data consistency.
- ✓ Synchronize with other administrative tasks.

Creating a Data Protector Informix Backup Specification

On UNIX, ensure that you have appropriate privileges. See “Configuring an Informix User in Data Protector” on page 16 for more information.

An Informix backup specification is created using the Data Protector GUI.

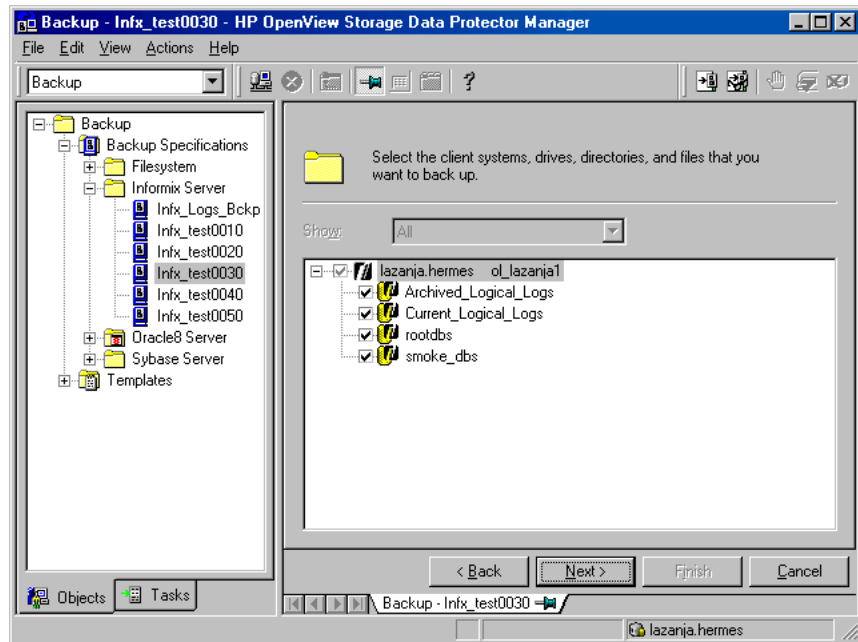
To create a Data Protector Informix backup specification on a client on which no backup specification has yet been configured, proceed from where you left off in “Using the Data Protector GUI” on page 22, or in “Using the Data Protector CLI” on page 19.

Procedure to Create a Backup Specification

1. In the Results Area, select the dbobjects you want to back up. The dbobjects include dbspaces, archive logical-logs, current logical-logs, and the root dbspace.

Figure 1-19

Selecting dbobjects to Backup



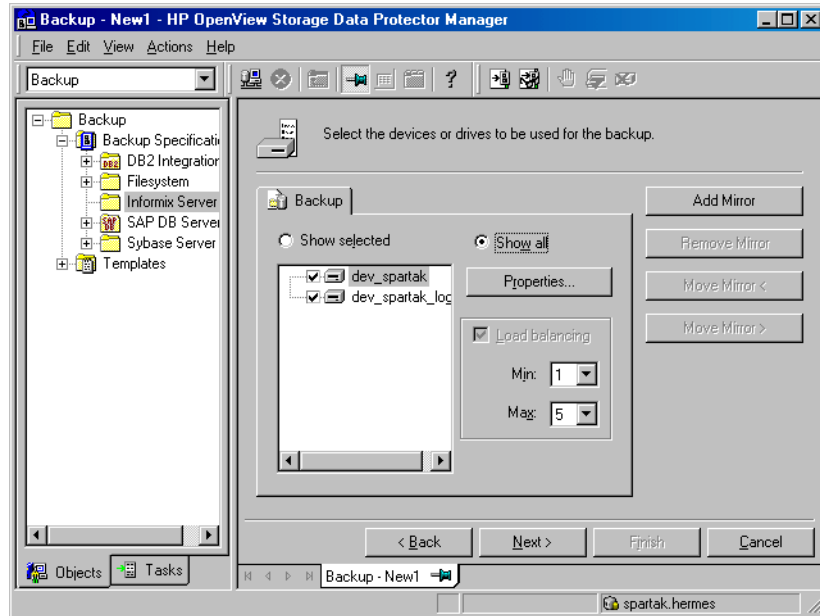
Click Next.

NOTE

If you still have not configured your devices and media, do so now. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

2. Select devices and media needed for your backup. For details, press F1.

Figure 1-20 Specifying Backup Devices



Allocate n primary devices that cover all resource types to be backed up. A typical configuration may include one device for logical logs and one for all other types.

Allocate m devices as secondary devices that cover all resource types in case any of the primary devices fails.

Specify the Load Balancing option. With this option set, Data Protector dynamically assigns backup objects to available devices. This enables devices to be used evenly and for backups to continue on available devices in case of failure of some device.

Specify the number of the primary devices (n) for the minimum and maximum value.

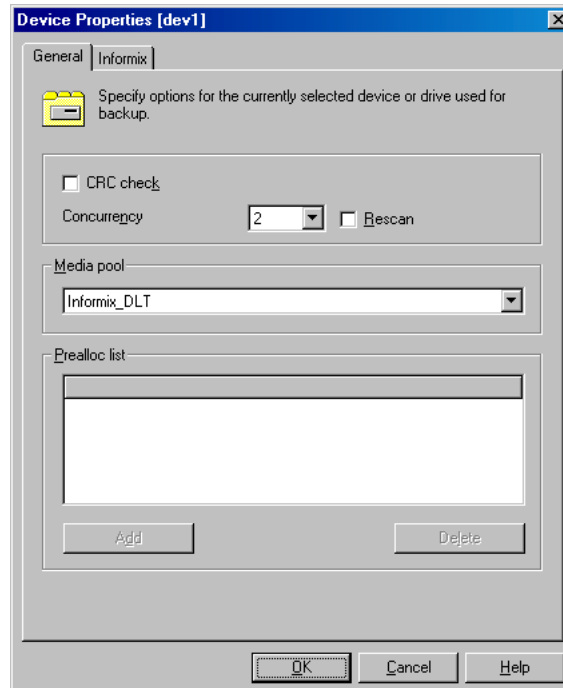
Make sure primary devices are not locked prior to starting Informix backup. You can do so by scheduling backups appropriately. If this is not true, secondary devices with possibly wrong resource type may get used.

You can also specify whether you want to create additional copies (mirrors) of the backup during the backup session. Specify the desired number of mirrors by clicking the *Add mirror* and *Remove mirror* buttons. Select separate devices for the backup and for each mirror.

For detailed information on the object mirror functionality, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Select a device you want to use and click *Properties*. The *Device Properties* dialog box is displayed. Specify the number of parallel backup streams in the *Concurrency* tab and the media pool you will use.

Figure 1-21 Specifying Device Properties

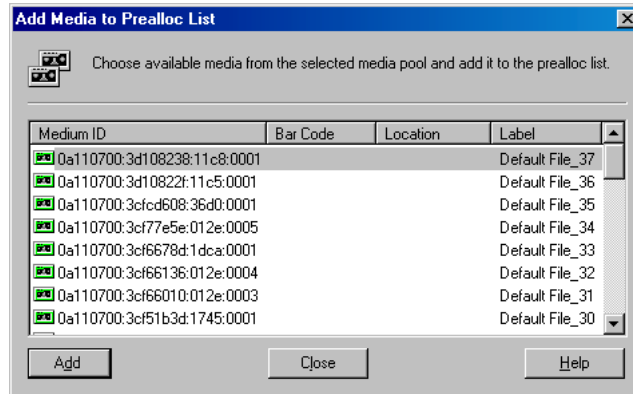


NOTE

Except for whole-system backups and restores, OnLine Server backs up and restores dbobjects concurrently to achieve better performance than it would if it backed up or restored dbobjects serially. ON-Bar creates a new process for each object up to a limit specified by the BAR_MAX_BACKUP configuration parameter.

Click Add to add specific media to the Prealloc list (a subset of media in the media pool used for backup), which specifies the order in which media are used for backup.

Figure 1-22 Adding Media to a Prealloc List



Select the media and click Add until all the media subsets have been added to the Prealloc List, and then click the Informix tab to set Informix resource types.

The resource type determines the types of dbobjects that will be backed up on this device. For example, if the resource type is set to R, only the root dbspace is backed up to this device.

The valid resource types are shown in Table 1-3.

Table 1-3 **Device Resources**

Resource Type	Description
B	blob space
CD	critical dbspace*
L	logical log
MR	master root dbspace
ND	noncritical dbspace
R	root dbspace

Legend

* The following dbspaces are critical dbspaces (CD):

A root dbspace

A dbspace that contains the physical log

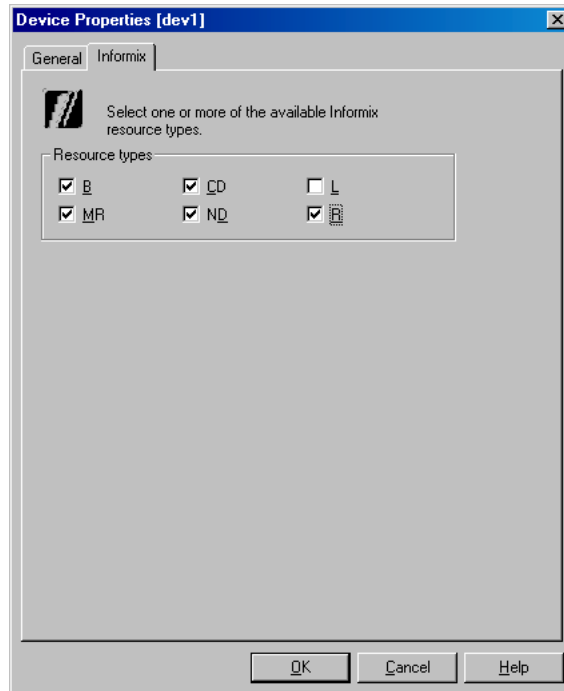
Any dbspace that contains a logical log file

As an example, select all types, except L. You will back up logical logs on a different medium dedicated only for that purpose.

NOTE

To backup logical logs, the `LTAPE` parameter in the `ONCONFIG` file must be set to a value that is not `/dev/null` or `' '`. The value will be ignored and the backup will be performed.

Figure 1-23 Informix Resource Types

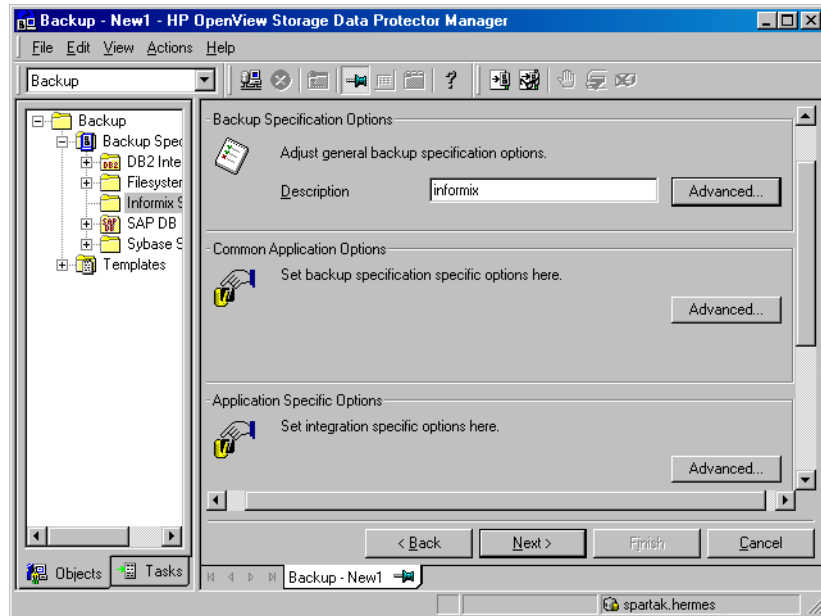


Click OK.

Repeat this step until you specify properties for all media.

3. Click Next to specify backup options.

Figure 1-24 Specifying Backup Options



Object-Specific Pre-Exec and Post-Exec Commands

Under Application Specific Options, click Advanced, to specify pre-exec and post-exec commands that will be started before ob2onbar is started on the Informix server and after it has finished.

These commands are different from the pre-exec and post-exec commands in the Backup Options dialog box (which you reach by clicking Advanced under Backup Specification Options) in that they are started by BSM on any specified client before and after ob2onbar is started and finished on the Informix server.

Under Informix Integration, optionally specify the following:

- Pre-exec

A command that will be started on the OnLine Server before backup. The command is started by the `ob2onbar.exe` command. On Windows, the command must reside in the `<Data_Protector_home>\bin` directory and only the filename must be provided in the backup specification. On UNIX, the full path for the command must be provided.

TIP

Use the `onmode -l OnLine` command as a Pre-exec command, to ensure that you always have a log file to back up. This is useful if you specified a logical log backup, since the backup will fail if there are no logical logs to back up.

- Post-exec

A command that will be started on the OnLine Server after backup. The command is started by the `ob2onbar.exe` command. On Windows, the command must reside in the `<Data_Protector_home>\bin` directory and only the filename must be provided in the backup specification. On UNIX, the full path for the command must be provided.

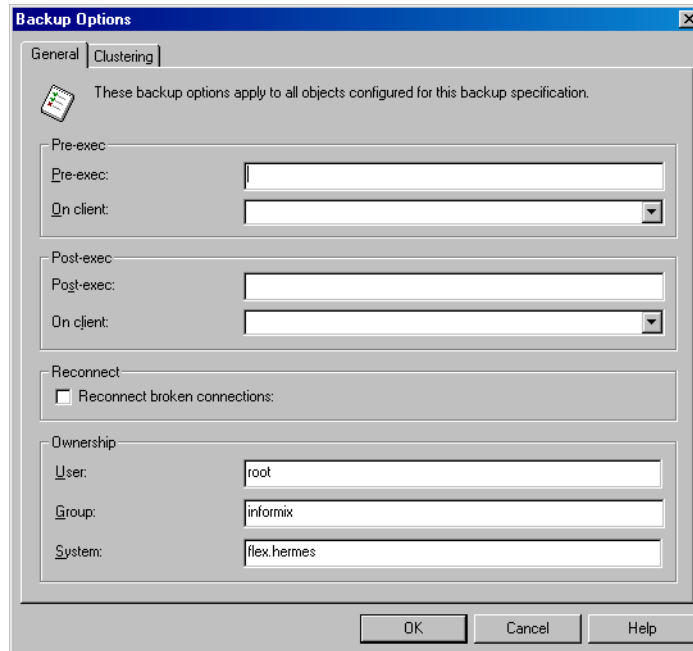
IMPORTANT

Do not use double quotes for object-specific pre-exec and post-exec commands.

Changing the Informix User on UNIX Systems

On UNIX, the Informix user is the person who configured the backup. Changing ownership allows another user to start the configured backup and to later restore the backed up data. To change the Informix user, click the `General` tab in the `Backup Options` dialog box. When you are done changing the user, click `OK` to return to the main backup options dialog box.

Figure 1-25 Changing the Informix User on UNIX Systems



Informix Whole-System Backup

A whole-system backup is a backup of all OnLine Server dbobjects from one `onbar` command. ON-Bar cannot back up dbobjects concurrently during a whole-system backup, so dbobjects are backed up serially. A whole-system backup is useful for disaster recovery and for restoring from a client other than the one to which the backup was made. If a computer's disk is completely destroyed and needs to be replaced with a new disk, you will need either a full (level-0) backup of every dbspace, blob space, and logical log file or a full (level-0) whole-system backup to completely restore data on the replacement computer.

As an example, select `Whole`, to make a whole-system Informix backup.

Figure 1-26 Whole-System Backup on Windows Systems

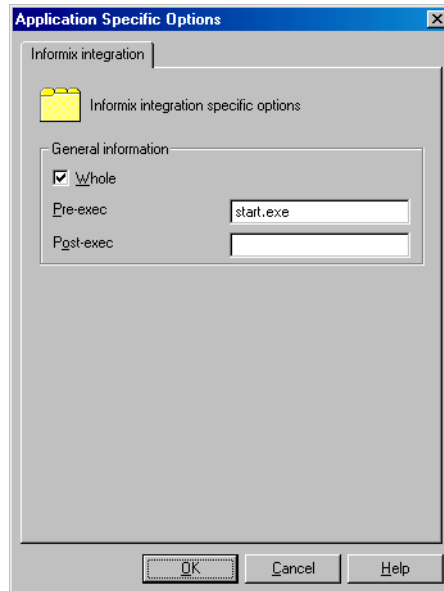
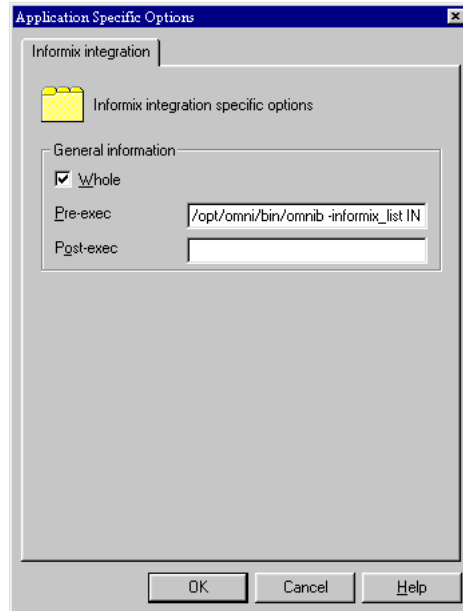


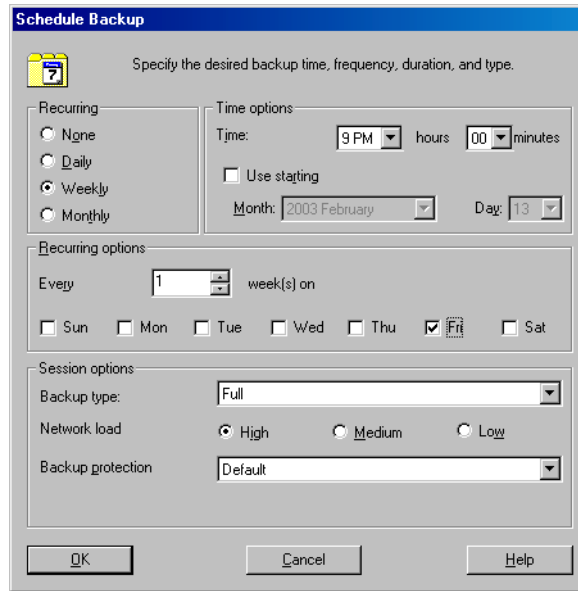
Figure 1-27 Whole-System Backup on UNIX Systems



4. Click OK and then Next, to schedule your backup specification. You can schedule your backup to start automatically and unattended on a specific date and time or at regular intervals for a period of up to a year in advance.

For example, to schedule a full backup to start at 9.00 p.m. every Friday, click Add to open the Schedule Backup dialog box and specify the options as shown in Figure 1-28.

Figure 1-28 Scheduling a Weekly Full Backup

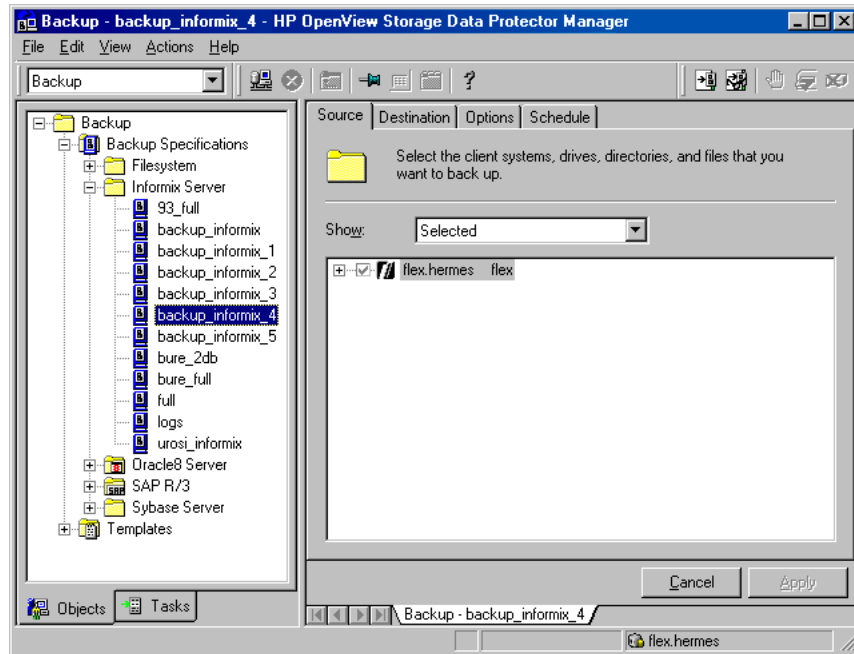


Click Next and then save your backup specification. Click Start Preview, to test your backup specification.

Editing Your Backup Specification

Now you have created your backup specification and are ready to run your backups. You can always revert to your backup specification to edit it by selecting it by name in the Backup context as shown in Figure 1-29. Click the appropriate tab and implement the changes you want. You need to save the backup specification afterwards.

Figure 1-29 **Editing a Backup Specification**



What's Next?

Follow the steps in this section to configure other backup specifications you might need, for example, a backup specification to back up logical logs.

Test your backup specifications thoroughly before using them for real. See “Testing the Integration” on page 47.

Configuring Informix Enterprise Decision Server (UNIX Systems Only)

Limitation

Currently the Informix Enterprise Decision Server (EDS) is supported only on HP-UX and Solaris. Refer to the latest versions of the Support Matrices at http://www.openview.hp.com/products/datapro/spec_0001.html for up-to-date information.

Integrating Informix and Data Protector

Configuring the Integration

The Informix Enterprise Decision Server uses onbar-workers to backup data. When a backup is started, the onbar starts onbar_d which then starts onbar-workers (if they are not running yet) using the `<Informix_home_dir>/etc/start_worker.sh` script. After onbar-workers are started, the onbar_d passes the information about what needs to be backed up to onbar-workers.

To configure a Data Protector Informix Enterprise Decision Server backup, you need to add the following lines to the `<Informix_home_dir>/etc/start_worker.sh` script after configuring and saving a backup specification:

```
export OB2APPNAME = <INFORMIXSERVERNAME>
export OB2BARLIST = <saved_backup_specification_name>
```

Testing the Integration

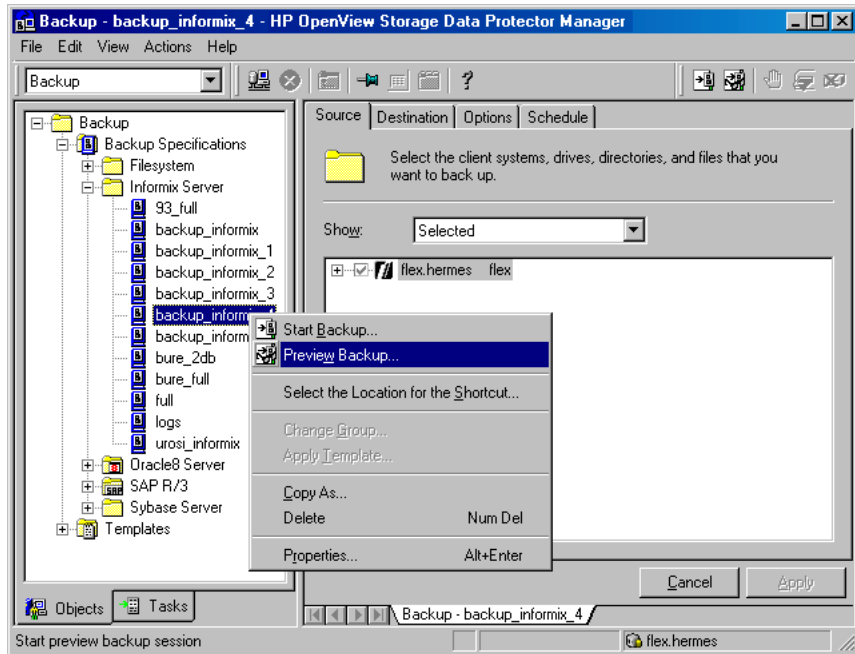
Test your backup specifications thoroughly by previewing them, then running them on file devices that are not NULL devices and then finally on the actual devices you intend to use. You can use either the Data Protector GUI or the Data Protector CLI.

Using the Data Protector GUI

To check if a backup specification has been properly configured, proceed with the following steps in the main HP OpenView Storage Data Protector Manager:

- Testing Procedure**
1. In the `Context List`, select `Backup`.
 2. In the `Scoping Pane`, expand `Backup`, and then `Backup Specifications`. Expand `Informix Server` and then right-click the backup specification you want to preview.

Figure 1-30 Testing the Informix Backup Specification



3. Click Preview Backup to open the Start Preview dialog box. Select the type of backup you want to run as well as the network load. For a description of these options, press **F1**.

Observe the generated messages. The “Session completed successfully” message is displayed at the end of a successful preview session.

Using the Data Protector CLI

You can also perform the same test using the Data Protector omnib command:

Windows

```
<Data_Protector_home>\bin\omnib -informix_list  
<backup_specification_name> -test_bar
```

UNIX

```
/opt/omni/bin/omnib -informix_list  
<backup_specification_name> -test_bar (HP-UX and Solaris  
systems)
```

```
/usr/omni/bin/omnib -informix_list
<backup_specification_name> -test_bar (other UNIX systems)
```

where <backup_specification_name> is the name of the backup specification to be tested.

Figure 1-31 Testing the IDS914 Backup Specification (UNIX Example)

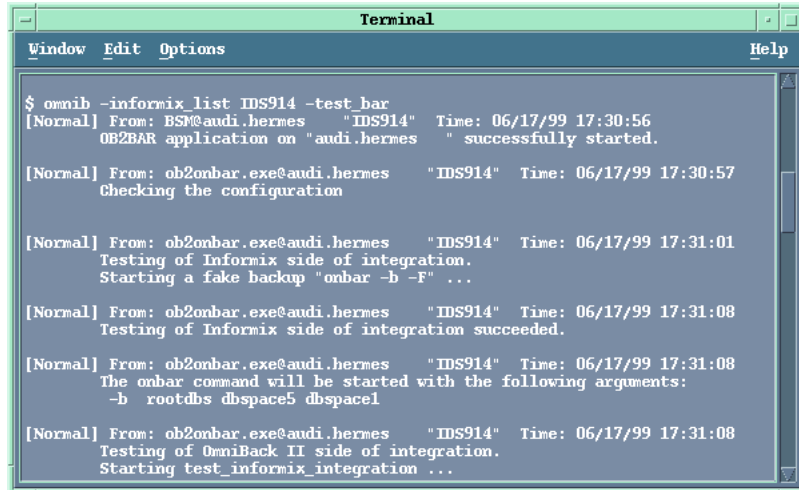
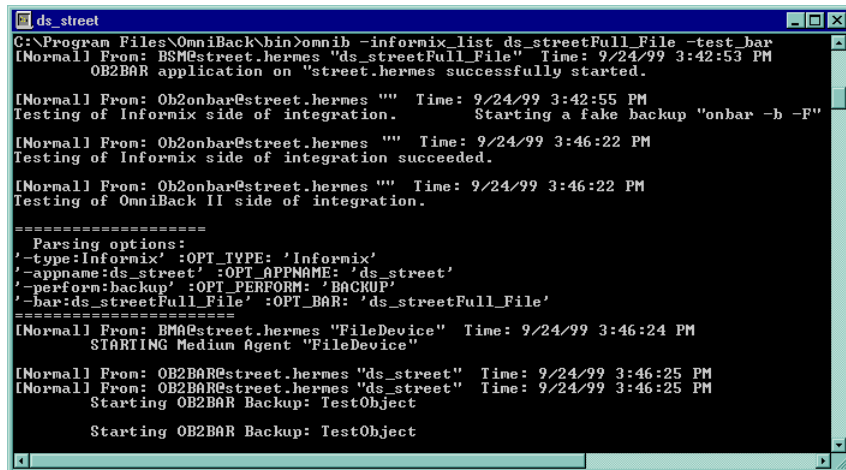


Figure 1-32 Testing the ds_street Backup Specification (Windows Example)



What Happens During the Testing?

The given procedure performs a backup preview that:

1. Starts the Informix `onbar` command with the `-F` Informix fake option, which tests if the Informix database is correctly configured for backup. This command only tests the Informix part of configuration.
2. Depending on the platform used, starts the following Data Protector command:

Windows

```
<Data_Protector_home>\bin\testbar.exe
```

UNIX

```
/opt/omni/bin/utilns/test_informix_integration or  
test_informix_integration_64bit (HP-UX and Solaris systems)  
  
/usr/omni/bin/utilns/test_informix_integration or  
test_informix_integration_64bit (other UNIX systems)
```

The command tests the following:

- Communication between the OnLine Server and Data Protector
- The syntax of the Informix backup specification
- If used devices are correctly specified
- If the needed media are in devices

Test Informix Integration Example

The `testbar.exe`, the `test_informix_integration`, or the `test_informix_integration_64bit` command only tests the Data Protector part of the configuration. You can run this command independently as shown in the following example:

Windows Example

```
<Data_Protector_home>\bin\testbar.exe -type:Informix  
-appname:ds_street -perform:backup -bar:InformixWhole
```

where `ds_street` is the name of OnLine Server and `InformixWhole` is the name of the backup specification that you want to test.

UNIX Example

```
/opt/omni/bin/utilns/test_informix_integration ODS730  
InformixWhole
```

where `ODS730` is the name of OnLine Server and `InformixWhole` is the name of the backup specification that you want to test.

Backing Up an Informix Database

In case of system failure, you can make a useful restore of your databases if *and only if* you have been making *regular* backups of the databases *and* logical-logs. This section describes how to configure and run backups of your Informix dbobjects.

To run a backup of Informix dbobjects, use any of the following methods:

Backup Methods

- Schedule the backup of an existing Informix backup specification using the Data Protector Scheduler. See “Scheduling an Existing Backup Specification” on page 54.
- Start an interactive backup of an existing Informix backup specification. You can start a backup using the Data Protector GUI or the Data Protector CLI. See “Using the Data Protector GUI” on page 56 or “Using the Data Protector CLI” on page 57.
- Start a backup using the Informix `onbar` command. See “Using Informix Commands” on page 59.
- On UNIX, start a backup using the Informix `log_full.sh` script. See “Using the Informix `log_full.sh` Script (UNIX Systems Only)” on page 62.

Backup Types

The Informix Data Protector integration provides online database backup of the following types:

Table 1-4

Informix Backup Types

Backup Type	Description
Full	Full backup
Incr1	First incremental backup. Backs up changes since the last full (level 0) backup.
Incr2	Second incremental backup. Backs up changes since the last incremental (level 1) backup.

Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for details on these backup types and on the syntax of the `onbar` utility.

What Happens?

The following happens when you start an Informix backup:

1. Data Protector executes the `ob2onbar.exe` command on the OnLine Server. This command checks the configuration of the integration and starts the `onbar` command.
2. During the backup session, the `onbar` utility receives data from OnLine Server, which reads data from disk. The `onbar` utility then sends the data to Data Protector for writing to devices.

Messages from the Data Protector backup session and messages generated by OnLine Server are logged to the IDB. Upon successful completion of the backup, the “Session completed successfully” message is displayed in the `Session Information` window.

What OnLine Server Does Not Back Up

OnLine Server backs up all `dbjects` with the following exceptions:

- `Dbospace` pages that are allocated to OnLine Server but are not yet allocated to a `tblspace` extent
- Configuration files
- Mirror chunks, if the corresponding primary chunks are accessible
- Blobs in `blobspaces` that are stored on optical platters
- Temporary `dbspaces`

What You Need to Back Up

In addition to OnLine `dbjects`, you should back up the files listed in the previous section, if you need them. You *must* back up the following files:

- `ONCONFIG` file, located in the `<INFORMIXDIR>\etc` (Windows systems), or in the `<INFORMIXDIR>/etc` (UNIX systems) directory.
- On UNIX, the `sqlhosts` file, located in the `<INFORMIXDIR>/etc` directory.
- `oncfg_<INFORMIXSERVER>.<SERVERNUM>` file, located in the `<INFORMIXDIR>\etc` (Windows systems), or in the `<INFORMIXDIR>/etc` (UNIX systems) directory.
- emergency boot file, an Informix configuration file that resides in the `<INFORMIXDIR>\etc` (Windows systems), or in the `<INFORMIXDIR>/etc` (UNIX systems) directory, and is called `ixbar.<server_id>`, where `<server_id>` is the value of the `<SERVERNUM>` configuration parameter.

IMPORTANT

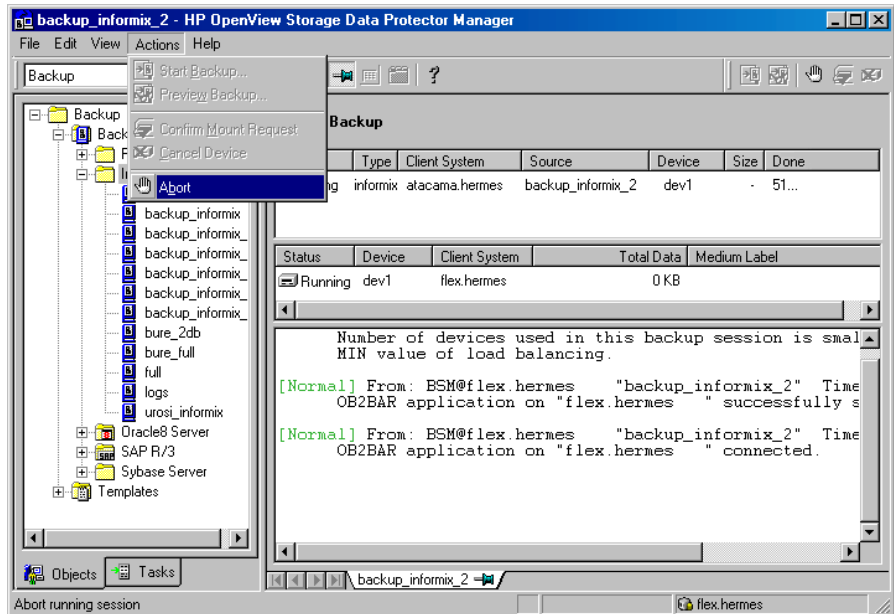
The Informix onbar utility does not back up these files. How often you need to back them up depends on how frequently changes are made to them. Back up the emergency boot file at least daily and always after you back up either a critical dbspace.

Aborting a Running Session

To abort a running Informix backup session, click **Abort** in the **Actions** menu, and then confirm the action.

In the following example, the backup session of the backup specification *InformixLogs* is being aborted.

Figure 1-33 Aborting an Informix Backup Session



IMPORTANT

The `BAR_RETRY` ON-Bar configuration parameter specifies how many times ON-Bar should retry a backup or restore operation if the first attempt fails. To successfully abort a backup or restore operation at the first attempt, set the `BAR_RETRY` value to 0. Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more information on this parameter.

Scheduling an Existing Backup Specification

For more detailed information on scheduling, refer to the online Help index keyword “scheduled backups”.

Data Protector allows you to run unattended backups at specific times or periodically. The powerful Data Protector Scheduler can highly influence the effectiveness and performance of your backup.

To schedule a new Informix backup specification, follow the steps described in “Creating a Data Protector Informix Backup Specification” on page 32.

To schedule an existing backup specification, perform the following steps in the HP OpenView Storage Data Protector Manager:

**Scheduling
Procedure**

1. In the `Context List`, select `Backup`.
2. In the `Scoping Pane`, expand `Backup`, then `Backup Specifications`. Click `Informix Server`.

A list of backup objects is displayed in the `Results Area`.

3. Double-click the backup specification you want to schedule and click the `Schedule` tab to open the `Schedule` property page.
4. In the `Schedule` property page, select a date in the calendar and click `Add` to open the `Schedule Backup` dialog box.
5. Specify `Recurring`, `Time options`, `Recurring options`, and `Session options`. See Figure 1-34 on page 55.
6. Click `OK` to return to the `Schedule` property page.
7. Click `Apply` to save the changes.

Scheduling Example

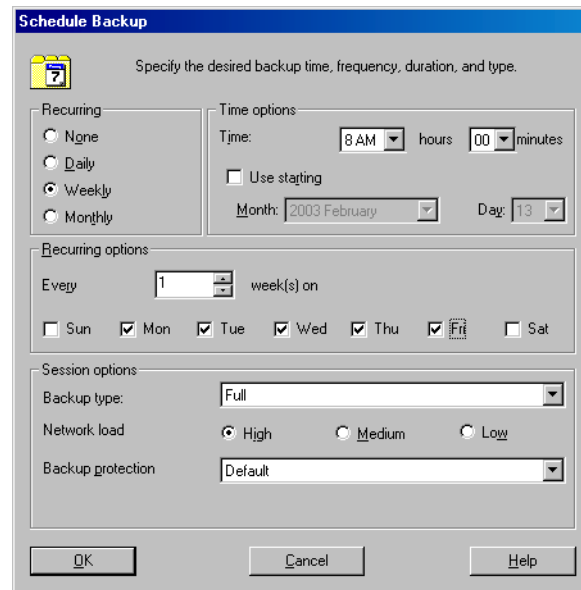
To schedule a backup specification called *InformixLogs* such that logical logs are backed up at 8.00 a.m., and then at 1.00 p.m. and at 6.00 p.m. during week days, open the *Schedule* property page of the backup specification as described in the above procedure, and then proceed as follows:

1. In the *Schedule* property page, select a date in the calendar and click *Add* to open the *Schedule Backup* dialog box.
2. Under *Recurring*, select *Weekly*. Under *Time options*, select the time 8 AM. Under *Recurring Options*, select *Mon, Tue, Wed, Thu, and Fri*. Leave other options as default and click *OK*.

See Figure 1-34 on page 55.

Figure 1-34

Scheduling the InformixLogs Backup Specification



3. Repeat steps 1 and 2 to schedule another backup. Specify options as described, except the time, which should be set to 1 PM.
4. Repeat steps 1 and 2 to schedule another backup. Specify options as described, except the time, which should be set to 6 PM.
5. Click *Apply* to save the changes.

Refer to the online Help or the *HP OpenView Storage Data Protector Administrator's Guide* for scheduling details.

After scheduling your backup, you can have it run unattended or you can still run it interactively, as shown in the next section.

Running an Interactive Backup

Interactive backups, as opposed to unattended scheduled backups, are run on demand. They are useful to test your scheduled backups, in case of failure of scheduled backups and to back up clients that need to be backed up urgently, before the regular scheduled periodic backup. You can run your interactive backups using the Data Protector GUI or the Data Protector CLI.

Using the Data Protector GUI

To start an interactive backup of an Informix dobject, perform the following steps in the HP OpenView Storage Data Protector Manager:

Running an Interactive Backup

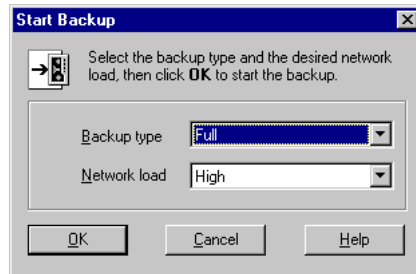
1. In the Context List, select Backup.
2. In the Scoping Pane, expand Backup, then Backup Specifications, and then Informix Server.
3. Select the backup specification you want to run and click Start Backup in the Actions menu.

TIP

You can also start a backup by right-clicking the Informix backup specification you want to back up and then clicking Start Backup.

The Start Backup dialog box is displayed.

Figure 1-35 Starting the Backup of the InformixWhole Backup Specification



Select the backup type {Full | Incr1 | Incr2} and network load {High | Medium | Low}. For a description of these options, press **F1**.

4. Click **OK**.

Upon successful completion of the backup session a message confirming the success of the session is displayed.

Using the Data Protector CLI

You can also start an interactive backup of an Informix dobject using the `omnib` command located in the `<Data_Protector_home>\bin` (Windows systems), `/opt/omni/bin/` (HP-UX and Solaris systems) or in the `/usr/omni/bin/` (other UNIX systems) directory:

```
omnib -informix_list <backup_specification_name>
                        [-barmode <InformixMode>]
                        [<List_options>]
```

`<InformixMode>` can be one of the following:

```
full|inf_incr1|inf_incr2
```

NOTE

The Informix terms level-0, level-1, and level-2 backup are equivalent to Data Protector terms full, inf_incr1, and inf_incr2 backup, respectively.

Table 1-5 Informix Backup Types

Backup Type	Onbar Arguments	Description
Full	-L 0	Full backup
Incr1	-L 1	First incremental backup. Backs up changes since the last full (level 0) backup.
Incr2	-L 2	Second incremental backup. Backs up changes since the last first incremental (level 1) backup.

<List_options> can be any of the following:

`-protect {none | weeks n | days n | until date | permanent}`

This option enables you to set the period of protection for the data you back up to prevent the backup media from being overwritten for the specified period. The default is permanent.

`-load {low | medium | high}`

This option enables you to set the network load during your backup. Set it to high for maximum performance and to low to reduce network load at busy times. The default is high.

`-crc`

Set this option on to have Data Protector calculate the cycle redundancy check when a backup is run. This option enables you to later confirm using the `Verify` option whether data has been correctly written to the medium. The default is off.

`-no_monitor`

By default, the command monitors the session and displays the status of the session.

```
-test_bar
```

Tests both the Informix and the Data Protector parts of the backup specification as described in “Testing the Integration” on page 47.

Backup Examples To start a full backup of the Informix backup specification called InformixWhole, execute the following command in the `<Data_Protector_home>\bin` (Windows systems), `/opt/omni/bin/` (HP-UX and Solaris systems) or in the `/usr/omni/bin/` (other UNIX systems) directory:

```
omnib -informix_list InformixWhole -barmode full
```

To start an incremental backup of the Informix backup specification called InformixIncr, execute the following command in the `<Data_Protector_home>\bin` (Windows systems), `/opt/omni/bin/` (HP-UX and Solaris systems) or in the `/usr/omni/bin/` (other UNIX systems) directory:

```
omnib -informix_list InformixIncr -barmode inf_incr1
```

Using Informix Commands

This chapter assumes that you are familiar with both OnLine Server and the UNIX or Windows operating system.

You can start a backup of an Informix dbject from the client where the database is located using the Informix onbar utility.

Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more details on the onbar utility.

Before You Begin Before running a backup using the onbar command, ensure that you are logged in as root (UNIX systems) or informix (Windows systems) and execute the following commands:

Windows

1. SET ONCONFIG=<onconfig_file>

Where <onconfig_file> is the name of OnLine Server ONCONFIG file, for example, ONCONFIG.

2. SET INFORMIXSQLHOSTS=<full_sqlhosts_file>

Where <full_sqlhosts_file> is the full pathname of the sqlhosts file, for example, c:\informix\etc\sqlhosts.

Integrating Informix and Data Protector

Backing Up an Informix Database

3. SET INFORMIXSERVER=<INFORMIXSERVER>

Where <INFORMIXSERVER> is the name of OnLine Server, for example, ds_street.

4. SET INFORMIXDIR=<Informix_home_dir>

Where <Informix_home_dir> is the home directory of OnLine Server, for example, d:\informix\.

5. SET OB2APPNAME=<INFORMIXSERVER>

Where <INFORMIXSERVER> is the name of OnLine Server, for example, ds_street.

6. SET OB2BARLIST=<backup_specification_name>

Where <backup_specification_name> is the name of the backup specification to be used for the backup, for example, InformixWhole.

Note that OB2APPNAME and OB2BARLIST are Data Protector-specific variables.

UNIX

1. export ONCONFIG=<onconfig_file>

Where <onconfig_file> is the name of OnLine Server ONCONFIG file, for example, ONCONFIG.

2. export INFORMIXSQLHOSTS=<full_sqlhosts_file>

Where <full_sqlhosts_file> is the full pathname of the sqlhosts file, for example, /applications/informix73/etc/sqlhosts.

3. export INFORMIXSERVER=<INFORMIXSERVER>

Where <INFORMIXSERVER> is the name of OnLine Server, for example, ODS730.

4. export INFORMIXDIR=<Informix_home_dir>

Where <Informix_home_dir> is the home directory of OnLine Server, for example, /applications/informix73/.

5. export OB2APPNAME=<INFORMIXSERVER>

Where <INFORMIXSERVER> is the name of OnLine Server, for example, ODS730.

6. export OB2BARLIST=<backup_specification_name>

Where <backup_specification_name> is the name of the backup specification to be used for the backup, for example, InformixWhole.

Note that `OB2APPNAME` and `OB2BARLIST` are Data Protector-specific variables.

OnLine Server has to be in online or in quiescent mode to perform a backup. Once you start a backup, do not change the mode until the backup finishes; changing the mode terminates your backup. Only online dbspaces and blobspaces are backed up. To see which dbobjects are online, type in the following command:

Windows `<INFORMIXDIR>\bin\onstat -d`

UNIX `<INFORMIXDIR>/bin/onstat -d`

where `<INFORMIXDIR>` is the home directory of OnLine Server.

Online Backups The online mode is convenient if you want your OnLine Server to be accessible while you create the backup. An online backup might contribute to a loss of performance.

Quiescent Backups The quiescent mode is useful when you want to eliminate partial transactions in a backup. A quiescent backup might not be practical if users need continuous access to OnLine Server databases.

Back Up Your Configuration Files Keep a copy of your `ONCONFIG`, emergency boot files, and on UNIX, `sqlhosts`, after you create a full backup. You need this information to restore OnLine Server dbobjects.

Onbar Utility Backup Examples To back up a list of dbspaces, proceed as follows:

```
onbar -b <dbspace_list>
```

To back up dbspaces `dbspace1` and `dbspace3`, type in the following command:

```
onbar -b dbspace1, dbspace3
```

To back up the current logical log file and switch to the next logical log file, use the `-c` option:

```
onbar -l -c
```

or

```
onbar -b -l -c
```

if you are using Informix 9.40.

Messages from the Data Protector backup session and messages generated by the Informix Integration Module are logged in the IDB. See “Monitoring an Informix Backup and Restore” on page 79 for additional information.

Using the Informix `log_full.sh` Script (UNIX Systems Only)

On UNIX, the **`log_full.sh`** script is used to start backing up logical log files when OnLine Server issues a log-full event alarm on the OnLine Server. See “On-Demand and Continuous Backups” for information on logical log file backups.

To enable an Informix backup from the `log_full.sh` script, follow these steps:

Backup Procedure

1. Add the following line to the Informix ONCONFIG configuration file:

```
ALARMPROGRAM <INFORMIXDIR>/etc/log_full.sh.
```

where `<INFORMIXDIR>` is the home directory of OnLine Server.

2. If you do not have the Data Protector User Interface installed on the OnLine Server, then create an Informix backup specification to back up logical logs only, and edit the `<INFORMIXDIR>/etc/log_full.sh` script.

Add the following at the beginning of the file:

```
export OB2BARLIST=<backup_specification_name>
```

```
export OB2APPNAME=<INFORMIXSERVER>
```

where `<backup_specification_name>` is the name of the Informix backup specification and `<INFORMIXSERVER>` is the name of OnLine Server.

3. If you have the Data Protector User Interface installed on the OnLine Server then create an Informix backup specification to back up logical logs only.

NOTE

The Informix Enterprise Decision Server does not use the `log_full.sh` script.

On-Demand and Continuous Backups

To back up all logical log files that are full and ready to be backed up, start an *on-demand* backup. An *on-demand* backup backs up all the full logical log files, then stops at the current logical log file.

You can also start a *continuous* backup on which OnLine Server backs up each logical log file as it becomes full. The *continuous* backup process then waits until the next log is full. Use continuous logical log backups, if you do not want to monitor the logical log files.

By default, the ALARMPROGRAM configuration parameter is set so that ON-Bar performs continuous backups.

IMPORTANT

If you use *continuous* backups, ensure that a device is always available for the logical log backup process.

See “Troubleshooting Logical Log Backups” on page 96 for information about troubleshooting logical log backups.

Examples

To make an *on-demand* backup of the logical log files that are full (instead of a *continuous* backup that takes place every time a logical log file fills), use the `-l` option as shown in the following example:

Windows Example

```
SET OB2BARLIST=<backup_specification_name>  
SET OB2APPNAME=<INFORMIXSERVER>  
  
onbar -l
```

To back up the current logical log file and switch to the next logical log file, use the `-c` option, as shown in the following example:

```
SET OB2BARLIST=<backup_specification_name>  
SET OB2APPNAME=<INFORMIXSERVER>  
  
onbar -l -c  
  
or  
  
onbar -b -l -c
```

if you are using Informix 9.40.

Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more information on *on-demand* and *continuous* backups.

UNIX Example

```
export OB2BARLIST=<backup_specification_name>  
export OB2APPNAME=<INFORMIXSERVER>  
onbar -l
```

To back up the current logical log file and switch to the next logical log file, use the `-c` option, as shown in the following example:

```
export OB2BARLIST=<backup_specification_name>  
export OB2APPNAME=<INFORMIXSERVER>  
onbar -l -c
```

or

```
onbar -b -l -c
```

if you are using Informix 9.40.

Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more information on *on-demand* and *continuous* backups.

Restoring an Informix Database

You can restore an Informix dbject in any of the following ways:

Restore Methods

- Using the Data Protector GUI. See “Restore Using the Data Protector GUI” on page 69.
- Using the Data Protector CLI. Refer to the `omnir` man page for more information.
- Using the `onbar` command on the OnLine Server. See “Restore Using Informix Commands” on page 73.

To restore a corrupted database, you need to find the right media and the session ID of the last backup session with a full backup. This and other information can be found using either the Data Protector CLI or the Data Protector GUI. See “Finding Information for Restore Using the Data Protector CLI” on page 66 or “Finding Information for Restore Using the Data Protector GUI” on page 68.

Cluster-Aware Clients

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before starting a restore procedure from the command line (on the client). When the GUI is used for restore, this is not required. The `OB2BARHOSTNAME` variable is set as follows:

- On UNIX: `export OB2BARHOSTNAME=<virtual_hostname>`
- On Windows: `set OB2BARHOSTNAME=<virtual_hostname>`

TIP

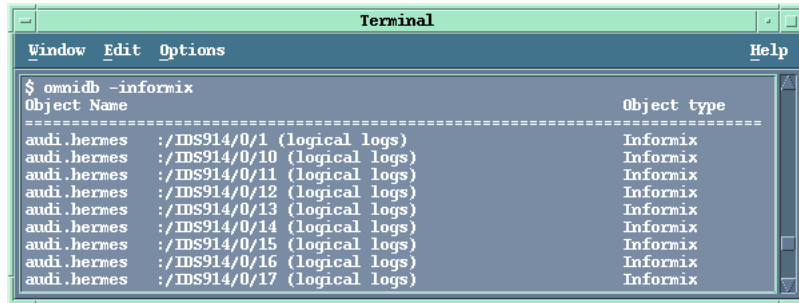
If the restore fails because the emergency boot file is too large, use the Informix ONBar `onsmsync` utility to remove expired backups from the Informix `sysutils` database and emergency boot file. Refer to the *IBM Informix Backup and Restore Guide* for more information on the Informix ONBar `onsmsync` utility. Note that the `onsmsync` utility was introduced with the Informix 7.3 release.

Finding Information for Restore Using the Data Protector CLI

To find the information needed to restore your data, execute the following commands in the `<Data_Protector_home>\bin` (Windows systems), `/opt/omni/bin/` (HP-UX and Solaris systems) or in the `/usr/omni/bin/` (other UNIX systems) directory:

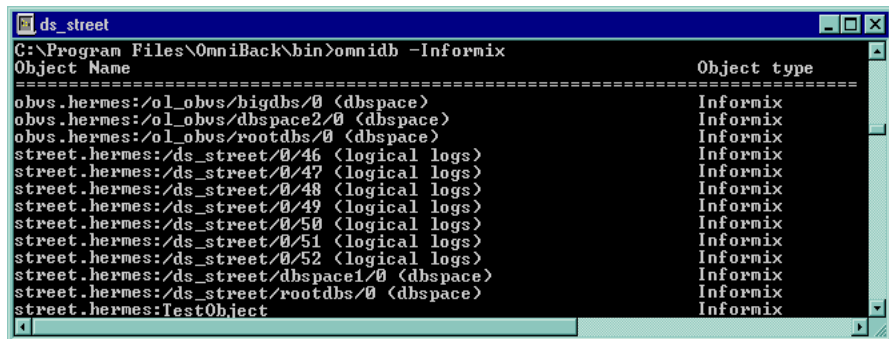
1. `omnidb -informix`
to get a list of Informix objects.

Figure 1-36 List of Informix Objects (UNIX Example)



```
Terminal
Window Edit Options Help
$ omnidb -informix
Object Name                                     Object type
-----
audi.hermes :/IDS914/0/1 (logical logs)         Informix
audi.hermes :/IDS914/0/10 (logical logs)        Informix
audi.hermes :/IDS914/0/11 (logical logs)        Informix
audi.hermes :/IDS914/0/12 (logical logs)        Informix
audi.hermes :/IDS914/0/13 (logical logs)        Informix
audi.hermes :/IDS914/0/14 (logical logs)        Informix
audi.hermes :/IDS914/0/15 (logical logs)        Informix
audi.hermes :/IDS914/0/16 (logical logs)        Informix
audi.hermes :/IDS914/0/17 (logical logs)        Informix
```

Figure 1-37 List of Informix Objects (Windows Example)

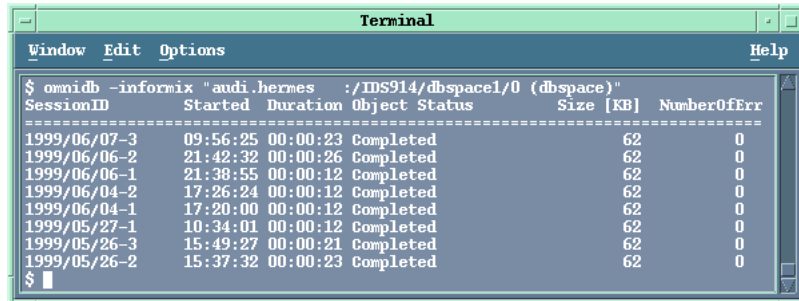


```
ds_street
C:\Program Files\OmniBack\bin>omnidb -Informix
Object Name                                     Object type
-----
obs.hermes:/ol_obs/bigdbs/0 (dbspace)          Informix
obs.hermes:/ol_obs/dbspace2/0 (dbspace)        Informix
obs.hermes:/ol_obs/rootdbs/0 (dbspace)         Informix
street.hermes:/ds_street/0/46 (logical logs)   Informix
street.hermes:/ds_street/0/47 (logical logs)   Informix
street.hermes:/ds_street/0/48 (logical logs)   Informix
street.hermes:/ds_street/0/49 (logical logs)   Informix
street.hermes:/ds_street/0/50 (logical logs)   Informix
street.hermes:/ds_street/0/51 (logical logs)   Informix
street.hermes:/ds_street/0/52 (logical logs)   Informix
street.hermes:/ds_street/dbspace1/0 (dbspace)  Informix
street.hermes:/ds_street/rootdbs/0 (dbspace)   Informix
street.hermes:TestObject                       Informix
```

2. `omnidb -informix "object_name"`

to get details on a specific object, including the Session ID of the backup session. In case of object copies, do not use the copy session ID for the restore, but the object's backup ID, which equals the object's backup session ID. Figure 1-38 shows how you get the objects pertaining to one of the objects specified in Figure 1-36.

Figure 1-38 Details About a Specific Session



```
Terminal
Window Edit Options Help
$ omnidb -informix "audi.hermes :/IDS914/dbospace1/0 (dbospace)"
SessionID      Started      Duration    Object Status      Size [KB]  NumberOfErr
-----
1999/06/07-3   09:56:25    00:00:23    Completed           62         0
1999/06/06-2   21:42:32    00:00:26    Completed           62         0
1999/06/06-1   21:38:55    00:00:12    Completed           62         0
1999/06/04-2   17:26:24    00:00:12    Completed           62         0
1999/06/04-1   17:20:00    00:00:12    Completed           62         0
1999/05/27-1   10:34:01    00:00:12    Completed           62         0
1999/05/26-3   15:49:27    00:00:21    Completed           62         0
1999/05/26-2   15:37:32    00:00:23    Completed           62         0
$
```

3. omnidb -session *SessionID* -media

to display media needed for restore. In the example depicted in Figure 1-39, media used for session 1999/06/07-3 are displayed.

Figure 1-39 Finding Media Needed for Restore



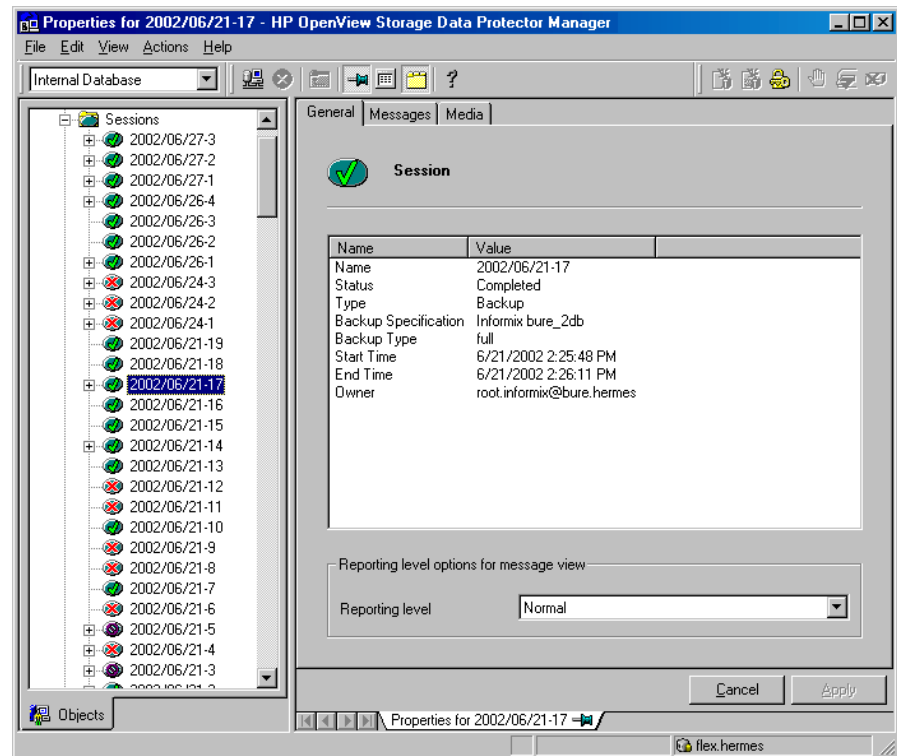
```
Terminal
Window Edit Options Help
$ omnidb -session 1999/06/07-3 -media
Medium Label      Medium ID      Free Blocks
-----
Default File_5    0a110154:375b7af1:5ad6:0001    100688
Default File_6    0a110154:375b7b2a:5ad6:0002    102784
$
```

For detailed information on the omnidb command, refer to the omnidb man page.

Finding Information for Restore Using the Data Protector GUI

You can find information needed for restore in the HP OpenView Storage Data Protector Manager by clicking the Data Protector Internal Database Context and expanding either Sessions or Objects. The sessions are listed by date. Double-click a session to view session details:

Figure 1-40 Checking Session Details



IMPORTANT

The `BAR_RETRY ON-Bar` configuration parameter specifies how many times ON-Bar should retry a backup or restore operation if the first attempt fails. To successfully abort a backup or restore operation at the

first attempt, set the `BAR_RETRY` value to 0. Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more information on this parameter.

Before You Begin Restoring

On UNIX, if you are *not* using the Informix Enterprise Decision Server, shut down OnLine Server before you restore a root dbspace. If you are using the Informix Enterprise Decision Server, bring the Informix server in microkernel mode as follows:

1. Shut down all coservers:

```
xctl onmode -ky
```

2. Bring database server to microkernel mode:

```
xctl -C oninit -m
```

Logged on to OnLine Server as user `informix`, type in the following command:

Windows

```
<INFORMIXDIR>\bin\onmode -ky
```

UNIX

```
<INFORMIXDIR>/bin/onmode -ky
```

where `<INFORMIXDIR>` is the home directory of OnLine Server.

Note that if you intend to restore only non-critical Informix dbspaces (`dbspace1`, `dbspace2`, etc.), then OnLine Server can be online.

The following sections describe how to run a restore. On UNIX, Data Protector starts the `onbar` command under the account of the user running the restore. This should be the Informix user.

Restore Using the Data Protector GUI

To run a restore, follow these steps in the HP OpenView Storage Data Protector Manager:

- Restore Procedure**
1. In the `Context List`, select `Restore`.
 2. In the `Scoping Pane`, expand `Restore` and then `Informix Server`, to get a list of OnLine Servers from which Informix dbobjects can be restored.
 3. Select the OnLine Server from which you want to restore.

Integrating Informix and Data Protector
Restoring an Informix Database

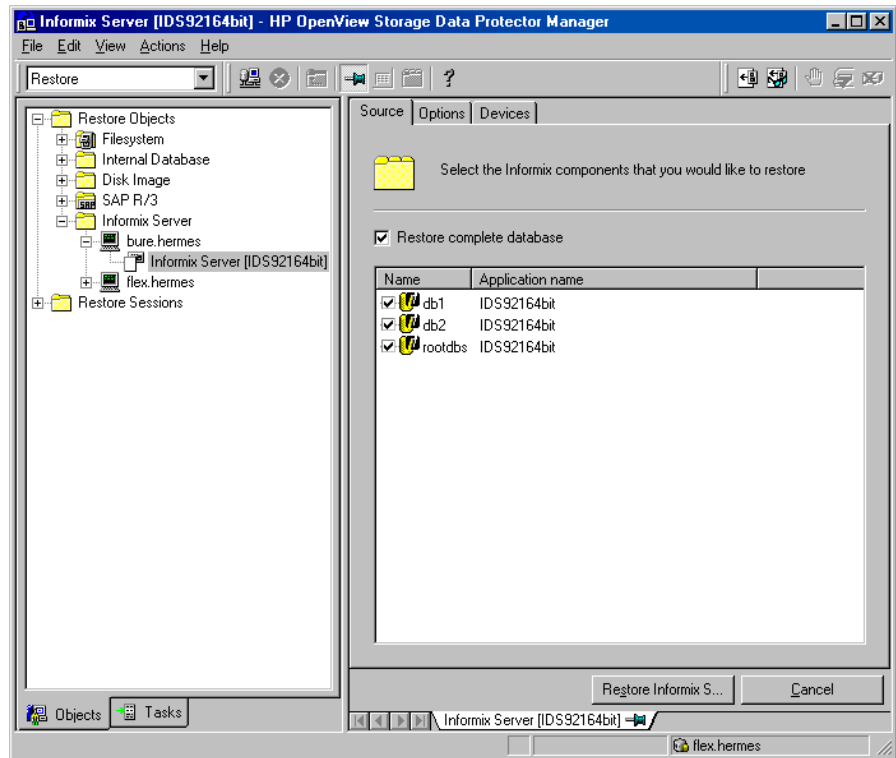
A list of OnLine Servers is displayed in the Results Area. Double-click the server from which you want to restore.

Select the dbjects you want to restore or Restore complete databases to restore all backed up objects.

NOTE

To make an Informix whole-system restore, you must first select the Restore complete databases option.

Figure 1-41 Selecting Objects for Restore



4. Select Options, to specify the options needed for restore. These options are explained in “Restore Options” on page 71.

Restore Options

Backup Specification

Specifies a backup specification to be used to salvage logical log files that are still on the disk before restoring. Note that this is not necessarily the backup specification used for the backing up.

User name, User group (UNIX Systems Only)

User name and group. The `onbar` command is started under the account of the specified user.

Restore to client

Specifies the name of the original backup client. To restore to another client, specify the name of the other client.

Restore by log number (UNIX Systems Only)

Restore all data up to the specific log number. If any logs exist after this one, the `onbar` utility does not restore them. This option invokes the `onbar -r -n <last_log_number>` command. Refer to the *INFORMIX OnLine Dynamic Server: Backup and Restore Guide* for details.

Restore by date

Indicates the date of the backup from which the restore is to be performed. This option invokes the `onbar -r -t <time>` command. Refer to the *INFORMIX OnLine Dynamic Server: Backup and Restore Guide* for details.

NOTE

You can browse your backup dates, regardless of backup type, using the Browse tab. The browse feature works only for backups of the current version of Data Protector. However, you can also enter other restore times, forcing a point in time restore to that particular time.

Restore the latest version

Restores the latest version of a backup.

Whole database restore

Searches the last whole-system backup and restores from that. This option invokes the `onbar -r -w` command. Refer to the *INFORMIX OnLine Dynamic Server: Backup and Restore Guide* for details.

NOTE

This option should only be used after a whole database backup. Data Protector does not automatically detect if you have a whole database backup.

5. Select the `Devices` tab to specify the devices from which you want to restore.
6. If the Informix Full or Whole restore are to be performed and the Informix server to be restored is in online mode, shut down the Informix server by issuing the following command on the Informix server that is to be restored:

```
onmode -ky
```

7. To start your restore session, proceed as follows:

Click the `Start Restore` button

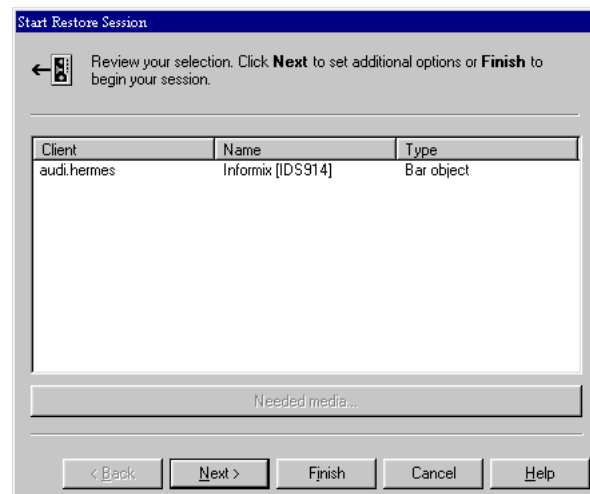
or

In the `Actions` menu, click `Start Restore`.

The `Start Restore Session` dialog box is displayed.

Figure 1-42

Starting the Informix Restore Session



Click **Next**, to select the **Report Level** and the **Network Load** of the restore session and then **Finish** to start the restore session.

8. Observe the session flow messages in the **Data Protector Monitor**.
The “Session successfully completed” message is displayed at the end of a successful session.
9. If the Informix Full or Whole restore was performed, put the Informix server back in online mode by issuing the following command on the Informix server that was restored, when the restore has finished:

```
onmode -m
```

What Happens?

The following happens when you start a restore using the **Data Protector User Interface**:

1. **Data Protector** executes the `ob2onbar.exe` command on the **OnLine Server**. This command starts the `onbar` restore command, with the specified options.
2. The `onbar` command contacts **OnLine Server**, which contacts **Data Protector** via **XBSA** and initiates a backup session to salvage logical logs.
3. During this backup session, **OnLine Server** reads data from the disk and sends it to the `onbar` utility, which sends the data to **Data Protector** for writing to the device.
4. The `onbar` command contacts **OnLine Server**, which contacts **Data Protector** via **XBSA** and initiates a restore session for the data selected for restore.
5. During this restore session, **Data Protector** reads the data from the device and sends the data to the `onbar` utility, which in turn sends the data to **OnLine Server** for writing to disk.
6. **OnLine Server** switches to quiescent mode.

Restore Using Informix Commands

Before You Begin

Before you restore an Informix database instance using the Informix `onbar` command, ensure that you are logged in as `root`, and execute the following commands:

Windows

1. `SET ONCONFIG=<onconfig_file>`

Integrating Informix and Data Protector

Restoring an Informix Database

Where *<onconfig_file>* is the name of OnLine Server ONCONFIG file, for example, ONCONFIG.

2. SET INFORMIXSQLHOSTS=*<sqlhosts_entry>*

Where *<sqlhosts_entry>* is the full pathname of the sqlhosts file, for example, c:\informix\etc\sqlhosts.

3. SET INFORMIXSERVER=*<INFORMIXSERVER>*

Where *<INFORMIXSERVER>* is the name of OnLine Server, for example, ds_street.

4. SET INFORMIXDIR=*<Informix_home_dir>*

Where *<Informix_home_dir>* is the home directory of OnLine Server, for example, d:\informix\.

5. SET OB2APPNAME=*<INFORMIXSERVER>*

Where *<INFORMIXSERVER>* is the name of OnLine Server, for example, ds_street.

6. SET OB2BARLIST=*<backup_specification_name>*

Where *<backup_specification_name>* is the name of the backup specification used for salvaging logical logs and not the one used for the backup.

Note that OB2APPNAME and OB2BARLIST are Data Protector-specific variables.

UNIX

1. export ONCONFIG=*<onconfig_file>*

Where *<onconfig_file>* is the name of OnLine Server ONCONFIG file, for example, ONCONFIG.

2. export INFORMIXSQLHOSTS=*<sqlhosts_entry>*

Where *<sqlhosts_entry>* is the full pathname of the sqlhosts file, for example, /applications/informix73/etc/sqlhosts.

3. export INFORMIXSERVER=*<INFORMIXSERVER>*

Where *<INFORMIXSERVER>* is the name of OnLine Server, for example, ODS730.

4. export INFORMIXDIR=*<Informix_home_dir>*

Where *<Informix_home_dir>* is the home directory of OnLine Server, for example, /applications/informix73/.

5. `export OB2APPNAME=<INFORMIXSERVER>`

Where `<INFORMIXSERVER>` is the name of OnLine Server, for example, ODS730.

6. `export OB2BARLIST=<backup_specification_name>`

Where `<backup_specification_name>` is the name of the backup specification used for salvaging logical logs and not the one used for the backup.

Note that OB2APPNAME and OB2BARLIST are Data Protector-specific variables.

Examples

The following are some examples of using the `onbar` command syntax for running restore.

Restoring Dbspaces and Logical Logs (Informix Full Restore)

If the Informix server to be restored is in online mode, shut down the Informix server by issuing the following command on the Informix server that is to be restored:

```
onmode -ky
```

To restore dbspaces and blobspaces as well as appropriate logical logs, use the `-r` option:

```
onbar -r
```

When the restore has finished, put the Informix server back in online mode by issuing the following command on the Informix server that was restored:

```
onmode -m
```

Restoring Dbspaces and Logical Logs (Informix Whole Restore)

If the Informix server to be restored is in online mode, shut down the Informix server by issuing the following command on the Informix server that is to be restored:

```
onmode -ky
```

To restore dbspaces and blobspaces as well as appropriate logical logs, use the `-r -w` options:

```
onbar -r -w
```

When the restore has finished, put the Informix server back in online mode by issuing the following command on the Informix server that was restored:

```
onmode -m
```

Restoring Dbspaces and Blobspaces Only

To restore dbspaces and blobspaces and not the logical log, use the `-r` and `-p` options:

```
onbar -r -p
```

Restoring a Particular Dbspace or Blobspace

To restore a specific dbspace, for example `dbspace_1`, use the following syntax:

```
onbar -r dbspace_1
```

Salvaging Logical Log files

If there has been a disk failure, salvage the logical log files that are still on the disk with the following command before restoring your data from a backup:

```
onbar -l -s
```

Refer to the *Informix-OnLine Dynamic Server: Backup and Restore Guide* for more details on the `onbar` command.

Messages from the Data Protector backup session and messages generated by the Informix Integration Module are logged in the IDB. See “Monitoring an Informix Backup and Restore” on page 79 for additional information on monitoring restore sessions.

To Another OnLine Server

To restore to an OnLine Server other than the one from which the backup was made, proceed as follows:

Restoring to Another OnLine Server

1. Install and configure the Informix Integration Module to the other client.
2. Create an Informix user on the client to which you intend to restore.

3. Create an Informix database with the same Informix instance name and number as the original database by using the Informix `onmonitor` utility. Before going to the next step, ensure that OnLine Server is running.
4. Configure the Informix integration with the same OnLine Server name on the target client as was on the original client. See “Configuring an OnLine Server” on page 19 for instructions.
5. Shut down the Informix database.
6. Copy the main Informix configuration files (`ONCONFIG`, emergency boot file, `oncfg_<INFORMIXSERVER>.<SERVERNUM>`, and on UNIX, `sqlhosts`) to the other client.
7. Modify the main client name in the Informix configuration files. This is necessary because the client name is changed when you restore to the other client.
8. Start a whole-system restore of the Informix objects from the Data Protector User Interface.

Using Another Device

Data Protector supports restore using a device other than the one that was used at backup time.

Restoring Using the Data Protector GUI

If you are performing a restore using the Data Protector GUI, refer to the “Restoring Under Another Device” section of the *HP OpenView Storage Data Protector Administrator’s Guide* for more information on how perform a restore using another device.

Restoring Using the Data Protector CLI or Informix Commands

If you are performing a restore using the Data Protector CLI or Informix commands, specify the new device in the

`<Data_Protector_home>\Config\server\Cell\restoredev` (Windows systems), or in the `/etc/opt/omni/server/cell/restoredev` (UNIX systems) file in the following format:”

```
"DEV 1" "DEV 2"
```

where

DEV 1 is the original device and DEV 2 the new device.

Note that this file should be deleted after it is used.

Windows

On Windows, this file has to be in the UNICODE format.

Example

Suppose you have Informix objects backed up on a device called DAT1. To restore them from a device named DAT2, specify the following in the `restoredev` file:

```
"DAT1" "DAT2"
```

Disaster Recovery

Disaster recovery is a very complex process that involves products from several vendors. As such, successful disaster recovery depends on all the vendors involved. The information provided here is to be used as a guideline.

Check the instructions of the database/application vendor on how to prepare for disaster recovery. Also refer to the Disaster Recovery chapter in the *HP OpenView Storage Data Protector Administrator's Guide* for instructions on how to approach system disaster recovery using Data Protector.

This is a general procedure on how to recover an application:

1. Recover the operating system.
2. Install, configure, and initialize the database/application so that data on Data Protector media can be loaded back to the system. Consult database/application vendor documentation for a detailed procedure and steps needed to prepare the database.
3. Ensure that the database/application server has the required Data Protector client software installed and is configured for the database/application. Follow the procedures in this chapter and the procedures in the troubleshooting section.
4. Start the restore. When the restore is complete, follow the instructions of the database/application vendor for any additional steps required to bring the database back online.

Monitoring an Informix Backup and Restore

Data Protector enables you to monitor currently running and view previous backup and restore sessions. When you run an interactive backup or restore session, a monitor window displays showing you the progress of the session. You can monitor the session from any Data Protector client in the network that has the User Interface component installed. Note that the session continues even with the User Interface closed.

Monitoring Current Sessions

To monitor a currently running session using the Data Protector GUI, proceed as follows:

1. In the Context List, click `Monitor`.
In the Results Area, all currently running sessions are listed.
2. Double-click the session you want to monitor.

Clearing Sessions To remove all completed or aborted sessions from the Results Area of the Monitor context, proceed as follows:

1. In the Scoping Pane, click `Current Sessions`.
2. In the Actions menu, select `Clear Sessions`. Or click the `Clear Sessions` icon on the toolbar.

To remove a particular completed or aborted session from the current sessions list, right-click the session and select `Remove From List`.

NOTE

All completed or aborted sessions are automatically removed from the Results Area of the Monitor context if you restart the Data Protector GUI.

For detailed information on a completed or aborted session, see “Viewing Previous Sessions”.

All actions and messages are logged to both Data Protector and Informix log files. Mount requests are displayed in the Data Protector monitor.

When the onbar utility encounters an error or a condition that warrants a warning, it writes a message to the Informix ON-Bar message file. The full pathname of this file is specified in the `BAR_ACT_LOG` configuration parameter. For more information on this file, refer to the *INFORMIX-OnLine Dynamic Server: Backup and Restore Guide*.

Viewing Previous Sessions

To view a previous session using the Data Protector GUI, proceed as follows:

1. In the Context List, click `Internal Database`.
2. In the Scoping Pane, expand `Sessions` to display all the sessions stored in the IDB.

The sessions are sorted by date. Each session is identified by a session ID consisting of a date in the `YY/MM/DD` format and a unique number.

3. Right-click the session and select `Properties` to view details on the session.
4. Click the `General`, `Messages` or `Media` tab to display general information on the session, session messages, or information on the media used for this session, respectively.

Troubleshooting

This section describes procedures you should follow to troubleshoot your configuration, back up, or restore problems.

Before You Begin

1. Ensure that the latest official Data Protector patches are installed. Refer to “Verifying Which Data Protector Patches Are Installed” in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* or

http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, and other information.

2. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a description of general Data Protector limitations as well as known problems and workarounds.

Troubleshooting on Windows Systems

Cluster Related Troubleshooting

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before performing some procedures run from the command line (on the client). When the GUI is used, this is not required. The `OB2BARHOSTNAME` variable is set as follows:

```
set OB2BARHOSTNAME=<virtual_hostname>
```

Configuration Problems

If you have problems configuring the Data Protector Informix integration, proceed as follows:

1. Make a test backup of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

2. Ensure that OnLine Server is up and running:

If OnLine Server is up and running, the -- On-Line -- message is displayed.

If not, then start OnLine Server using the following command:

```
<INFORMIXDIR>\bin\oninit
```

where <INFORMIXDIR> is the home directory of OnLine Server.

3. If you have any non-default Informix settings, then ensure that they are registered in the Data Protector Informix configuration file. For more information on Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
4. Examine system errors reported in
<Data_Protector_home>\log\debug.log on the Online Server.

Backup Problems

If you have problems backing up Informix dobjects, proceed as follows:

1. Make a test backup of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

2. Ensure that OnLine Server is up and running:

If OnLine Server is up and running, the -- On-Line -- message is displayed.

If not, then start OnLine Server using the following command:

```
<INFORMIXDIR>\bin\oninit
```

where <INFORMIXDIR> is the home directory of OnLine Server.

3. Verify the configuration of your OnLine Server using the following command:

where <INFORMIXSERVER> is the name of OnLine Server.

```
util_informix.exe -CHECKCONF <INFORMIXSERVER>,
```

In case of an error, the error number is displayed in the form
RETVAL<error_number>.

4. Test the Data Protector Informix configuration as per instructions in “Testing the Integration” on page 47.

Example

Run the following command to test the configuration of the backup specification called `InformixWhole`:

```
<Data_Protector_home>\bin\omnib -informix_list  
InformixWhole -test_bar
```

- If the Informix part of the test fails, then proceed as follows:

Make a test run using the `onbar -F -b` option. If the test fails, then this is probably not a Data Protector problem. Refer to the Informix manuals for further instructions.

- If the Data Protector part of the test fails then create an Informix backup specification to back up to a null or file device. If the backup succeeds, then the problem is probably related to devices.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions on troubleshooting devices.

- If the test succeeds, start a backup directly from an OnLine Server. See “Using Informix Commands” on page 59 for instructions.

If this backup succeeds, then the problem may be that the client on which the Data Protector User Interface runs does not have enough memory, disk space, or other operating system resources.

5. If you have any non-default Informix settings, then ensure that they are registered in the Data Protector Informix configuration file. For more information on Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
6. Start the backup directly from Online Server. See “Using Informix Commands” on page 59.

Troubleshooting the Informix Side This section is not meant to teach you about OnLine Server. Following the given procedure might help you solve some Informix-related problems:

1. Check the following Informix files for error descriptions:

```
bar_act.log
```

```
bar_dbg.log
```

```
online.log
```

The locations of these files are specified in the Informix `ONCONFIG` file.

2. Start a backup, not using Data Protector:

Set the `BAR_BSALIB_PATH` shell variable to
`<ISMDIR>\bin\libbsa.dll`, where `<ISMDIR>` is the path to the ISM.

Use the `onbar` command to start the backup.

Troubleshooting Logical Log Backups

Description

After the continuous backup of logical logs is done, the Backup Session Manager waits for a specified time-out for the next logical log to be backed up. If there is no new connection in the specified time-out, the Backup Session Manager completes the session and goes down. If Informix sends a request for the backup of the next logical log, Data Protector first checks if the Backup Session Manager and other processes are up and running. If the Backup Session Manager is up, then a request is sent to the Backup Session Manager to create a new backup object.

And if between these last two events the Backup Session Manager goes down because it didn't receive a new request, you receive a system error and a new session is not started.

Resolution

Organize the backup of logical logs with more than two backup specifications.

Detailed Description

The backup of logical logs is started when a logical log is full. At that time, Informix starts a script specified by `ALARMPROGRAM` configuration parameter in the `ONCONFIG` file. This script then starts the backup using the specified backup specification.

When the next logical log is full, then it restarts the `ALARMPROGRAM` script. This script will now start the backup using a different backup specification than the previous one and this way the new session will be started and the problem cannot appear.

Use at least 3 backup specifications, because during the backup of one logical log it can happen that Informix calls the `ALARMPROGRAM` script more than once.

About the Backup Specifications

Backup specifications must be the same. You can use the same device in all the backup specifications.

IMPORTANT

The backup specification names must be different.

The following is an example of an alarm script for 4 backup specifications named BARLIST1, BARLIST2, BARLIST3, and BARLIST4. The script automates logical log backups using event alarms from the database server. To install this script, add the following line to the ONCONFIG file:

```
ALARMPROGRAM <INFORMIXDIR>\etc\log_full.sh, where  
<INFORMIXDIR> is OnLine Server home directory.
```

NOTE

The Informix Enterprise Decision Server does not use the ALARMPROGRAM script for continuous logical log backup. Onbar_d starts the backup automatically (if the LOG_BACKUP_MODE parameter in the ONCONFIG file is set to CONT) and passes a request to workers which perform the backup.

Figure 1-43 Example of an Alarm Script

```
PROG=`basename $0`
Barlist=`cat /etc/opt/omni/informix/IDS914/barlist`
export OB2BARLIST=$Barlist
export OB2APPNAME=IDS914
USER_LIST=informix
BACKUP_CMD="/opt/omni/bin/omnib -informix_list $Barlist"
EXIT_STATUS=0

EVENT_SEVERITY=$1
EVENT_CLASS=$2
EVENT_MSG="$3"
EVENT_ADD_TEXT="$4"
EVENT_FILE="$5"

case "$EVENT_CLASS" in
    23)
        # onbar assumes no operator is present,
        # so all messages are written to the activity
        # log and there shouldn't be any output, but
        # send everything to /dev/null just in case
        $BACKUP_CMD 2>&1 >> /dev/null
        EXIT_STATUS=?
        ;;

# One program is shared by all event alarms.  If this ever gets expan
# handle more than just archive events, uncomment the following:
*)
    #
    EXIT_STATUS=1
    ;;
esac

case "$Barlist" in
    "BARLIST1")
        echo BARLIST2 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST2")
        echo BARLIST3 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST3")
        echo BARLIST4 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST4")
        echo BARLIST1 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    *)
        echo BARLIST2 > /etc/opt/omni/informix/IDS914/barlist
        ;;
esac

exit $EXIT_STATUS
```

Restore Problems

If you have problems restoring Informix dbobjects, proceed as follows:

1. Examine system errors reported in the
`<Data_Protector_home>\log\debug.log` file on the Online Server.
2. Make a Data Protector test backup and restore of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

3. Ensure that the backup specification used for salvaging logical logs is properly configured. Note that this is *not* the same backup specification used to back up your data.
4. Test Data Protector data transfer using the testbar utility. Log in as the Informix user on the Online Server and proceed as follows:

```
<Data_Protector_home>\bin\testbar
-type: Informix
-appname: <INFORMIXSERVER>
-bar: <backup_specification_name>
-perform: restore
-object: <OBJECT_NAME>
-version: <OBJECT_VERSION>
```

where `<INFORMIXSERVER>` is the name of OnLine Server,
`<OBJECT_NAME>` is the name of an object backed up,
`<OBJECT_VERSION>` is an object version, and
`<backup_specification_name>` the name of the Data Protector backup specification.

If the test is not successful, proceed as follows:

- a. Troubleshoot errors reported by the testbar utility using the Data Protector troubleshooting file,
`<Data_Protector_home>\docs\Trouble.txt`.
- b. Examine system errors reported in the
`<Data_Protector_home>\log\debug.log` file on the Online Server.

Restoring to Another Client If you backed up your data to one client and exported the media and then imported them to another client in a different cell, the Data Protector session IDs of backup sessions may be changed in the IDB. However, the session IDs are not automatically changed in the Informix emergency boot file (`ixbar.<server_id>`, where `<server_id>` is the value of the SERVERNUM configuration parameter).

Therefore, the restore of such objects may fail.

Action

Edit the emergency boot file to reflect the changed Data Protector session IDs. List the changed session IDs during the import procedure.

Information about backed up objects is stored in the emergency boot file in the format shown in Table 1-7.

Table 1-6

Emergency Boot File Format

```
ODS730   rootdbs   R  1  7  0  9  1999008018   1999-08-18   18:10:25   1
```

Information that makes up the Data Protector session ID is in columns 7 and 9. Column 9 represents the date and column 7 the unique session number.

For example, the session ID denoted in Table 1-7 is 1999/08/18-9. Note that the delimiter in the date field is “-” in the emergency boot file and “/” in the Data Protector session ID.

Also note that the value of the SERVERNUM configuration parameter is given in column 4.

Troubleshooting the Informix Side Following the given procedure might help you solve some Informix-related problems:

1. Check the following Informix files for error descriptions:

```
bar_act.log  
bar_dbg.log  
online.log
```

The locations of these files are specified in the Informix ONCONFIG file.

2. Verify that the dbspaces you want to restore are offline in order to run a cold restore:
 - a. Log on to your OnLine Server.
 - b. Type in the following command:

```
<INFORMIXDIR>\bin\onstat -d
```

where *<INFORMIXDIR>* is the home directory of OnLine Server.
3. Ensure that Informix configuration files (ONCONFIG, emergency boot file, oncfg_<INFORMIXSERVER>.<SERVERNUM>) are not corrupted. If they are corrupted, restore them manually.

Troubleshooting on UNIX Systems

Cluster Related Troubleshooting

In a cluster environment, the environment variable `OB2BARHOSTNAME` must be defined as the virtual hostname before performing some procedures run from the command line (on the client). When the GUI is used, this is not required. The `OB2BARHOSTNAME` variable is set as follows:

```
export OB2BARHOSTNAME=<virtual_hostname>
```

Configuration Problems

If you have problems configuring the Data Protector Informix integration, proceed as follows:

1. Make a test backup of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.
2. Ensure that OnLine Server is up and running:
 - a. Log on to OnLine Server as user `informix`
 - b. Type in the following command:

```
<INFORMIXDIR>/bin/onstat -d
```

where *<INFORMIXDIR>* is the home directory of OnLine Server.

If OnLine Server is up and running, the `-- On-Line --` message is displayed.

If not, then start OnLine Server using the following command:

```
<INFORMIXDIR>/bin/oninit
```

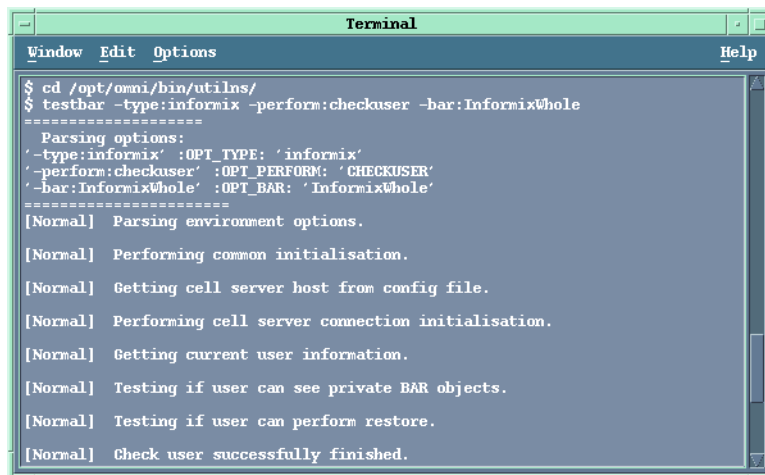
where <INFORMIXDIR> is the home directory of OnLine Server.

3. If you have any non-default Informix settings, then ensure that they are registered in the Data Protector Informix configuration file. For more information on the Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
4. Examine system errors reported in /usr/omni/log/debug.log on the OnLine Server.
5. Test if the Informix user has the appropriate privileges in Data Protector. Log in as the Informix user, for example, as user *informix*, change to the /opt/omni/bin/utilns/ (HP-UX and Solaris systems) or /usr/omni/bin/utilns/(other UNIX systems) directory and run the following command on the OnLine Server:

```
testbar -type:informix -perform:checkuser  
-bar:InformixWhole
```

Figure 1-44

Checking the Informix User



```
Terminal  
Window Edit Options Help  
$ cd /opt/omni/bin/utilns/  
$ testbar -type:informix -perform:checkuser -bar:InformixWhole  
-----  
Parsing options:  
'-type:informix' :OPT_TYPE: 'informix'  
'-perform:checkuser' :OPT_PERFORM: 'CHECKUSER'  
'-bar:InformixWhole' :OPT_BAR: 'InformixWhole'  
-----  
[Normal] Parsing environment options.  
[Normal] Performing common initialisation.  
[Normal] Getting cell server host from config file.  
[Normal] Performing cell server connection initialisation.  
[Normal] Getting current user information.  
[Normal] Testing if user can see private BAR objects.  
[Normal] Testing if user can perform restore.  
[Normal] Check user successfully finished.
```

In the preceding example, the user has all the appropriate rights for the backup specification called *InformixWhole*.

If a user ana on OnLine Server nyasha.zim.com is not in the operator or admin group, you get an error message like the following:

```
[Critical] From: OB2BAR@nyasha.zim.com " " Time: 08/06/99  
17:35:37
```

```
[131:53] User "ana.users@nyasha.zim.com" is not allowed to  
perform a restore.
```

See “Configuring an Informix User in Data Protector” on page 16 for information about the right privileges.

Backup Problems

If you have problems backing up Informix dobjects, proceed as follows:

1. Make a test backup of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.

2. Ensure that OnLine Server is up and running:

- a. Log on to OnLine Server as user informix

- b. Type in the following command:

```
<INFORMIXDIR>/bin/onstat -d
```

where <INFORMIXDIR> is the home directory of OnLine Server.

If OnLine Server is up and running, the -- On-Line -- message is displayed.

If not, then start OnLine Server using the following command:

```
<INFORMIXDIR>/bin/oninit
```

where <INFORMIXDIR> is the home directory of OnLine Server.

3. Verify the configuration of your OnLine Server using the following command:

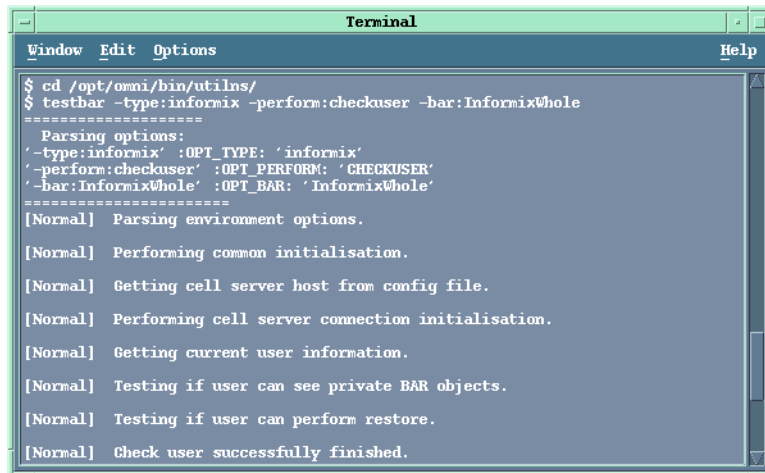
where <INFORMIXSERVER> is the name of OnLine Server.

```
util informix.exe -CHECKCONF <INFORMIXSERVER>
```

In case of an error, the error number is displayed in the form *RETVAL*<error_number>.

- To get the error description, start the command,
`/opt/omni/lbin/omnigetmsg 12 <error_number>` (HP-UX and Solaris systems) or `/usr/omni/bin/omnigetmsg 12 <error_number>` (other UNIX systems).
4. Test if the Informix user has the right privileges in Data Protector. Log in as the Informix user, for example, as user `informix`, and run the following command on the OnLine Server:
`/opt/omni/bin/utilns/testbar -type:informix -perform:checkuser -bar:InformixWhole` (HP-UX and Solaris systems)
`/usr/omni/bin/utilns/testbar -type:informix -perform:checkuser -bar:InformixWhole` (other UNIX systems)

Figure 1-45 Checking the Informix User



```
Terminal
Window Edit Options Help
$ cd /opt/omni/bin/utilns/
$ testbar -type:informix -perform:checkuser -bar:InformixWhole
=====
Parsing options:
'-type:informix' :OPT_TYPE: 'informix'
'-perform:checkuser' :OPT_PERFORM: 'CHECKUSER'
'-bar:InformixWhole' :OPT_BAR: 'InformixWhole'
=====
[Normal] Parsing environment options.

[Normal] Performing common initialisation.

[Normal] Getting cell server host from config file.

[Normal] Performing cell server connection initialisation.

[Normal] Getting current user information.

[Normal] Testing if user can see private BAR objects.

[Normal] Testing if user can perform restore.

[Normal] Check user successfully finished.
```

In the preceding example, the user has all the appropriate rights for the backup specification named `InformixWhole`.

If a user `andrea` on OnLine Server `cool.shon.com`, does not have the appropriate rights, you get an error message like the following:

```
[Critical] From: OB2BAR@cool.shon.com "" Time: 08/06/99 17:51:41
[131:53] User "andrea.users@cool.shon.com" is not allowed to
perform a restore.
```


See “Configuring an Informix User in Data Protector” on page 16 for information about the right privileges.

5. Verify that the `onbar` (or `onbar_d` for Informix 7.3x or later) command has the switch ownership (s) bit set and that it is owned by the Informix user, for example, `root : informix`.
6. Test the Data Protector Informix configuration as per instructions in “Testing the Integration” on page 47.

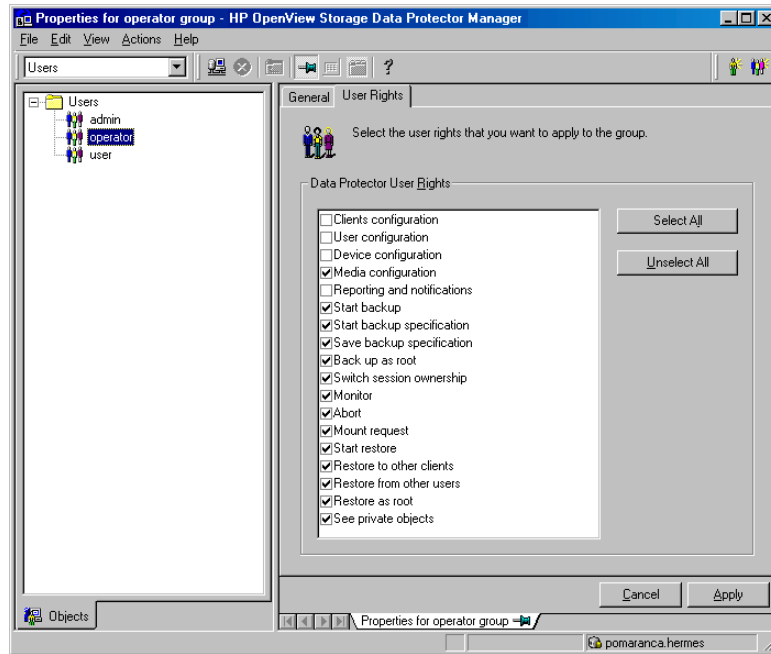
Example

Run the following command to test the configuration of the backup specification called `InformixWhole`:

```
opt/omni/bin/omnib -informix_list InformixWhole -test_bar
```

- If the Informix part of the test fails, make a test run using the `onbar -F -b` option. If the test fails, then this is probably not a Data Protector problem. Refer to the Informix manuals for further instructions.
- If the Data Protector part of the test fails, create an Informix backup specification to back up to a null or file device. If the backup succeeds, proceed as follows:
 - a. Verify that the owner of the backup specification is the Informix user, and that they are in the Data Protector operator or admin group.
 - b. Ensure that the `See private objects` user right of the Data Protector operator group, which allows users to browse private objects, is selected:
 1. In the Context List, select `Users`.
 2. In the Results Area, right-click operator and click `Properties`.

Figure 1-46 Selecting the See Private Objects User Right



3. If the See private objects user right is selected, click Apply.

- c. Create an Informix backup specification to back up to a null or file device. If the backup succeeds, the problem is probably related to devices.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions on troubleshooting devices.

- If the test succeeds, start a backup directly from an OnLine Server. See "Using Informix Commands" on page 59 for instructions.

If this backup succeeds, then the problem may be that the client on which the Data Protector User Interface runs does not have enough memory, disk space, or other operating system resources.

7. Test Data Protector data transfer using the testbar utility. Log in as the Informix user on the OnLine Server, change to the `/opt/omni/bin/utilns/` (HP-UX and Solaris systems) or `/usr/omni/bin/utilns/` (other UNIX systems) and proceed as follows:

```
testbar
-type:Informix
-appname:<INFORMIXSERVER>
-bar:<backup_specification_name>
-perform:backup
```

where `<INFORMIXSERVER>` is the name of OnLine Server and `<backup_specification_name>` the name of the Data Protector backup specification.

If the test is successful, then proceed to the next step, otherwise proceed as follows:

- a. Troubleshoot errors reported by the testbar utility using the Data Protector troubleshooting file, `/opt/omni/gui/help/Trouble.txt`.
 - b. Examine system errors reported in the `/var/opt/omni/log/debug.log` (HP-UX and Solaris systems) or `/usr/omni/log/debug.log` (other UNIX systems) file on the OnLine Server.
8. If you have any non-default Informix settings, then ensure that they are registered in the Data Protector Informix configuration file. For more information on Data Protector Informix configuration file, see “Data Protector Informix Configuration File” on page 9.
 9. Start the backup directly from the OnLine Server. See “Using Informix Commands” on page 59.

Troubleshooting the Informix Side This section is not meant to teach you about OnLine Server. Following the given procedure might help you solve some Informix-related problems:

1. Check the following Informix files for error descriptions:

```
bar_act.log
bar_dbg.log
online.log
```

The locations of these files are specified in the Informix ONCONFIG file.

2. Start a backup, not using Data Protector:

Set the `BAR_BSALIB_PATH` shell variable to
`<INFORMIXDIR>/lib/ibsad001.sl`

Use the `onbar` command to start the backup.

Troubleshooting Logical Log Backups Backup of Informix logical logs fails.

Description

After the continuous backup of logical logs is done, the Backup Session Manager waits for a specified time-out for the next logical log to be backed up. If there is no new connection in the specified time-out, the Backup Session Manager completes the session and goes down. If Informix sends a request for the backup of the next logical log, Data Protector first checks if the Backup Session Manager and other processes are up and running. If the Backup Session Manager is up, then a request is sent to the Backup Session Manager to create a new backup object.

And if between these last two events the Backup Session Manager goes down because it didn't receive a new request, you receive a system error and a new session is not started.

Resolution

Organize the backup of logical logs with more than two backup specifications.

Detailed Description

The backup of logical logs is started when a logical log is full. At that time, Informix starts a script specified by `ALARMPROGRAM` configuration parameter in the ONCONFIG file. This script then starts the backup using the specified backup specification.

When the next logical log is full, then it restarts the `ALARMPROGRAM` script. This script will now start the backup using a different backup specification than the previous one and this way the new session will be started and the problem cannot appear.

Use at least 3 backup specifications, because during the backup of one logical log it can happen that Informix calls the `ALARMPROGRAM` script more than once.

About the Backup Specifications

Backup specifications must be the same. You can use the same device in all the backup specifications.

IMPORTANT

The backup specification names must be different.

The following is an example of an alarm script for 4 backup specifications named BARLIST1, BARLIST2, BARLIST3, and BARLIST4. The script automates logical log backups using event alarms from the database server. To install this script, add the following line to the ONCONFIG file:

```
ALARMPROGRAM <INFORMIXDIR>/etc/log_full.sh, where  
<INFORMIXDIR> is OnLine Server home directory.
```

NOTE

The Informix Enterprise Decision Server does not use the ALARMPROGRAM script for continuous logical log backup. Onbar_d starts the backup automatically (if the LOG_BACKUP_MODE parameter in the ONCONFIG file is set to CONT) and passes a request to workers which perform the backup.

Figure 1-47 Example of an Alarm Script

```
PROG=`basename $0`
Barlist=`cat /etc/opt/omni/informix/IDS914/barlist`
export OB2BARLIST=$Barlist
export OB2APPNAME=IDS914
USER_LIST=informix
BACKUP_CMD="/opt/omni/bin/omnib -informix_list $Barlist"
EXIT_STATUS=0

EVENT_SEVERITY=$1
EVENT_CLASS=$2
EVENT_MSG="$3"
EVENT_ADD_TEXT="$4"
EVENT_FILE="$5"

case "$EVENT_CLASS" in
    23)
        # onbar assumes no operator is present,
        # so all messages are written to the activity
        # log and there shouldn't be any output, but
        # send everything to /dev/null just in case
        $BACKUP_CMD 2>&1 >> /dev/null
        EXIT_STATUS=$?
        ;;

# One program is shared by all event alarms.  If this ever gets expan
# handle more than just archive events, uncomment the following:
*)
    #
    EXIT_STATUS=1
    ;;
esac

case "$Barlist" in
    "BARLIST1")
        echo BARLIST2 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST2")
        echo BARLIST3 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST3")
        echo BARLIST4 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    "BARLIST4")
        echo BARLIST1 > /etc/opt/omni/informix/IDS914/barlist
        ;;
    *)
        echo BARLIST2 > /etc/opt/omni/informix/IDS914/barlist
        ;;
esac

exit $EXIT_STATUS
```

Restore Problems

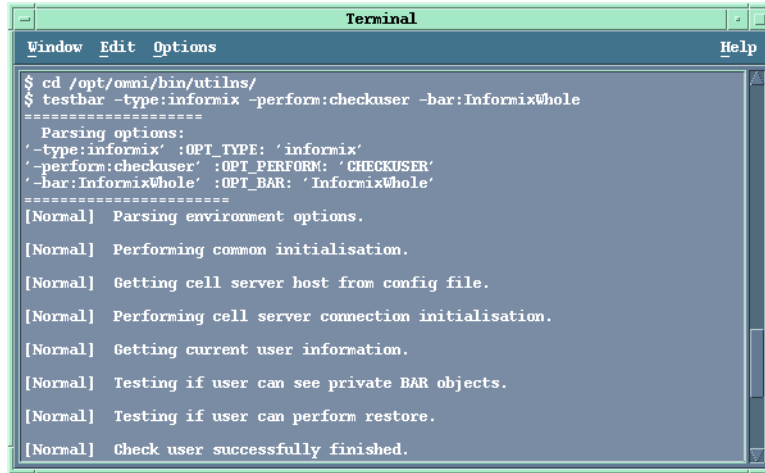
If you have problems restoring Informix dbobjects, proceed as follows:

1. Examine system errors reported in the `/var/opt/omni/log/debug.log` (HP-UX and Solaris systems) or `/usr/omni/log/debug.log` (other UNIX systems) file on the OnLine Server.
2. Make a Data Protector test backup and restore of any filesystem on the problematic client.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions.
3. Verify that the user specified for the restore session is the Informix user, and that they are in the Data Protector operator or admin group.
4. Ensure that the `See private objects` user right of the Data Protector operator group is selected.
5. Verify that the `onbar` (or `onbar_d` for Informix 7.3x or later) command has the switch ownership (`s`) bit set and that it is owned by the Informix user, for example, `root:informix`.
6. Test if the Informix user has the right privileges in Data Protector. Log in as the Informix user, for example, as user `informix`, and run the following command in the `/opt/omni/bin/utilns/` (HP-UX and Solaris systems) or in the `/usr/omni/bin/utilns/` (other UNIX systems) directory on the OnLine Server:

```
testbar -type:informix -perform:checkuser  
-bar:InformixWhole
```

Figure 1-48 **Checking the Informix User**



```
Terminal
Window Edit Options Help
$ cd /opt/omni/bin/utlins/
$ testbar -type:informix -perform:checkuser -bar:InformixWhole
=====
Parsing options:
'-type:informix' :OPT_TYPE: 'informix'
'-perform:checkuser' :OPT_PERFORM: 'CHECKUSER'
'-bar:InformixWhole' :OPT_BAR: 'InformixWhole'
=====
[Normal] Parsing environment options.
[Normal] Performing common initialisation.
[Normal] Getting cell server host from config file.
[Normal] Performing cell server connection initialisation.
[Normal] Getting current user information.
[Normal] Testing if user can see private BAR objects.
[Normal] Testing if user can perform restore.
[Normal] Check user successfully finished.
```

In the preceding example, the user has all the appropriate rights for the backup specification named InformixWhole.

If a user andrea on OnLine Server cool.shon.com, does not have the appropriate rights, you get an error message like the following:

```
[Critical] From: OB2BAR@cool.shon.com "" Time: 08/06/99 17:51:41
[131:53] User "andrea.users@cool.shon.com" is not allowed to
perform a restore.
```

See “Configuring an Informix User in Data Protector” on page 16 for information about the right privileges.

7. Ensure that the backup specification used for salvaging logical logs is properly configured. Note that this is *not* the same backup specification used to back up your data.

8. Test Data Protector data transfer using the testbar utility. Log in as the Informix user on the OnLine Server, change to the /opt/omni/bin/utilns/ (HP-UX and Solaris systems) or /usr/omni/bin/utilns/ (other UNIX systems) directory and proceed as follows:

```
testbar
-type:Informix
-appname:<INFORMIXSERVER>
-bar:<backup_specification_name>
-perform:restore
```

where <INFORMIXSERVER> is the name of OnLine Server and <backup_specification_name> the name of the Data Protector backup specification.

If the test is not successful, proceed as follows:

- a. Troubleshoot errors reported by the testbar utility using the Data Protector troubleshooting file, /opt/omni/gui/help/Trouble.txt.
- b. Examine system errors reported in the /var/opt/omni/log/debug.log (HP-UX and Solaris systems) or /usr/omni/log/debug.log (other UNIX systems) file on the OnLine Server.

Restoring to Another Client If you backed up your data to one client and exported the media and then imported them to another client in a different cell, the Data Protector session IDs of backup sessions may be changed in the IDB. However, the session IDs are not automatically changed in the Informix emergency boot file (ixbar.<server_id>, where <server_id> is the value of the SERVERNUM configuration parameter).

Therefore, the restore of such objects may fail.

Action

Edit the emergency boot file to reflect the changed Data Protector session IDs. List the changed session IDs during the import procedure.

Information about backed up objects is stored in the emergency boot file in the format shown in Table 1-7.

Table 1-7

Emergency Boot File Format

ODS730	rootdbs	R	1	7	0	9	1999008018	1999-08-18	18:10:25	1
--------	---------	---	---	---	---	---	------------	------------	----------	---

Information that makes up the Data Protector session ID is in columns 7 and 9. Column 9 represents the date and column 7 the unique session number.

For example, the session ID denoted in Table 1-7 is 1999/08/18-9. Note that the delimiter in the date field is “-” in the emergency boot file and “/” in the Data Protector session ID.

Also note that the value of the SERVERNUM configuration parameter is given in column 4.

Troubleshooting the Informix Side Following the given procedure might help you solve some Informix-related problems:

1. Check the following Informix files for error descriptions:

```
bar_act.log  
bar_dbg.log  
online.log
```

The locations of these files are specified in the Informix ONCONFIG file.

2. Verify that the dbspaces you want to restore are offline in order to run a cold restore:
 - a. Log on to your OnLine Server as UNIX user `informix`
 - b. Type in the following command:

```
<INFORMIXDIR>/bin/onstat -d
```

where `<INFORMIXDIR>` is the home directory of OnLine Server.

3. Ensure that Informix configuration files (ONCONFIG, `sqlhosts`, emergency boot file, `oncfg_<INFORMIXSERVER>.<SERVERNUM>`) are not corrupted. If they are corrupted, restore them manually.

In This Chapter

This chapter explains how to configure and use the Data Protector IBM DB2 UDB integration.

The chapter is organized into the following sections:

“Overview” on page 105

“Prerequisites and Limitations” on page 107

“Integration Concept” on page 109

“Configuring the Integration” on page 115

“Backing Up a DB2 Database” on page 128

“Restoring a DB2 Database” on page 134

“Monitoring a DB2 Backup and Restore” on page 146

“Troubleshooting” on page 149

Overview

The Data Protector integration with IBM DB2 Universal Database (UDB) Server (hereafter referred to as DB2 Server) allows you to perform online and offline backups of the DB2 database objects.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* for information about platforms and devices supported by the Data Protector DB2 integration.

Backup Types

You can perform the following types of backup using the Data Protector DB2 integration:

- Backup of one or several databases
- Backup of one or several table spaces
- Backup of several table spaces from different databases
- Incremental database/table space backup
- Delta database/table space backup

Each backup type may be performed both online and offline.

Restore Types

The Data Protector DB2 integration supports the following restore types:

- Offline database restore and rollforward operations.
- Offline and online table space restore and rollforward operations.
- Automatic restore from incremental or delta backups. In this case, the following must be installed:
 - On HP-UX and AIX: DB2 7.2 with Fixpack 7 or higher must be installed.
 - On Linux and Windows: DB2 8.1.2 or higher must be installed.
- Restore to a new database (for database-level backups only).
- Restore to a different system.

Advantages

Integrating Data Protector with DB2 Server offers several advantages over using the internal DB2 backup and restore functionality:

- Central Management for all backup operations

The administrator can manage backup operations from a central point.

- Media Management

Data Protector has an advanced media management system, which allows users to monitor media usage and set protection for stored data, as well as to organize and manage devices in media pools.

- Backup Management

Backed up data can be duplicated during or after the backup to increase fault tolerance of backups, to improve data security and availability, or for vaulting purposes.

- Scheduling

Data Protector has a scheduler that allows the DB2 administrator to automate backups to run periodically. Using the Data Protector Scheduler, you can configure the backups to run unattended, at specified times, if the devices and media are set properly.

- Device Support

Data Protector supports a wide range of devices: files, standalone drives, very large multiple drive libraries, etc.

- Reporting

Data Protector has reporting capabilities that allow you to receive information about your backup environment. You can schedule reports to be issued at a specific time or attached to a predefined set of events, such as the end of a backup session or a mount request.

- Monitoring

Data Protector has a feature that allows the DB2 administrator to monitor currently running sessions and view finished sessions from any system that has the Data Protector User Interface installed.

All backup sessions are logged in the Data Protector internal database (IDB), which provides the administrator with a history of activities that can be queried later.

Prerequisites and Limitations

This is a list of prerequisites and limitations for the Data Protector DB2 integration:

Prerequisites

- It is assumed that you are familiar with the DB2 database administration and basic Data Protector functionality.
- Before you begin, make sure that you have correctly installed and configured DB2 Server and Data Protector systems. Refer to the:
 - *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, devices, and other information.
 - *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions on how to install Data Protector on various architectures and how to install the Data Protector IBM DB2 UDB integration.
 - *HP OpenView Storage Data Protector Administrator's Guide* for general information on how to configure and run backups.
 - *DB2 Administration Guide*
 - *DB2 Server Books Online* for online information on DB2 Server.
- To perform an online backup of DB2 objects you need to set the DB2 `logretain` and `userexit` parameters to `ON`. The backup will fail if the database does not have these parameters set correctly.

On Windows, to perform an offline backup of one or several DB2 tablespaces (not the whole database), the DB2 `logretain` parameter must be set to `ON`.
- To perform incremental or delta backup, the DB2 `trackmod` parameter must be set to `ON`.
- On HP-UX and AIX systems, fixpack 7 is required for Data Protector integration with DB2 7.2. After you have installed the fixpack, update the DB2 instances by running the DB2 command `db2iupdt`.

On Linux and Windows systems, DB2 8.1.2 version is required.

Limitations

- The following is not supported:
 - Backup or restore to Data Protector media using the DB2 Command-Line Processor or the DB2 Control Center.
 - Backup of a partitioned database.
 - Table or datafile backup and restore.
 - Restore to a new database is supported for database-level backups only.
 - DB2 temporary table spaces can only be backed up during the full database backup.
 - Rollforward recovery of system catalog can only be performed if no other table spaces from the same DB2 database are being restored from the same session.
- If a backed up tablespace is dropped in DB2 after the backup, such a tablespace can only be restored from a full database backup session.

Integration Concept

DB2 Components The DB2 part of the integration provides an open interface for backing up and restoring DB2 objects. This allows you to use Data Protector as a data transferring module for database backup and restore operations.

Data Protector Components The Data Protector integration software consists of the following components:

- The `db2bar` module, which is installed on the DB2 Server system. It controls the activities between DB2 Server and the Data Protector backup and restore processes.
- The `libob2db2` component, which is the actual data transferring module, called by DB2 Server.
- The `db2arch` program, which performs backup and restore of the DB2 log files. It is called automatically if the `DB2 logretain` and `userexit` parameters are set to ON.
- The `util_db2` utility, which is used by Data Protector to configure a DB2 instance and check the instance configuration.
- The `testbar2` utility, which checks the Data Protector part of the integration.

From the perspective of DB2 Server, Data Protector is seen as media management software. On the other hand, DB2 Server is a Data Protector client from the Data Protector Cell Manager's point of view.

The concept of the Data Protector DB2 integration is described in Figure 2-2 on page 114.

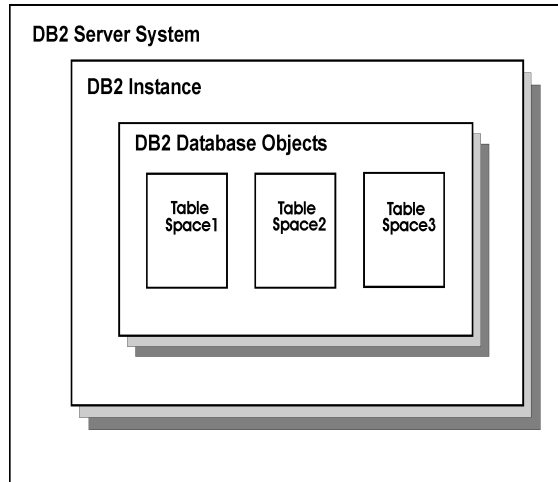
DB2 Database Concepts The following DB2 database concepts are important from the backup perspective:

- **Instance**, which controls the operations performed on data and manages system resources assigned to it. Each instance has its own *databases*, which other instances cannot access.
- **Database**, which presents data as a collection of tables, where each table consists of a defined number of columns and any number of rows. A database is organized into the parts called *table spaces*.

- **Table spaces**, which are the places for storing tables. A table space can be spread over to one or more physical storage devices.

See Figure 2-1 on page 110 for the DB2 database structure overview.

Figure 2-1 DB2 Database Structure



Recovery Methods Two recovery methods, used to restore DB2 database objects, are version and rollforward recovery. They are closely connected with the DB2 database logs, which keep records of database changes. If a database needs to be restored to a point beyond the last full offline backup, logs are required to roll the data forward to the point of failure.

- **Version recovery** is the restore of a previous version of the database using an image created during a backup operation. A database restore operation rebuilds the entire database using a database backup performed earlier. This allows you to restore a database to the state identical to the one at the time that the backup was made.

A “ring” of online log files is used to provide recovery from transaction failures and system crashes. This behavior is called **circular logging**. With this type of logging, only full offline backups of the database are possible. Circular logging does not allow you to roll forward a database through prior transactions from the last full

backup. Recovery from media failures and disasters is done by restoring from a full offline backup. Every unit of work from the time of a full backup to the time of failure is lost.

- **Rollforward recovery** is the restore of a database or a table space to its state at a specified point in time. A log is closed and becomes archived when changes in the active log are no longer needed for normal processing. This behavior is called **archived logging**. At the end of the restore operation, the database is in the rollforward pending state that allows the rollforward recovery to take place.

The archived logs can be online, meaning that a log is stored in the database log path directory, and offline, meaning that a log is no longer found in the database log path directory.

The archived logs are backed up and restored using the DB2 User Exit program, which is called whenever a new offline redo log appears, but no sooner than the previous backup or restore is completed.

There are two types of rollforward recovery:

- ✓ Database rollforward recovery. If this type of rollforward recovery is used, the transactions, recorded in database logs, are applied following the database restore operation. The database logs record all changes made to the database. This method completes the recovery of the database to its state at a particular point in time, or to its state immediately before the failure.
- ✓ Table space restore and rollforward. If the database is enabled for rollforward recovery, you may also back up, restore and roll forward table spaces. To perform a table space restore and rollforward, you must have the following:
 - Backup image of either the entire database (that is, all table spaces), or one or more individual table spaces.
 - The log records affecting the table spaces that are to be recovered.

You can roll forward through the logs to one of the following two points:

- the end of logs
- a particular point in time (point-in-time recovery).

NOTE

All DB2 timestamps in messages during rollforward recovery are by DB2 design in Universal Coordinated Time (UCT) format.

See “Restore Options” on page 140 for information on the rollforward restore options.

Backup Flow

The basic backup unit is a table space. It means that only table spaces or databases can be selected for backup.

A backup session is started by the Data Protector Backup Session Manager (BSM). The BSM invokes `db2bar`, which, using the DB2 API, starts the backup applying the backup options defined in the backup specification. After that, DB2 Server calls the sequence of functions from the `libob2db2` shared library, which performs the backup. At this point, the BSM starts General Media Agents, which write the data to the backup devices.

In case of an online backup, DB2 Server closes the log files, and then calls the `db2arch` module, which is the User Exit program responsible for backing up log files. After a successful backup of a log file, the file is automatically deleted by DB2 Server.

Messages from the backup session are sent to the BSM, which writes them and the information regarding the respective session to the IDB.

Backup Types

Three types of backup supported by the Data Protector DB2 integration are **full**, **incremental**, and **delta**.

A full backup is a backup of all selected database objects regardless of whether they have been changed after the last backup was made. Some data, such as database configuration, history file, etc, which is important for restore, is included into the full backup automatically. An incremental backup selects all the changes made to the database after the last full backup. A delta backup is a backup containing all the changes made to the database from the last backup of any type.

Restore Flow

A restore session is started by the Data Protector Restore Session Manager (RSM). The RSM invokes the `db2bar` utility, which starts the restore using the DB2 API. After that, DB2 Server calls the sequence of functions from the `libob2db2` shared library, which performs the restore. At this point, the RSM starts General Media Agents, which read

the data from the backup devices and send it to the DB2 Server through the processes `libob2db2` library. The DB2 Server processes write the data to disks.

In case you are performing a recovery from an incremental or delta backup, Data Protector will first restore the selected backup session in order to get information about DB2 backup chain history. Then it will restore the last full backup (of the selected incremental/delta backup) and finally the last incremental backup and/or all subsequent delta backups.

In case of a restore from an online backup, the rollforward operation is performed. DB2 Server calls the `db2arch` module, which is the User Exit program responsible for restoring log files, to restore the logs, needed for rollforward, one by one.

Messages from the restore session are sent to the RSM, which writes them and the information regarding the respective session to the IDB.

The architecture of the Data Protector DB2 integration is presented in Figure 2-2 on page 114.

Figure 2-2 Data Protector DB2 Integration Concept

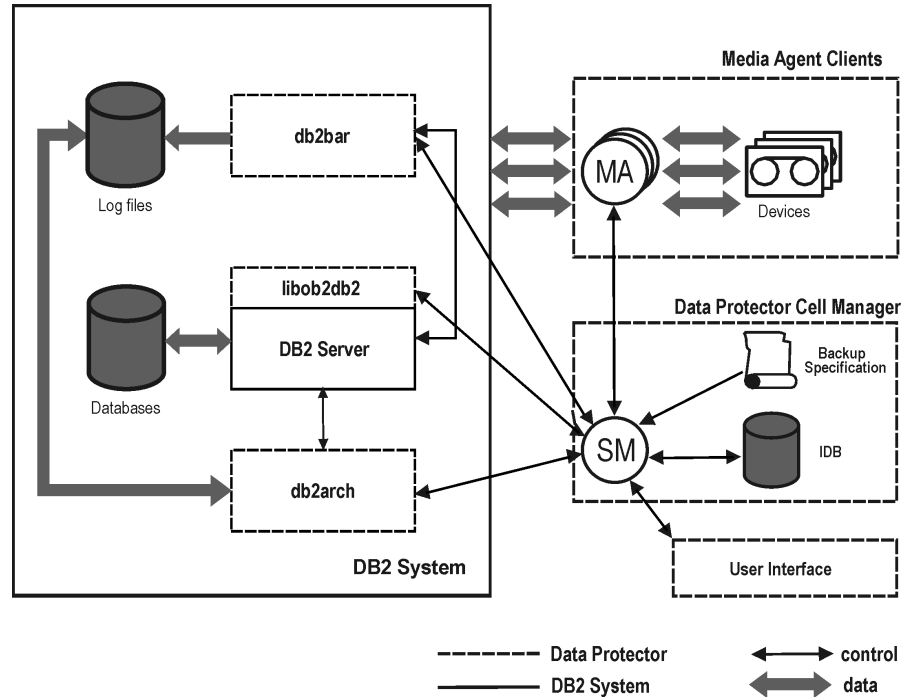


Table 2-1

Legend

SM	The Data Protector Session Manager, which is the Data Protector Backup Session Manager during a backup session, and the Data Protector Restore Session Manager during a restore session.
MA	The Data Protector General Media Agent, which reads and writes data from and to media devices.
IDB	The Data Protector internal database where all the information about Data Protector sessions, including session messages, objects, data, used devices and media is written.

Configuring the Integration

It is assumed that the installation of the Data Protector software components on the DB2 Server system was successful.

Prerequisites

To perform incremental or delta backup, the DB2 `trackmod` parameter must be set to `ON`.

To perform an online backup of DB2 objects you need to set the DB2 `logretain` and `userexit` parameters to `ON`. The backup will fail if the database does not have these parameters set correctly.

On Windows, to perform an offline backup of one or several DB2 tablespaces (not the whole database), the DB2 `logretain` parameter must be set to `ON`.

For the information on how to set these database parameters, refer to the *DB2 Administration Guide*.

Configuration Overview

The following list gives an overview of the global tasks for configuring the DB2 integration:

1. “Configuring a DB2 User” on page 115.
2. “Configuring a DB2 Instance” on page 116
3. “Configuring a DB2 Backup” on page 117.

Configuring a DB2 User

A DB2 user must be created in the operating system and has to be given either the `SYSADM`, `SYSCTRL`, or `SYSMAINT` DB2 authorities in order to perform backup and restore-related operations. This user must be entered during the configuration and restore procedure.

Additionally, the root user (UNIX systems) or the a DB2 user (Windows systems) has to be a member of the Data Protector `admin` group and of the DB2 `admin` group. This user is needed by Data Protector to start the Data Protector `Inet` service (Windows systems) or `process` (UNIX systems).

Configuring a DB2 Instance

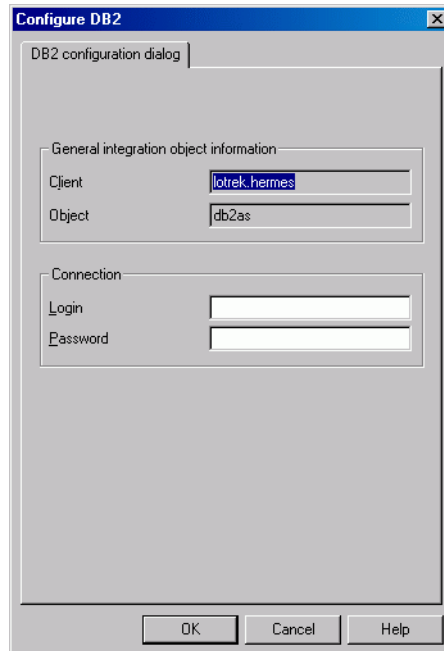
The parameters that need to be specified during the configuration of a DB2 instance are the username and the password of the DB2 user. This user is described in “Configuring a DB2 User” on page 115. These parameters will be also used for establishing the connection to the DB2 Server system if the user starts non-backup and non-restore-related operations, such as listing of objects for backup.

The configuration is performed during the creation of a new backup specification, or by modifying an existing backup specification. For a step-by-step procedure on creating a backup specification, see “Creating a Backup Specification” on page 118.

The procedure below describes the configuration of a DB2 instance using an existing backup specification:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand Backup, Backup Specifications, and then DB2 Integration. Click an existing backup specification.
3. Right-click the name of the DB2 Integration listed in the Source property page, and then select Configure from the pop-up window.
4. In the Configure DB2 window, specify the username and the password of the DB2 user. This user is described in “Configuring a DB2 User” on page 115.

Figure 2-3 DB2 Configuration



Click **OK** to confirm the configuration.

If properly configured, the DB2 user is allowed to back up or restore the DB2 database objects. In order to start a backup of a DB2 database object using Data Protector, the user must also be the owner of the Data Protector backup specification.

Refer to the DB2 documentation for further information on different types of connections, the roles and authorities of DB2 database administrators and security issues that must be considered.

Configuring a DB2 Backup

To configure a DB2 backup, perform the following steps:

1. Configure the backup devices, media, and media pools.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* or online Help for instructions.

2. Create a backup specification.

The Data Protector backup specification is stored on the Cell Manager system and contains instructions on how to perform a backup using Data Protector.

Once the backup specification is created and saved, it can be scheduled so that unattended backups can be performed.

Creating a Backup Specification

To create a backup specification for backing up the DB2 database objects, proceed as follows:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand Backup, and then Backup Specifications.
3. Right-click DB2 Integration and then select Add Backup. The Create New Backup dialog box is displayed.
4. Select one of the templates described below:

Database_Backup

Used for online and offline backups of DB2 database objects only. You cannot perform an archive log backup using this template.

Archived_Logs_Backup

Used for backing up archived logs only. You cannot perform a database objects backup using this template. The backup specification created using this backup template can only be saved, and not started or scheduled. It will be used any time the User Exit program starts the backup of archived logs.

You should not create a new archived logs backup specification if an older archived logs backup specification already exists. You must erase the old one first.

IMPORTANT

Whenever an online database backup is started, DB2 also tries to back up archive logs, therefore you must create an archive logs backup specification prior to running online db2 backup. Since the backup of archived logs is started automatically at the time a new offline archived log appears, you must always have a device that will be used only for the backup specification created using the `Archived_Logs_Backup` template.

Click OK.

5. Select the client on which DB2 Server is running (if the application is cluster-aware, select the virtual server), and the application database. Data Protector lists all the configured DB2 instances located on this system. If the instance has not been configured yet, enter the instance name.

On UNIX systems, enter the username and the password for the DB2 user. This user is described in “Configuring a DB2 User” on page 115.

If the application database you have entered had not been configured yet, the configuration window appears. See step 4 on page 116 for information on parameters that must be entered in the configuration window.

Figure 2-4 Selecting a Client System and an Instance on UNIX Systems

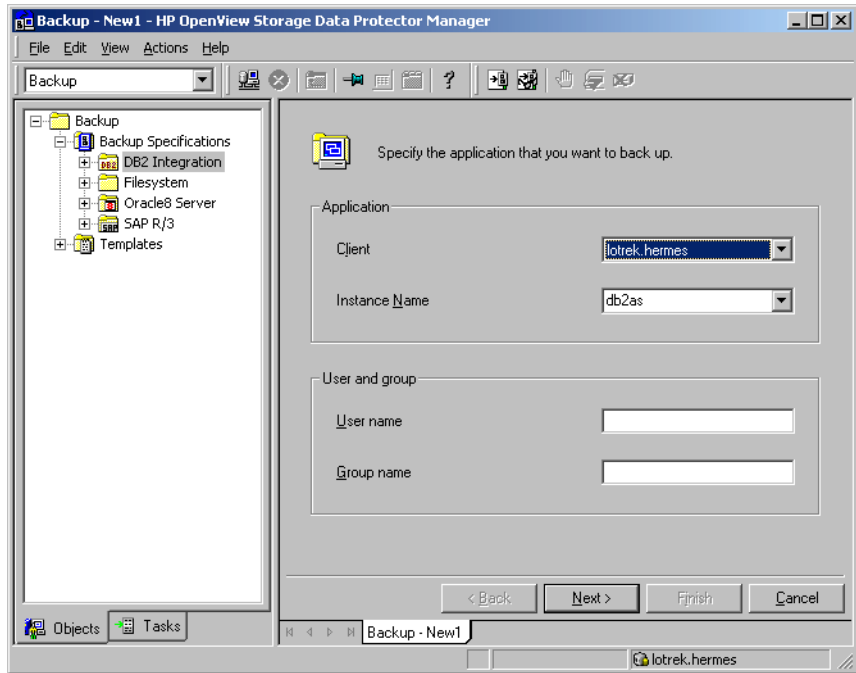
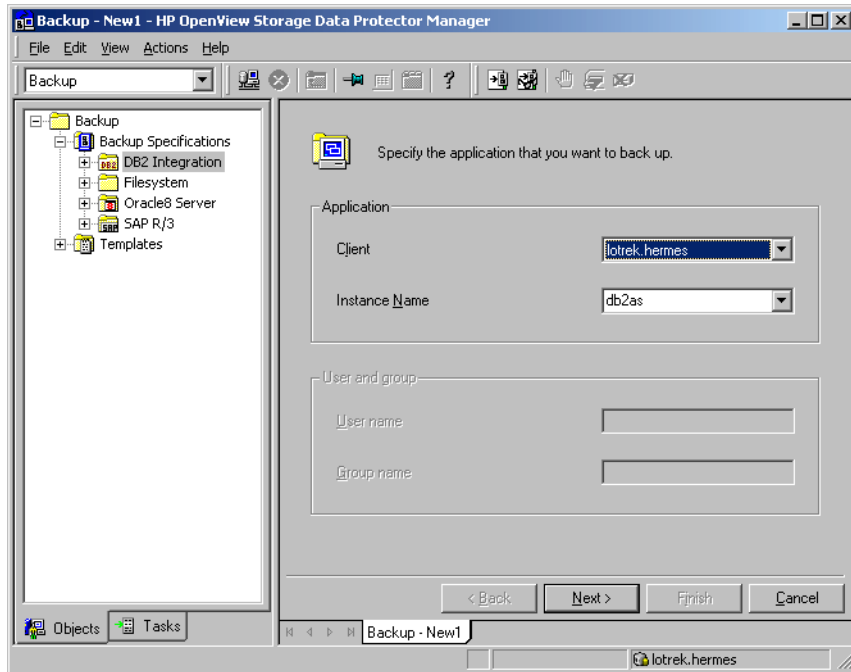
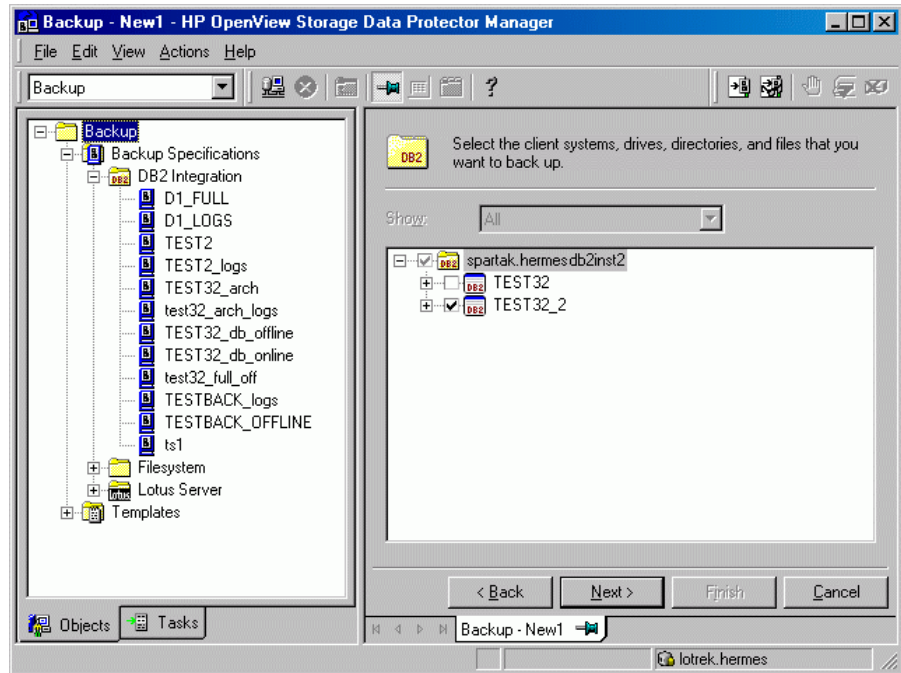


Figure 2-5 Selecting a Client System and an Instance on Windows Systems



6. Click Next.
7. In the next step of the wizard, select the database objects you want to back up.

Figure 2-6 Selecting Backup Objects



8. Follow the wizard to define devices, options, and schedule.

Refer to the Data Protector online Help and the *HP OpenView Storage Data Protector Administrator's Guide* for a description of the backup options common to all backup objects.

Select the device(s) you want to use for the backup. Click **Properties** to set the device concurrency, media pool, and preallocation policy. For more information on these options, click **Help**.

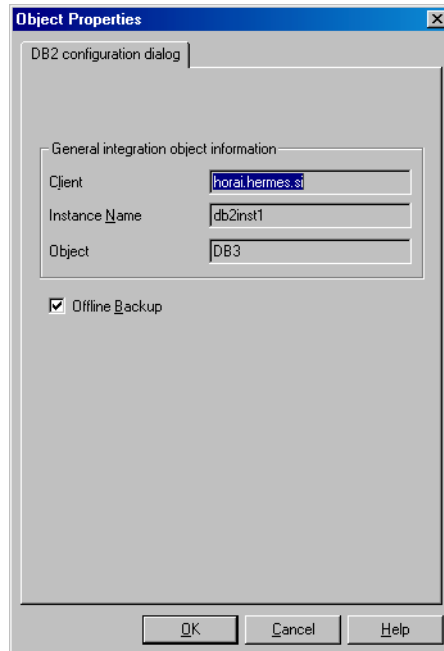
You can also specify whether you want to create additional copies (mirrors) of the backup during the backup session. Specify the desired number of mirrors by clicking the **Add mirror** and **Remove mirror** buttons. Select separate devices for the backup and for each mirror. The minimum number of devices required for mirroring DB2 integration objects equals the number of devices used for backup.

For detailed information on the object mirror functionality, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

See “DB2 Specific Backup Options” on page 124 for details about the DB2 backup options.

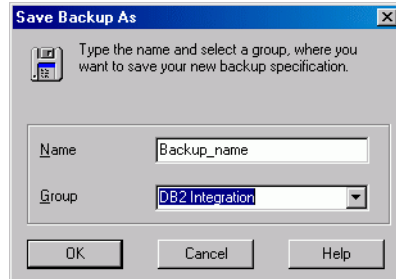
9. To perform an offline backup of the object, click **Properties** in the **Backup Object Summary** page at the end of the wizard. The **Object Properties** dialog box is displayed. Select the **Offline Backup** option. See Figure 2-7.

Figure 2-7 **The Offline Backup Option**



10. Once you have defined all the backup options, name and save your DB2 backup specification. It is recommended that you save all the DB2 backup specifications in the **DB2 Integration group**.

Figure 2-8 Saving the Backup Specification



After the backup specification is saved, it can be started either from the Data Protector GUI or the Data Protector CLI, or can be scheduled to run automatically using the Data Protector Scheduler. See “Backing Up a DB2 Database” on page 128 for information on how to perform a backup using the Data Protector GUI or the Data Protector CLI and on how to schedule a backup specification.

You can examine the newly created and saved backup specification in the Backup context. The backup specification is stored in the `<Data_Protector_home>\config\server\barlists\db2\<backup_specification_name>` file on the Windows Cell Manager and in the `/etc/opt/omni/server/barlists/db2/<backup_specification_name>` file on the UNIX Cell Manager.

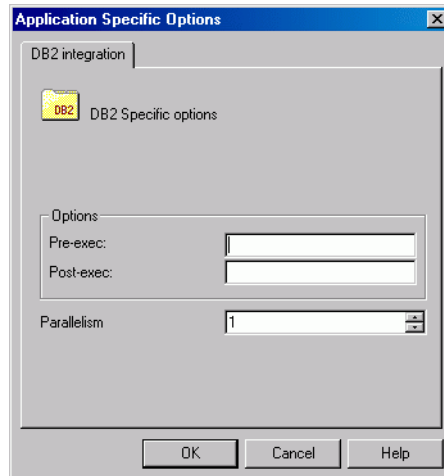
It is recommended that you test the backup specification by clicking the Start Preview button. This is an interactive test that does not back up any data. However, as a result of this test, the file `<Data_Protector_home>\tmp\<Backup_Specification_Name>_TEST_FILE` is created on the DB2 Server system. It should be deleted after the test. See “Testing the Integration” on page 126 for a step-by-step procedure.

You can start an interactive backup that includes data transfer by clicking the Start Backup button.

DB2 Specific Backup Options

The DB2 specific backup options are specified using the Data Protector GUI by clicking the Advanced button next to Application Specific Options.

Figure 2-9 Backup Options



The following are the DB2 specific backup options:

Pre-exec Specifies a command with arguments or a script that will be started on DB2 Server before the backup. This command/script is started by the Data Protector db2bar module and must reside in the /opt/omni/lbin (HP-UX systems), in the /usr/omni/bin (other UNIX systems), or in the <Data_Protector_home>\bin (Windows systems) directory. Only the filename, relative to the directory named above, must be provided in the backup specification. For more information on pre-exec commands, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Post-exec Specifies a command with arguments or a script that will be started on DB2 Server after the backup. This command/script is started by the Data Protector db2bar module and must reside in the /opt/omni/lbin (HP-UX systems), in the /usr/omni/bin (other UNIX systems), or in the <Data_Protector_home>\bin (Windows systems) directory. Only the filename, relative to the directory named above, must be provided in the

backup specification. For more information on post-exec commands, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Parallelism Specifies the number of data streams created during the backup. The default value is 1.

Testing the Integration

Once you have created and saved a backup specification, you should test it before running a backup.

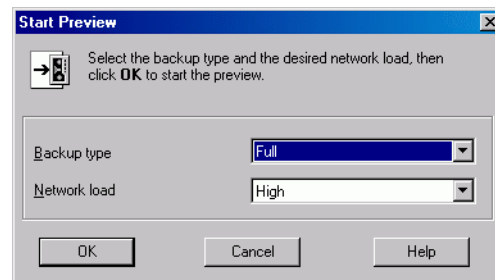
Testing Using the Data Protector GUI

Testing Procedure The testing procedure consists of checking the Data Protector part of the integration to ensure the communication within Data Protector is established and the data transfer works properly. Proceed as follows to test the integration:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand Backup, then Backup Specifications, DB2 Integration and right-click the backup specification you want to preview.
3. Click Preview Backup to open the Start Preview dialog box. Select the type of backup you want to run as well as the network load. For a description of these options, press **F1**.

Figure 2-10

Previewing a Backup



Testing Using the Data Protector CLI

To test a backup specification, run the `omnib` command with the `-test_bar` option.

On HP-UX systems, execute the following command:

```
/opt/omni/lbin/omnib -db2_list <backup_specification_name> \  
-test_bar
```

On other UNIX systems, execute the command given below:

```
/usr/omni/bin/omnib -db2_list <backup_specification_name> \  
-test_bar
```

On Windows systems, execute the command given below:

```
<Data_Protector_home>\bin\omnib -db2_list  
<backup_specification_name> -test_bar
```

What Happens?

The session messages are displayed on the screen during the command execution.

The `db2bar` program is started, which then starts the Data Protector `testbar2` command. This command checks the following:

- if the communication within Data Protector works properly.
- if the syntax of the DB2 Integration backup specification is correct.
- if the devices are correctly specified.
- if the required media reside in the devices.

After that, the DB2 part of the preview is started, which checks if all the backup objects are present and are in a correct state for a backup.

Backing Up a DB2 Database

There are two modes for backing up DB2 database objects: the online and the offline database backups.

During an online backup, the database is open and available for the other applications. During an offline backup, the database is closed and unavailable for use.

IMPORTANT

Before you perform an online backup of DB2 objects, set the DB2 `logretain` and `userexit` parameters to `ON`. The backup of archive log files will not be possible if the database does not have these parameters set correctly.

To perform incremental or delta backup, the DB2 `trackmod` parameter must be set to `ON`.

On Windows, to perform an offline backup of one or several DB2 tablespaces (not the whole database), the DB2 `logretain` parameter must be set to `ON`.

If a backed up tablespace is dropped in DB2 after the backup, such a tablespace can only be restored from a full database backup session.

To run a backup, use any of the following methods:

- Schedule a backup of an existing DB2 Integration backup specification using the Data Protector Scheduler.
- Start an interactive backup using the Data Protector GUI or the Data Protector CLI.

To back up archived logs, you have to create a backup specification using the `Archive_Log_Backup` template. See “Creating a Backup Specification” on page 118. Note that you can only save this type of backup specification, but not execute or schedule it. The backup of archived logs will be started automatically as soon as a new offline archived log file appears.

To back up DB2 temporary table spaces, you have to perform full database backup. Individual restore of temporary table spaces is possible only from full database backup.

To enable incremental or incremental delta online backups you must first enable modification tracking. To do so, you have to perform the following steps:

1. Run the following command to activate modification tracking:

```
db2 update db cfg for <DatabaseName> USING TRACKMOD ON
```

2. Restart the database.
3. Perform a full offline database backup to a non-Data Protector media using the following command:

```
backup db <db_name>
```

Scheduling an Existing Backup Specification

For more detailed information on scheduling, refer to the online Help index keyword “scheduled backups”.

Data Protector allows you to run unattended backups at specific times or periodically. The powerful Data Protector Scheduler can highly influence the effectiveness and performance of your backup.

To schedule a new DB2 backup specification, follow the steps described in “Creating a Backup Specification” on page 118.

To schedule an existing backup specification, perform the following steps in the HP OpenView Storage Data Protector Manager:

Scheduling Procedure

1. In the Context List, select Backup.
2. In the Scoping Pane, expand Backup, then Backup Specifications. Click DB2 Integration.

A list of backup objects is displayed in the Results Area.

3. Double-click the backup specification you want to schedule and click the Schedule tab to open the Schedule property page.
4. In the Schedule property page, select a date in the calendar click Add to open the Schedule Backup dialog box.
5. Specify Recurring, Time options, Recurring options, and Session options. See Figure 2-11 on page 130.
6. Click OK to return to the Schedule property page.
7. Click Apply to save the changes.

NOTE

You cannot schedule a DB2 backup specification created using the Archive_Log_Backup template, because such a backup specification is only triggered by a finished log file transaction.

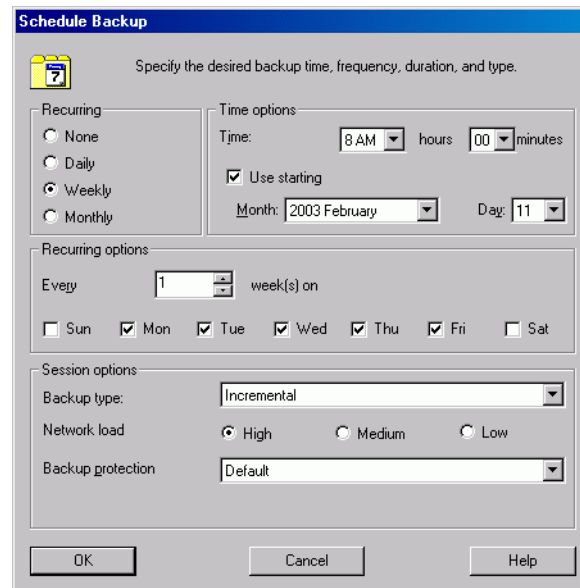
Scheduling Example

To schedule a backup specification so as to back up table spaces at 8.00 a.m., and then at 1.00 p.m. and at 6.00 p.m. during week days, open the Schedule property page of the backup specification as described in the above procedure, and then proceed as follows:

1. In the Schedule property page, click Add to open the Schedule Backup dialog box.
2. Under Recurring, select Weekly. Under Time options, select the time 8 AM. Under Recurring Options, select Mon, Tue, Wed, Thu, and Fri. Under Session options, select the Incremental backup type. Click OK.

See Figure 2-11 on page 130.

Figure 2-11 Scheduling the Backup Specification



3. Repeat steps 1 and 2 to schedule another backup. Specify options as described, except the time, which should be set to 1 PM.
4. Repeat steps 1 and 2 to schedule another backup. Specify options as described, except the time, which should be set to 6 PM.
5. Click Apply to save the changes.

After scheduling your backup, you can have it run unattended or you can still run it interactively, as shown in the next section.

Refer to the online Help or the *HP OpenView Storage Data Protector Administrator's Guide* for scheduling details.

NOTE

When creating a DB2 backup specification, you access the Data Protector Scheduler through the Backup Wizard. See “Creating a Backup Specification” on page 118 for information about accessing the Backup Wizard.

Running an Interactive Backup Using the Data Protector GUI

An interactive backup can be run any time after the backup specification has been created and saved.

Backup Procedure To start an interactive backup of a DB2 backup object using the Data Protector GUI, perform the following steps:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand the Backup, and then the Backup Specifications items.

Expand DB2 Integration. A list of backup specifications appears.

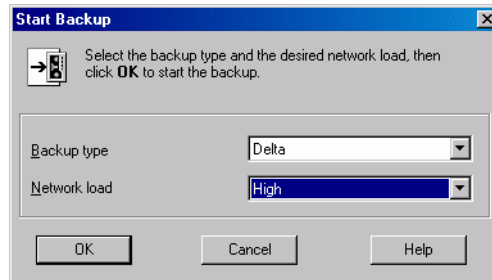
3. Right-click the backup specification you want to back up, and then select Start Backup from the pop-up menu.

The Start Backup dialog box appears.

Select the backup type and network load. For a description of these options, press **F1**.

Click OK.

Figure 2-12 Starting an Interactive Backup



Messages appear in the Results Area as the backup session proceeds. Upon successful completion of the backup session, the `Session completed successfully` message and backup size are displayed. Backup size is by DB2 design calculated as size of full database backup + size of incremental/delta backup.

Running an Interactive Backup Using the Data Protector CLI

You can start an interactive backup from the Data Protector CLI. Switch to the `/opt/omni/lbin` (HP-UX systems), to the `/usr/omni/bin` (other UNIX systems), or to the `<Data_Protector_home>\bin` (Windows systems) directory and run the following command:

```
omnib -db2_list <ListName> [-barmode <db2mode>]
[<list_options>] [-preview]
```

The `<ListName>` parameter is the name of a backup specification.

The `<db2mode>` parameter specifies the type of the backup.

The `<list_options>` parameter sets the level of the protection, the level of the network traffic generated by the session, enables writing a CRC checksums, and disables monitoring of the backup session.

You can select among the following `<db2mode>`: {full | incr | delta}

You can select among the following `<list_options>`:

```
-protect {none | weeks n | days n | until date | permanent}
-load {low | medium | high}
-crc
-no_monitor
```


Example

To start a full backup using an existing DB2 backup specification called TEST, and to set data protection to 10 weeks, execute the following command:

```
omnib -db2_list TEST -barmode full -protect weeks 10
```

Restoring a DB2 Database

You can restore a DB2 object using either the Data Protector GUI or the Data Protector CLI.

You can restore a previous version of the database using an image created during a backup operation, that is, to perform a version recovery. Also, you can restore the database(s)/table space(s) to their state at a specified point in time, that is, to perform a rollforward recovery. The rollforward operation ensures that all the changes made to the database during the online backup are captured and reapplied.

NOTE

Rollforward recovery of system catalog can only be performed if no other table spaces from the same DB2 database are being restored from the same session. Rollforward recovery of a system catalog can only be performed to the end of logs.

For more information on recovery methods, see “Integration Concept” on page 109.

NOTE

If you use the version recovery method, make sure that you perform full offline database backups on a regular basis.

IMPORTANT

The database restore and rollforward operations must always be performed offline. The table space (except for DB2 System Catalog) restore and rollforward can be performed online; though the table space itself is not available until the operation completes, you still can access data in other table spaces.

Restoring a DB2 Object Using the Data Protector GUI

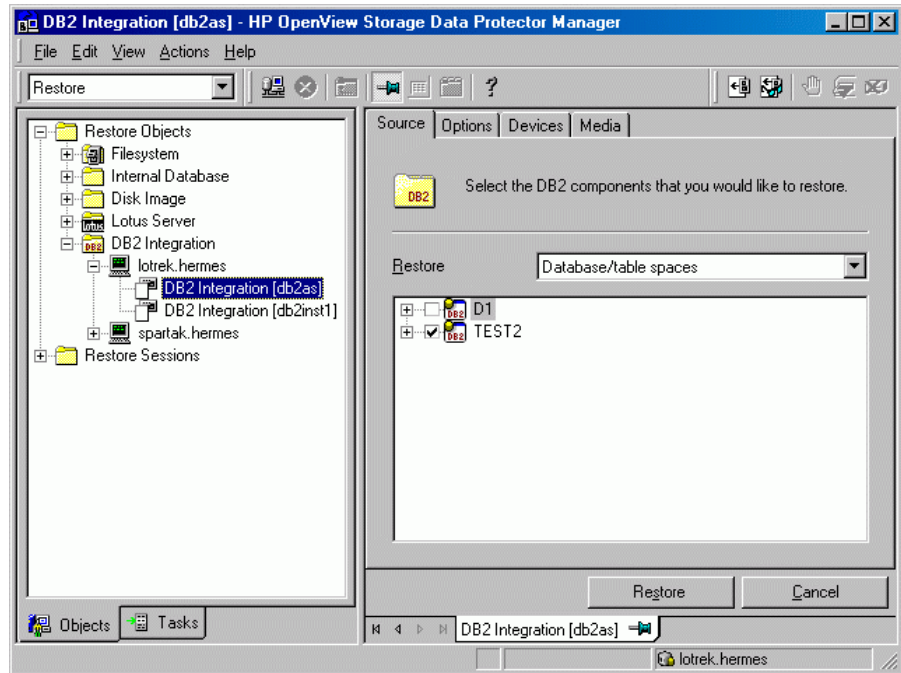
Use the following procedure to restore a DB2 database object using the DP GUI:

1. In the HP OpenView Storage Data Protector Manager, switch to the Restore context.
2. In the Scoping Pane, expand DB2 Integration, and then the name of the client system from which the data you want to restore was backed up.
3. In the Source property page, browse for and select the backed up DB2 database objects you want to restore. The top-level elements are databases, and the second-level elements are table spaces.

The latest backed up version of each log file is restored automatically during the rollforward operation. However, in some cases, you may want to restore the version of a log file other than the latest. If you want to restore specific log files, select the Archive logs option and then select log files you want to restore.

You may check the properties of each object by right-clicking the object name.

Figure 2-13 Restore Objects

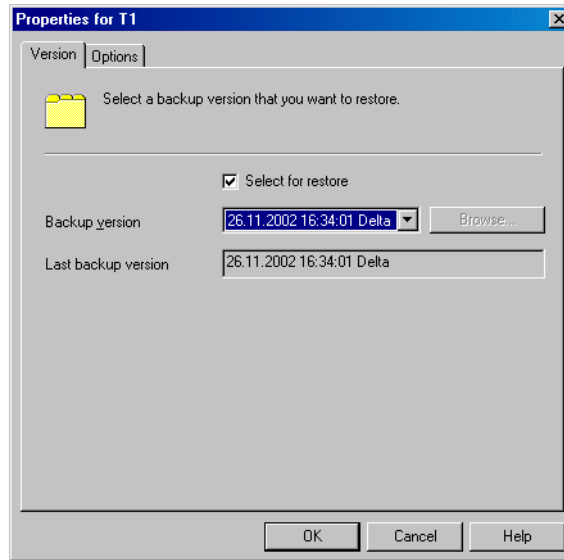


Under the Version tab in the Properties window, select the version from which you want to restore the data. The version is identified by the date and time of a backup and the backup type. If you are restoring the log files, only the date and time of a backup is displayed.

NOTE

By default, the latest version of the object is selected. If you want to restore some other version, select it from the Backup version drop-down list.

Figure 2-14 **Selecting a Version**

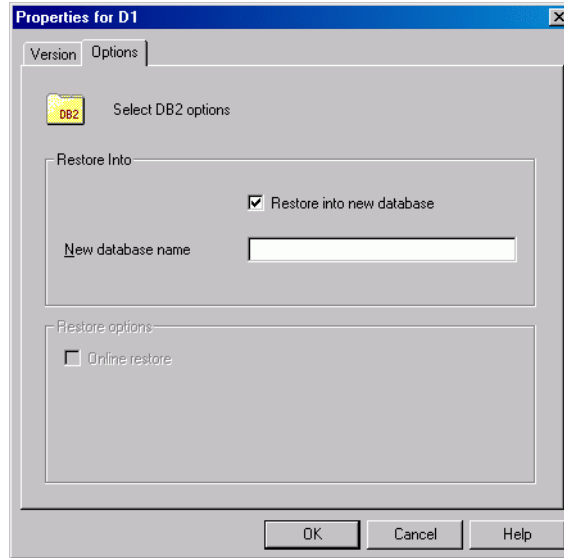


Under the Options tab in the Properties window, select the destination to which you want to restore the data. If the whole database was selected for restore, you can specify whether you want to restore it into a current or into a new database. To restore to a new database, enter the name of the new database. See “Restoring into a New Database” on page 142.

You can also specify whether you want to restore a table space offline or online.

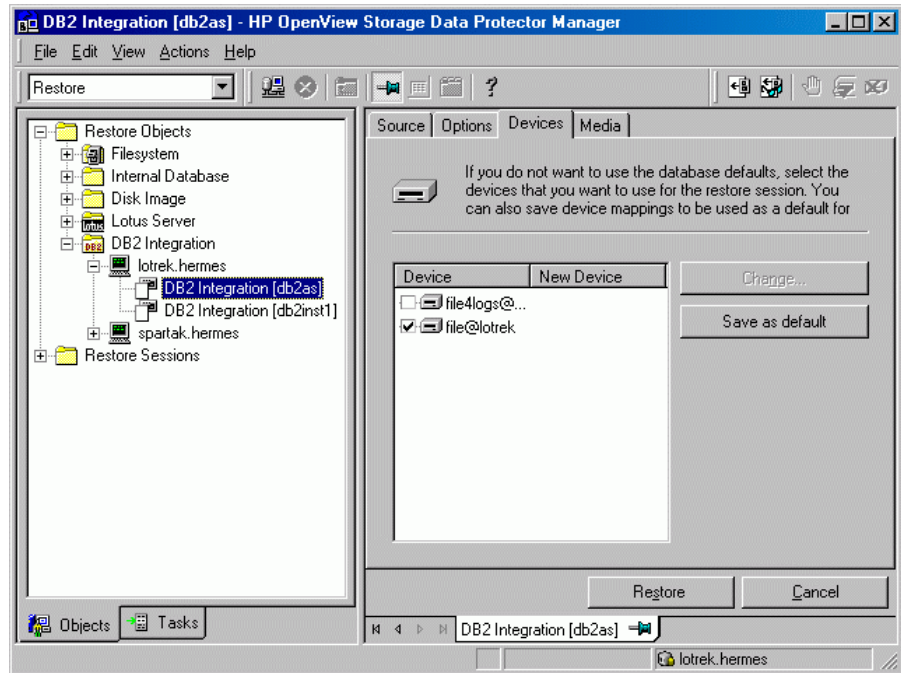
NOTE The default restore mode is online.

Figure 2-15 **Selecting a Destination**



4. Select the restore options from the `Options` property page. See “Restore Options” on page 140.
5. In the `Devices` property page, the names of devices used for backup are displayed. If you want to restore from a device different from the one used for backup, select the device you want to change, and click `Change`. The list of all configured devices is displayed. From this list, select the device you want to use for restore, and then click `OK`.

Figure 2-16 Selecting a Device



Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for more information on how to perform a restore using another device.

NOTE

If the devices, used for restore, are not those used for backup, select the same number of devices in the *Devices* property page as you used when you backed up the object.

6. Click `Restore DB2` to start the restore procedure.

The restore session messages are displayed in the *Results Area*.

Restore Options

The following restore options are specific to the Data Protector DB2 integration:

User name Enter the name of the DB2 user. This user is described in “Configuring a DB2 User” on page 115.

User group Group account of the above user.

Password Password of the above user.

Restore to client By default, the data is restored to the original backup client. However, you may restore your data to another client. In this case, enter the name of this client in the `Restore to client` text box. This option is valid for the whole database restore only. The instance with the name, specified in the `Restore to instance` text box, must be already created on the specified client and configured for use with Data Protector.

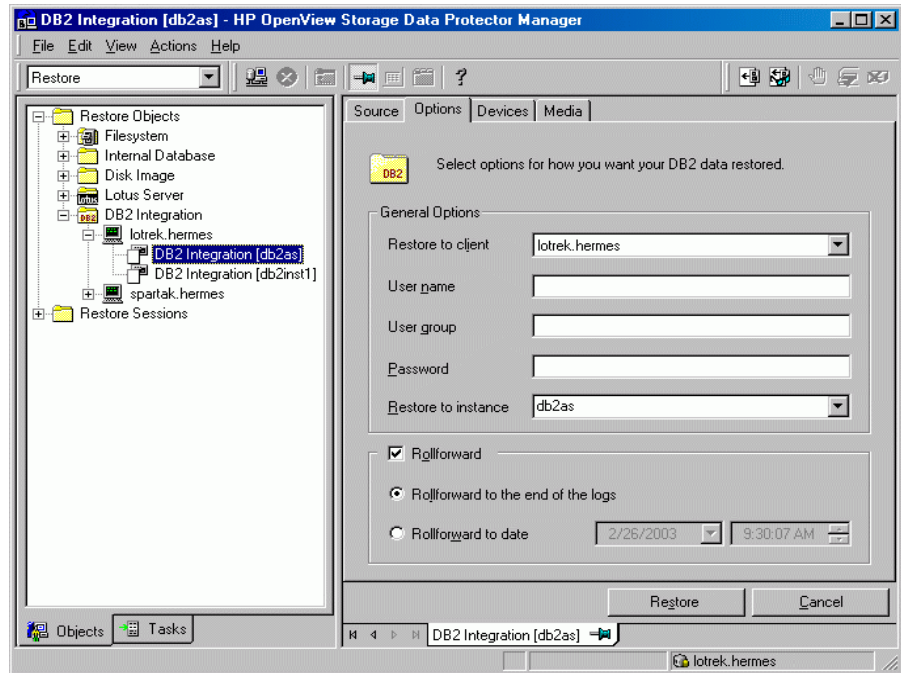
Restore to instance If you want to perform a restore to an instance other than the original, specify its name here. This instance must be created and configured prior to starting a restore session. See “Restoring to Another Instance” on page 144. By default, the original instance name is displayed.

Rollforward This option is selected by default. To perform a version recovery, deselect the `Rollforward` restore option. However, if you deselected the `Rollforward` option and you are restoring from an online backup, the database goes into the rollforward pending state and is unavailable for use. To make the database available, start the rollforward operation using the DB2 Command-Line Processor or the DB2 Control Center.

Rollforward to the end of logs Rollforward is performed to the end of logs. This option is available only if the `Rollforward` option is selected.

Rollforward to date Rollforward is performed to a particular point in time. This option is available only if the `Rollforward` option is selected.

Figure 2-17 Restore Options



Restoring a DB2 Object Using the Data Protector CLI

You can also start a restore session from the Data Protector CLI. Switch to the `/opt/omni/sbin` (HP-UX systems), to the `/usr/omni/bin` (other UNIX systems), or to the `<Data_Protector_home>\bin` (Windows systems) directory and run the following command:

```
omnir -db2
-barhost <ClientName>
[-destination <ClientName>]
-instance <InstName>
-dbname <DBName> [-session <SessionID>] [-newdbname
<NewDBName>] ...
[-frominstance <InstName>] ...
-tsname <TSName> [-session <SessionID>] [-offline] ...
-logfile <LogFileName> [-session <SessionID>] ...
[-rollforward [time: <YYYY-MM-DD.hh.mm.ss>]]
```

The `-barhost <ClientName>` parameter is the name of the DB2 Server system from which you are restoring; the `-destination <ClientName>` parameter is the name of the target DB2 Server.

The `<DBName>` parameter is the name of the DB2 database you want to restore (in case of a database restore); `<SessionID>` is the ID of the backup session. In case of object copies, do not use the copy session ID, but the object's backup ID, which equals the object's backup session ID. The `<NewDBName>` parameter is the name of a new database and it needs to be specified if you are restoring to a database (instance) other than the original.

The `-instance <InstName>` parameter is the name of the instance in which you want to restore the data.

The `-frominstance <InstName>` is the name of the instance from which you want to restore the data in case of restoring to a new instance.

The `<TSName>` parameter is the name of a table space you want to restore (in case of a table space restore); `<SessionID>` is the ID of the respective session.

The `<LogFileName>` parameter is the name of a log file you want to restore; `<SessionID>` is the ID of the respective session.

Example

To start an online restore of a DB2 database called TEMP on host degas and rollforward it till the 10th of January 2003, 9:15 a.m., execute the following command:

```
omnir -db2 -barhost degas -dbname TEMP -rollforward time:  
2003-01-10.09.15.00
```

Restoring into a New Database

Before you can start restoring a database into a new database, you must define the new table space containers for non-system table spaces. A container is the directory, file, or raw disk that stores table spaces.

To find all the containers needed for redirection, you can use two following commands:

- To list all table spaces in database:

```
db2 list tablespaces
```

- To find the name of the container for table space:

```
db2 list tablespace containers for <table_space_number>
```

To redefine table space containers, you have to put additional options for redirection to the DB2 configuration file using `util_cmd` utility. Execute the following command:

```
util_cmd -putopt DB2 <instance_name> "<old_container>" "<new_container>" -sublist Redirection/<dbname>
```

This command has to be executed for every container.

After that you can start restoring to a new database using GUI. The new database will be in rollforward pending state. In the case of restore from offline backup, execute the following command:

```
db2 rollforward db <dbname> stop
```

In the case of restore from online backup you will have to restore log files using Data Protector GUI and then perform rollforward from CLI with the `OVERFLOW LOG PATH` option equal to a log path of the original database:

```
db2 rollforward db <dbname> to <time> OVERFLOW LOG \  
PATH "(<original database log path>)"
```

Example

The following steps show how to perform online restore of the `db2db_old` database, which resides in `db2inst` instance, into the `db2db_new` database. The log files for `db2db_old` database are in the `/db2_db/db2inst/NODE0000/SQL00003/SQLLOGDIR` directory. In this example, one of the table spaces resides in `"/tmp/db2cont1"` container.

1. Define new container `"/tmp/db2cont2"` for table space using the `util_cmd` utility:

```
/util_cmd -putopt DB2 db2inst "/tmp/db2cont1" \  
"tmp/db2cont2" -sublist Redirection/db2db_old
```

2. Using Data Protector GUI start restoring the `db2db_old` database into the new `db2db_new` database, or using CLI, start restore using `omnir` command with the following parameters:

```
omnir -db2 -barhost <ClientName> -instance db2inst \  
-dbname db2db_old -newdbname db2db_new
```

3. Using Data Protector GUI restore all log files needed for rollforward.
4. Using Data Protector CLI perform rollforward to the end of logs executing the following command:

```
db2 rollforward db db2db_new to end of logs OVERFLOW \  
LOG PATH "(<original database log path>)"
```

Restoring to Another Instance

Before you can start restoring a database to an instance different from the original instance, you must configure the target instance by defining the new table space containers for non-system table spaces. A container is the directory, file, or raw disk that stores table spaces.

To find all the containers needed for redirection, you can use two following commands:

- To list all table spaces in database:

```
db2 list tablespaces
```

- To find the name of the container for table space:

```
db2 list tablespace containers for <table_space_number>
```

To redefine table space containers, you have to put additional options for redirection to the DB2 configuration file using `util_cmd` utility. Execute the following command:

```
util_cmd -putopt DB2 <instance_name> "<old_container>" "<new_container>" -sublist Redirection/<dbname>
```

The `<instance name>` is the name of the target instance. This command has to be executed for every container.

After configuring the target instance you can start restoring to it using Data Protector GUI. The restored database will be in rollforward pending state. In the case of restore from offline backup, execute the following command:

```
db2 rollforward db <dbname> stop
```

In the case of restore from online backup you will have to restore log files using Data Protector GUI, and then perform rollforward from CLI with the `OVERFLOW LOG PATH` option equal to a log path of the restored database:

```
db2 rollforward db <dbname> to <time> OVERFLOW LOG \  
PATH "(<restored_database_log_path>)"
```

DB2 logs will be restored to the same directory where they resided during the backup. Set the write permissions of that directory to be able to restore the logs. After log files have been restored, check if the instance you are restoring into, has all the needed permissions for the log files you are restoring.

Example

The following steps show how to perform restore of the db2db database, which resides in inst1 instance, to the db2db database in the inst2 instance.

1. Define new container "/tmp/db2cont2" for table space using the util_cmd utility:

```
/util_cmd -putopt DB2 inst2 "/tmp/db2cont1" \  
"tmp/db2cont2" -sublist Redirection/db2db
```

2. Using Data Protector GUI start restoring the db2db database to the inst2 instance, or using CLI, start restore using omnir command with the following parameters:

```
omnir -db2 -barhost <ClientName> [-destination \  
<destination_client_name>] -instance inst2 - dbname \  
db2db -frominstance inst1
```

Use the -destination option if you want to make restore to another host only.

NOTE

If you are restoring a DB2 database to another instance on another host, use db2 list tables for all command to list tables.

Monitoring a DB2 Backup and Restore

The Data Protector GUI enables you to monitor current or view previous backup and restore sessions.

Monitoring is automatically activated when you start a restore or backup interactively.

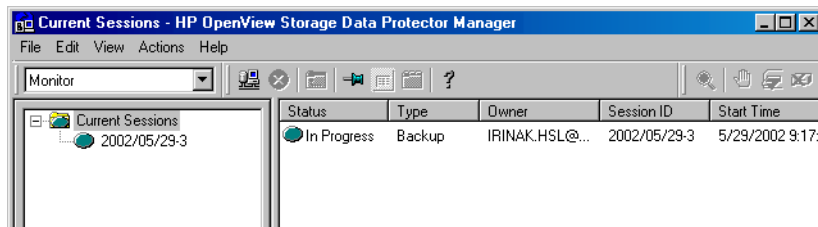
Monitoring Current Sessions

To monitor a currently running session using the Data Protector GUI, proceed as follows:

1. In the Context List, click **Monitor**.
In the Results Area, all currently running sessions are listed.
2. Double-click the session you want to monitor. See Figure 2-18.

Figure 2-18

Monitoring a Current Session



Clearing Sessions

To remove all completed or aborted sessions from the Results Area of the Monitor context, proceed as follows:

1. In the Scoping Pane, click **Current Sessions**.
2. In the Actions menu, select **Clear Sessions**. Or click the **Clear Sessions** icon on the toolbar.

To remove a particular completed or aborted session from the current sessions list, right-click the session and select **Remove From List**.

NOTE

All completed or aborted sessions are automatically removed from the Results Area of the Monitor context if you restart the Data Protector GUI.

For detailed information on a completed or aborted session, see “Viewing Previous Sessions”.

Viewing Previous Sessions

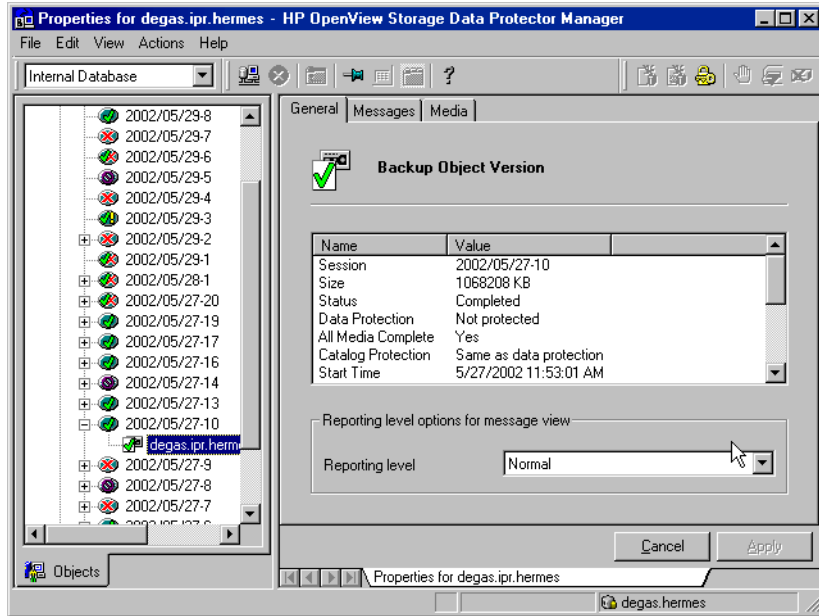
To view a previous session using the Data Protector GUI, proceed as follows:

1. In the Context List, click `Internal Database`.
2. In the Scoping Pane, expand `Sessions` to display all the sessions stored in the IDB.

The sessions are sorted by date. Each session is identified by a session ID consisting of a date in the YY/MM/DD format and a unique number.

3. Right-click the session and select `Properties` to view details on the session.
4. Click the `General`, `Messages` or `Media` tab to display general information on the session, session messages, or information on the media used for this session, respectively. See Figure 2-19.

Figure 2-19 Viewing a Previous Session



Troubleshooting

The following section provides some testing procedures you should perform before calling the Data Protector support. Following these guidelines, you may either resolve the problem yourself or identify the area where the problems occur.

Should you fail when performing a troubleshooting procedure, actions are proposed to help you work around the problem.

The section is divided into the following subsections:

- General troubleshooting
- Backup problems
- Restore problems

General Troubleshooting

1. Ensure that the latest official Data Protector patches are installed. Refer to the “Verifying Which Data Protector Patches Are Installed” section in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* or

http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, and other information.

2. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a description of general Data Protector limitations, problems and workarounds, as well as for a list of related Data Protector patches.
3. Try to run a backup and restore without using Data Protector. Use the DB2 Command-Line Processor or the DB2 Control Center to back up and restore the DB2 database objects. For details, refer to the DB2 administration reference.

Backup Problems

General Backup Troubleshooting

Start a preview of the Data Protector DB2 Integration backup specification.

- If the DB2 Server part of the preview fails, refer to the DB2 documentation.
- If the Data Protector part of the preview fails, create a DB2 Integration backup specification to back up to a null or file device and run the backup. If the backup succeeds, the problem may be related to the backup devices. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions on troubleshooting devices.
- If the preview succeeds, proceed as follows:
 1. Check if the filesystem backup of the problematic client works. It is much easier to troubleshoot a filesystem backup.
 2. Examine the errors reported in the `/var/opt/omni/log/debug.log` and `/var/opt/omni/log/db2.log` files (HP-UX systems), in the `/usr/omni/log/debug.log` and `/usr/omni/log/db2.log` files (other UNIX systems), or in the `<Data_Protector_home>\log\debug.log` and `<Data_Protector_home>\log\db2.log` files (Windows systems).
 3. Try to restart DB2 Server and start the backup again.

Online Backup Is Not Allowed

Problem	DB2 reports that online backup is not allowed because either <code>logretain</code> or <code>userexit</code> option for rollforward is not activated or that a backup pending condition is in effect for the database.
Action	After configuring the DB2 database for the rollforward recovery (<code>userexit</code> and <code>logretain ON</code>), the database has to be first backed up offline. If online backup is started first, the above error will be reported.

Offline Backup of One or Several Tablespaces Is Not Allowed (Windows Specific)

- Problem** On Windows, when backing up one or several DB2 tablespaces (not the whole database), DB2 reports that offline backup is not allowed because the DB2 logretain option is not activated or that a backup pending condition is in effect for the database.
- Action** Set the DB2 logretain option to ON.

Archived Logs Are Not Backed Up

- Problem** If you create several backup specifications and the last one is removed, the older backup specifications are not used and archived logs are not backed up.
- Action** Create a new backup specification.

Incremental Backup Is Not Enabled For the Database

- Problem** The following error message is displayed by Data Protector if incremental backup is attempted but no full backup has been performed: Incremental backup is not enabled for this database.
- Action** Perform the following steps:
1. Run the following command to activate modification tracking:
`db2 update db cfg for <DatabaseName> USING TRACKMOD ON`
 2. Restart the database.
 3. Perform a full database backup.

Error Occurred While Accessing an Object

- Problem** DB2 reports: SQL2048N An error occurred while accessing object <object>. Reason code: <CodeNumber>
- The following can be a reason (code number) for this error message:
1. An invalid object type is encountered.
 2. A lock object operation failed. The lock wait may have reached the lock timeout limit specified in the database configuration.

3. An unlock object operation failed during the processing of a database utility.
4. Access to an object failed.
5. An object in the database is corrupted.
6. The object being accessed is a table space. Either the table space is in such a state that the operation is not allowed or one or more containers of the table space is not available. (`LIST TABLESPACES` will list the current table space state.)
7. A delete object operation failed.
8. Trying to load/quiesce into a table that is not defined on this partition.

Action

If a lock object operation failed, ensure that the lock timeout limit in the database configuration is adequate and resubmit the utility command. You may also consider using the `QUIESCE` command to bring the database to a quiesced state to ensure access.

Cannot List Table Spaces

Problem

Data Protector reports: `Cannot list table spaces.`

Action

- Make sure that the database is not in a backup/restore/rollforward pending state.
- Make sure that:
 - on UNIX, the root user is in the DB2 and Data Protector admin groups, or
 - on Windows, the DB2 user is in the DB2 and Data Protector admin groups.

Restore Problems

General Restore Troubleshooting

- To restore to another instance, make sure that this instance is configured in Data Protector and running.

- Ensure that the filesystem restore of the problematic client works. It is much easier to troubleshoot a filesystem restore. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for information on troubleshooting filesystem restores.
- Examine the errors reported in the `/var/opt/omni/log/debug.log` and `/var/opt/omni/log/db2.log` files (HP-UX systems), in the `/usr/omni/log/debug.log` and `/usr/omni/log/db2.log` files (other UNIX systems), or in the `<Data_Protector_home>\log\debug.log` and `<Data_Protector_home>\log\db2.log` files (Windows systems).

A Restore from an Object Copy Hangs

Problem

When restoring from an object copy, the restore hangs.

Action

Before restarting the restore:

- Increase the number of Disk Agent buffers for the device used for the restore.
- If all objects of the backup are recorded in the IDB, perform the following steps:
 1. In the Internal Database context of the Data Protector GUI, search for all objects belonging to the same backup. The objects are identified by the same backup ID.
 2. Copy each object in a separate object copy session to a separate device, for example a file library. For each object, use a separate medium with the non-appendable media policy.
 3. Set the highest media location priority for the newly created copies.

Restore Finishes Successfully, But Rollforward Fails

Problem

When you are performing a rollforward recovery from an online backup, restore finishes successfully, but rollforward fails.

Action

Archived logs must be available in order to perform rollforward recovery. Check if they are available. If they are not available, restore them from the last backup.

3**Integrating Lotus Notes/Domino
Server and Data Protector**

In This Chapter

This chapter explains how to configure and use the Data Protector Lotus Integration. It explains the concepts and methods that you need to understand to back up and restore Lotus Notes/Domino Server.

The chapter is organized into the following sections:

“Overview” on page 157

“Prerequisites and Limitations” on page 160

“Integration Concepts” on page 161

“Configuring the Integration” on page 164

“Backing Up Lotus Notes/Domino Server” on page 176

“Restoring Lotus Notes/Domino Server Data” on page 188

“Monitoring a Lotus Notes/Domino Server Backup and Restore” on page 195

“Troubleshooting” on page 198

Overview

The Data Protector integration with Lotus Notes/Domino Server allows you to perform online as well as offline backups. To enable a recovery from an online backup, the respective Lotus Notes/Domino Server has to be set to use transactional logging. This way the transactions are stored to the transaction log directory and can be used to apply or undo database transactions during database recovery.

The online backup concept is now widely accepted because it addresses the business requirement of high application availability. During the backup, the database is online and actively used. The backup is performed quickly and efficiently, with minimal impact on database performance.

The integration also provides you with features such as library support, parallel backups, and media management for backup and restore.

Data Protector backs up all types of databases (NSF, NTF, and BOX). Full and incremental backups are possible on online as well as offline databases. You can back up a specific database or databases, or the whole server (all databases under the Lotus Notes/Domino Server).

Database restore is possible even if Lotus Notes/Domino Server is running. The restore of a specific database does not have an impact on other databases currently in use. There is also the possibility to perform a recovery to a specific point in time on a given database or on all databases under a specific server.

Lotus Integration Agent

The Data Protector Lotus Integration Agent helps to protect and manage Domino Server data by making it easy to perform the following actions:

- Online backup of the whole Lotus Notes/Domino Server or a specific database
- Backup of archived transaction logs when archive logging is in effect
- Backup of the currently filling transaction log file if Lotus Domino Server 5.0.4 or later is installed
- Centralized, online, full and incremental backup of Lotus Notes/Domino databases
- Maintenance of multiple versions of Lotus Notes/Domino database backups

Overview

- Automated scheduled backups
- Restore without performing a recovery
- Restore of backup versions of a Lotus Notes/Domino database and apply changes made since the backup from the transaction log
- Restore of Lotus Notes/Domino databases to a specific point in time or to the latest possible consistent state
- Recover to same or different Lotus Notes/Domino Server
- Restore of databases to other Lotus Notes/Domino Server location than originally backed up from
- Automatic restore of archived transaction logs in case of recovery

The Lotus Integration Agent provides online and offline backups of Notes/Domino databases and transaction logs. The Lotus Integration Agent supports two types of backup:

1. Full backup

Performs a full backup of specified Lotus Notes/Domino Server databases. In case archive transaction logging is enabled, the full backup of all archived transaction logs is taken, including the current filling transaction log, which is not yet marked as 'ready to be archived'.

2. Incremental backup

If the data changed from the last backup is more than specified in the `Amount of log` option, a full backup of specified databases is performed. Otherwise, the specified database is skipped. If archive transaction logging is enabled, the full backup of all archived transaction logs is also taken.

Advantages

Using Data Protector together with Lotus Notes/Domino Server offers several advantages over using Lotus Notes/Domino Server alone:

- Central Management for all backup operations:

The administrator can manage backup operations from a central point.

- **Media Management:**

Data Protector has an advanced media management system that allows users to monitor media usage and set protection for stored data, as well as organize and manage devices in media pools.
- **Backup management:**

Backed up data can be duplicated during or after the backup to increase fault tolerance of backups, to improve data security and availability, or for vaulting purposes.
- **Scheduling:**

Data Protector has a built-in scheduler that allows the administrator to automate backups to run periodically. Using the Data Protector Scheduler, the backups you configure run unattended at specified times, as long as the devices and media are properly set.
- **Device Support:**

Data Protector supports a wide range of devices: files, standalone drives, very large multiple drive libraries, etc.
- **Reporting:**

Data Protector has reporting capabilities that allow you to get information on your backup environment. You can schedule reports to be issued at a specific time or to be attached to a predefined set of events, such as the end of a backup session or a mount request.
- **Monitoring:**

Data Protector has a feature that allows the administrator to monitor currently running sessions and view finished sessions from any system that has the Data Protector GUI installed.

All backup sessions are logged in the IDB, which provides the administrator with a history of activities that can be queried later.

Prerequisites and Limitations

This is a list of prerequisites and limitations for the Data Protector Lotus Integration:

- You need a special license to use the Data Protector Lotus Integration. Refer to the *HP OpenView Storage Data Protector Installation and Licensing Guide* for detailed information about Data Protector licensing.
- Before you begin, ensure that you have correctly installed and configured Lotus Notes/Domino Server and Data Protector systems. Refer to the:
 - *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, devices, limitations, and other information.
 - *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions on how to install Data Protector on various architectures and how to install the Data Protector Lotus Notes/Domino Server integration.
 - *HP OpenView Storage Data Protector Administrator's Guide* for instructions on how to configure and run backups.
- It is assumed that you are familiar with Lotus Notes/Domino Server administration and the basic Data Protector functionality.

Integration Concepts

Data Protector Lotus Integration provides efficient online backup, restore and recovery of Lotus Notes/Domino Server. It uses the Lotus C API to allow third party applications to perform online backups and restores.

The central component of the Data Protector Lotus Integration is the Data Protector `ldbar.exe` executable, which is installed on the Lotus Notes/Domino Server system and which controls the activities between Lotus Notes/Domino Server and Data Protector backup and restore processes.

From the perspective of Lotus Notes/Domino Server, Data Protector is seen as a media management software. On the other hand, the Lotus Notes/Domino Server is a Data Protector client from the Data Protector Cell Manager's point of view.

Backup Flow

A Data Protector backup session can be started only from the Data Protector side.

The Data Protector Backup Session Manager reads the backup specification and starts the `ldbar.exe` command on the Lotus Notes/Domino Server system.

The `ldbar.exe` reads data from Lotus Notes/Domino Server and passes it to the Data Protector General Media Agent.

Lotus Notes/Domino Server databases are backed up in parallel depending on the sum of all concurrencies for individual device defined in the backup specification.

Backup session messages are sent to the Backup Session Manager, which then writes the messages and information regarding the respective session to the Data Protector database.

The two types of backup supported by the Data Protector Lotus Integration are **Full** and **Incremental**.

A full backup includes all backup objects specified in the backup specification regardless of whether they have changed since the last backup. An incremental backup performs a full backup of specified databases if the data changed from the last full backup is bigger than specified in the `Amount of Log` options.

There is only one level of incremental backup. It references the previous full or incremental backup, whichever was performed last.

Restore Flow

Using the Data Protector User Interface, you define which objects and objects versions to restore. The Restore Session Manager is invoked, which then starts the `ldbar.exe` with specific restore parameters. `ldbar.exe` passes the information about the objects and backup versions on to the Lotus C API. General Media Agents are started by `ldbar.exe`, and data flows from the media to target Lotus Notes/Domino Server. Refer to Figure 3-1.

Messages from the restore session are sent to the Data Protector Restore Session Manager, which writes the messages and the information regarding the respective session to the IDB.

Figure 3-1 Data Protector Lotus Integration Concept

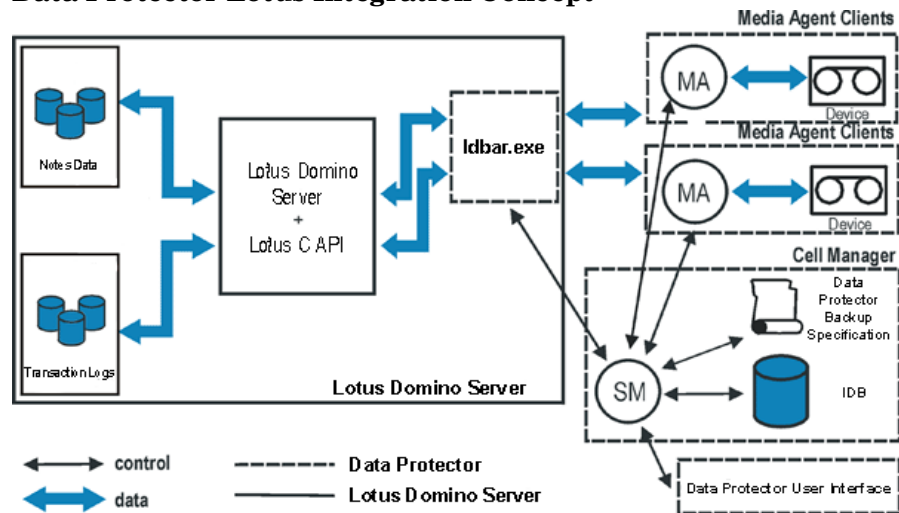


Table 3-1

Legend

SM	Data Protector Session Manager, which is, the Data Protector Backup Session Manager during a backup and Data Protector Restore Session Manager during a restore.
MA	Data Protector General Media Agent

Table 3-1

Legend

Lotus C API	The Lotus defined interface that enables data transfer between Data Protector and Lotus Notes/Domino Server.
Notes Data	The Notes/Domino database is the basic component of a Notes application. It is a repository where users create, update, store, and track documents in various formats.
Transaction Logs	Domino supports transaction logging and recovery by capturing database changes and writing them to the transaction log.

Configuring the Integration

The configuration of the Data Protector Lotus Integration is a set of procedures needed after the installation of Lotus Integration software. It consists of the following:

1. “Configuring the Lotus Notes/Domino Server” on page 164
2. “Configuring the Data Protector Lotus Integration” on page 167

Configuring the Lotus Notes/Domino Server

The configuration is performed using the ‘Lotus Domino Administrator’ on the Lotus Notes/Domino Server system. The same can be achieved with ‘Web Administrator’ or by editing the `notes.ini` file directly.

To configure Lotus Notes/Domino Server, you have to enable transaction logging with archive transaction log style. No transaction logging is set as the default mode for Lotus Notes/Domino Server. There are also two transaction logging styles.

In case you select circular logging, the transaction log files are automatically overwritten, when the disk space available for transaction log files is reached. If turned on, this option reduces disk storage space requirements, but does not allow you to perform incremental backups or use the database recovery feature.

IMPORTANT

To perform incremental backups and archive log files, the transaction logging has to be set to archive logging style.

Cluster-Aware Clients

If the application is cluster-aware, enable transaction logging on all cluster nodes.

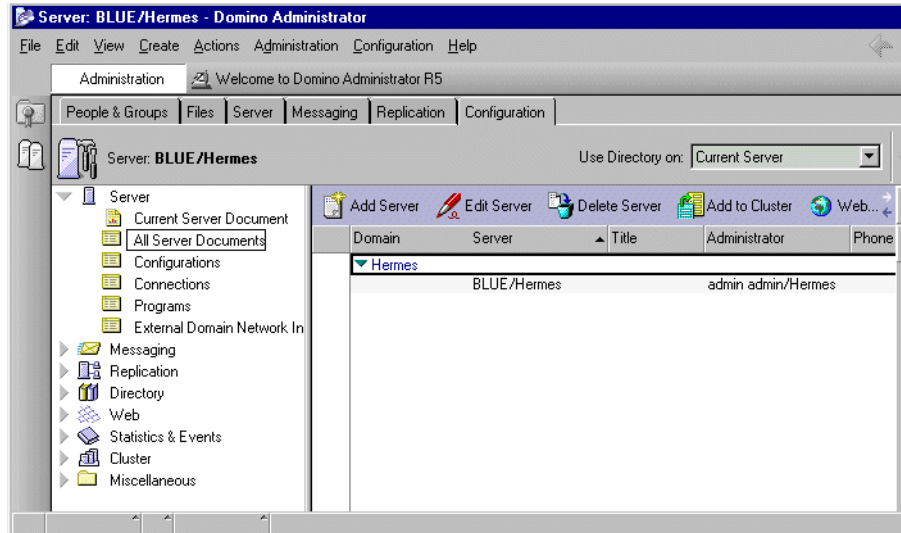
Enabling Transaction Logging

Proceed as follows to enable transaction logging and turn the circular logging style off on Domino Server.

1. Start the Lotus Domino Administrator.
2. Log on to the Domino Server, select the Configuration tab and expand Server. Move to All Server Documents and select the

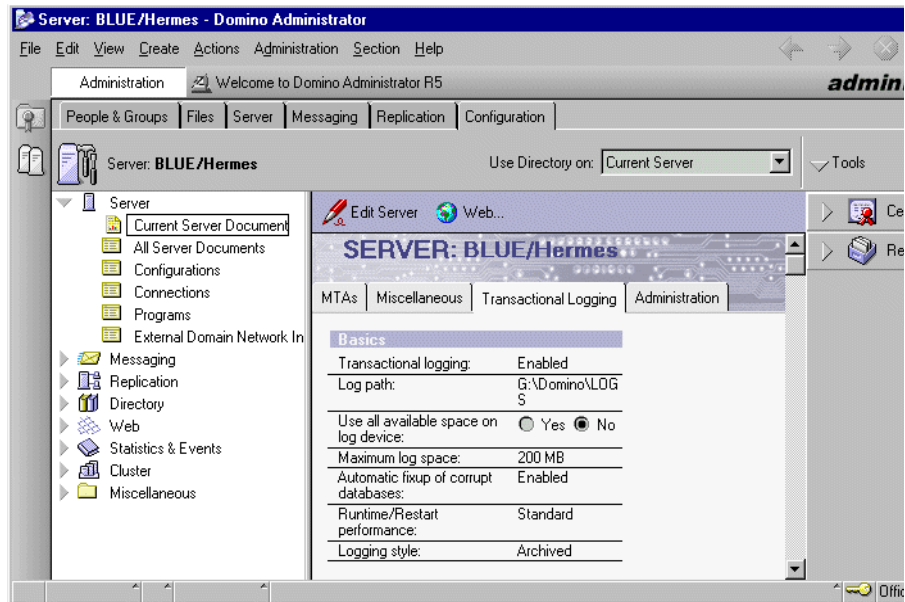
Notes/Domino Server you want to edit.

Figure 3-2 Browsing Lotus Notes/Domino Server



3. Select the Transactional Logging tab, and set appropriate values. Save the settings.

Figure 3-3 Enabling Archived Transactional Logging Style



4. Restart the server for changes to take effect.

For complete details on transactional logging, refer to Lotus/Domino documentation.

Transaction Logging (Circular Versus Archived)

Domino supports transaction logging and recovery by capturing database changes and writing them to the transaction log. If a system or media failure occurs, you can use the transaction log and a third-party backup utility to recover your databases.

Transaction logging simplifies your daily backup procedure. You can use a third-party backup utility (like the Data Protector Lotus Integration Agent) to perform daily full backups of the transaction logs, instead of full database backups.

Transaction logging only works with databases in Domino Release 5 format or later. After you enable transaction logging, all databases in Release 5 format are automatically logged.

As mentioned above there are two different logging styles when transaction logging is enabled:

- Circular logging

This is the default mode when transaction logging is enabled. The Notes/Domino Server continuously reuses the same log file, which is defined at a designated size, thus overwriting old transactions once the transaction log is filled. You are limited to restoring only the transactions stored in the transaction log. Archiving of transaction logs is not possible if circular transaction logging is used.

- Archived logging

Transaction logging is an integral part of recovering from system and media failures. As mentioned before, this is the only way to perform a backup of transaction logs. This reduces the time needed to perform a restore in case of a media or system failure.

The Notes/Domino Server does not reuse the log extents until they are backed up. The system uses the transaction logs to apply or undo database transactions not flushed to disk for databases that were open during the system failure.

A media failure may cause a database to be damaged or lost. To recover, use the Data Protector Lotus Integration Agent to restore database backups and archived transaction log files.

When transaction logging is enabled, you may see multiple S0000000.TXN files in the \log directory (you can, optionally, specify different log directory). The maximum size of each log extent (.txn file) is 64 MB. The default log space used for log extents is 192 MB. The maximum log space used for log extents is 4 GB. Domino formats at least 3 and up to 64 log files, depending on the maximum log space you allocate.

Configuring the Data Protector Lotus Integration

It is assumed that the installation of the Data Protector software components on the Lotus Notes/Domino Server was successful.

It is recommended that you configure and run a Data Protector filesystem backup of the Notes/Domino Server system. A filesystem backup can be performed only if you have installed the Disk Agent on the Notes/Domino Server system.

In case of failures, this type of backup is much easier to troubleshoot than the integration of the Notes/Domino Server with Data Protector.

Configuring the Data Protector Lotus Integration means preparing the environment for starting backup. The environment parameters (Domino Server name and path to the `notes.ini` file; on UNIX, also, path to the Lotus Notes/Domino home directory, path to Lotus Notes/Domino data directory, and path to Domino executables) are saved in the Data Protector Lotus configuration files on the Cell Manager. The configuration has to be done for each Notes/Domino Server.

Data Protector Lotus Notes/Domino Configuration Files

Data Protector stores Lotus Integration parameters in two files on the Cell Manager. These files are created during the configuration of the Lotus Notes/Domino Server with Data Protector. These files are:

- Global configuration file

This file is used to define the names of all configured Lotus Notes/Domino Servers. It is stored on the following location:

— on Windows:

```
<Data_Protector_home>\Config\server\Integ\Config\Lotus\  
<client_name>%_OB2_LOTUS
```

— on UNIX:

```
/etc/opt/omni/server/integ/config/lotus/<client_name>%  
_OB2_LOTUS
```

- Server specific configuration file

This file is used to define the absolute pathname to the `notes.ini` file; on UNIX, it also defines the pathname to the Lotus Notes/Domino home directory, Lotus Notes/Domino data directory, and Domino executables for every configured Lotus Notes/Domino client. It is stored on the following location:

— on Windows:

```
<Data_Protector_home>\Config\server\Integ\Config\Lotus\  
<client_name>%<srv_name>
```

— on UNIX:
/etc/opt/omni/server/integ/config/Lotus/<client_name>%
<srv_name>

Syntax The syntax of the global configuration file is as follows:

IMPORTANT Take extra care that the syntax of your configuration file matches the examples, to avoid problems with your backups.

```
SRV_LIST=( 'SRV_NAME1' [ , 'SRV_NAME2' , 'SRV_NAME3' ... ] );
```

Example This is an example of the global configuration file:

```
SRV_LIST=( 'RED' , 'BLUE' );
```

Syntax The syntax of the server specific configuration file is as follows:

IMPORTANT Take extra care that the syntax of your configuration file matches the examples, to avoid problems with your backups.

```
INI_FILE='<full path to notes.ini file>';
```

UNIX

```
LOTUS_HOME='<full path to Lotus home directory>';  
LOTUS_DATA='<full path to Domino data directory>';  
LOTUS_EXEC='<full path to Domino executables>';
```

This is an example of the server specific configuration file:

Windows

```
INI_FILE='d:\lotus\domino\BLUE\notes.ini';
```

UNIX

```
INI_FILE='/opt/lotus/notesdata/notes.ini';  
LOTUS_HOME='/opt/lotus/';  
LOTUS_DATA='/opt/lotus/lotusdata';  
LOTUS_EXEC='/opt/lotus/notes/latest/hppa';
```

Creating a Link to the Lotus C API Library on UNIX Systems

It is necessary to create a link to the Lotus C API library to run the Lotus Integration Agent. To create the link, follow the steps below:

1. Connect to the respective Lotus Notes/Domino Server. You must be logged in as a root user.
2. Change to the `/opt/omni/lib` directory:
`cd /opt/omni/lib` on HP-UX systems
`cd /usr/omni/lib` on other UNIX systems
3. If you have Lotus Notes/Domino Server installed on an HP-UX system, create a soft link of the `libnotes.sl` library pointing to the `<DOMINO_EXEC>/libnotes.sl` library by executing the following command:

```
ln -s <DOMINO_EXEC>/libnotes.sl libnotes.sl
```

4. If you have Lotus Notes/Domino Server installed on an AIX system, create a soft link of the `libnotes_r.a` library pointing to the `<DOMINO_EXEC>/libnotes_r.a` library by executing the following command:

```
ln -s <DOMINO_EXEC>/libnotes_r.a libnotes_r.a
```

Example of Creating Soft Links

If you are running a Lotus Notes/Domino Server on an HP-UX system, execute the following command:

```
ln -s /opt/lotus/notes/latest/hppa/libnotes.sl libnotes.sl
```

If you are running a Lotus Notes/Domino Server on an AIX system, execute the following command:

```
ln -s /opt/lotus/notes/latest/ibmpow/libnotes_r.a  
libnotes_r.a
```

Configuring a UNIX Lotus Notes/Domino Server User in Data Protector

To start a Lotus Notes/Domino backup session, you need an operating system logon for the system on which the Lotus Notes/Domino Server is running.

By default, the username is `notes` and the group is `notes`.

This user is allowed to back up or restore a Lotus Notes/Domino Server database. To start a backup of a Lotus Notes/Domino Server database using Data Protector, this user has to become the owner of the Data Protector backup specification.

IMPORTANT

Additionally, the operating system root user on the Lotus Notes/Domino Server also has to be added to either the Data Protector admin or operator user group.

After the two users are added to either the Data Protector admin or operator user group, Data Protector sessions can be started under the user account with all the privileges required to perform a Lotus Notes/Domino Server database backup with Data Protector.

Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for detailed information on Data Protector user rights and how to add a user to a user group.

Configuring the Lotus Integration Using the Data Protector GUI

The configuration is performed during the creation of a backup specification. Refer to “Creating a Backup Specification” on page 178 for instructions on how to create a backup specification.

Checking the Configuration

You can check the configuration after it has been configured or it can also be checked if you have already created and saved a backup specification for backing up a particular Domino Server:

1. In HP OpenView Storage Data Protector Manager, switch to the Backup context. In the Scoping Pane, expand Backup, Backup Specification, and then Lotus Notes.
2. In the Results Area, right-click the backup specification.
3. In the Source property page, right-click the name of the client system, then click Check Configuration.

If the configuration is successful, you will receive a message confirming that the integration was properly configured. If not, you will receive a message explaining reasons for the unsuccessful configuration.

Configuring the Lotus Integration Using the Command Line

Execute the following command to configure the Lotus Integration using the Data Protector CLI:

Syntax

- On Windows:

```
<Data_Protector_home>\bin\util_notes.exe -CONFIG  
-SERVER:<SRV_NAME> -INI:<path to the notes.ini file>
```

- On HP-UX:

```
/opt/omni/lbin/util_notes.exe -CONFIG -SERVER:<SRV_NAME>  
-INI:<path to the notes.ini file> -HOMEDIR:<path to Lotus  
home directory> -DATADIR:<path to Domino data directory>  
-EXECDIR:<path to Domino executables directory>
```

- On other UNIX:

```
/usr/omni/bin/util_notes.exe -CONFIG -SERVER:<SRV_NAME>  
-INI:<path to the notes.ini file> -HOMEDIR:<path to Lotus  
home directory> -DATADIR:<path to Domino data directory>  
-EXECDIR:<path to Domino executables directory>
```

The variables are defined as follows:

- *<path to the notes.ini file>*

Full path to the Lotus Notes/Domino Server `notes.ini` file.

- *<SRV_NAME>*

The Lotus Notes/Domino Server name. If the application is cluster-aware, *<SRV_NAME>* specifies the virtual server of Lotus Notes/Domino Server resource group.

- *<path to Lotus home directory>*

Full path to the Lotus Notes/Domino Server home directory.

- *<path to Domino data directory>*

Full path to the Lotus Notes/Domino data directory.

- *<path to Domino executables directory>*

Full path to the Lotus Notes/Domino executables.

Example In the example below, the Lotus Notes/Domino Server name is BLUE and notes.ini is located in the d:\Lotus\Domino\BLUE\notes.ini (Windows systems) or /opt/lotus/notesdata/notes.ini (UNIX systems) directory:

Windows `<Data_Protector_home>\bin\util_notes.exe -CONFIG
-SERVER:BLUE -INI:d:\Lotus\Domino\BLUE\notes.ini`

UNIX `/opt/omni/lbin/util_notes.exe -CONFIG -SERVER:BLUE
-INI:/opt/lotus/notesdata/notes.ini -HOMEDIR:/opt/lotus
-DATADIR:/opt/lotus/notesdata
-EXECDIR:/opt/lotus/notes/latest/hppa`

Checking the Configuration To check the configuration, you can run the following command on the Lotus Notes/Domino Server system:

- on Windows: `<Data_Protector_home>\bin\util_notes.exe
-CHKCONF -SERVER:BLUE`
- on HP-UX: `/opt/omni/lbin/util_notes.exe -CHKCONF
-SERVER:BLUE`
- on other UNIX: `/usr/omni/bin/util_notes.exe -CHKCONF
-SERVER:BLUE`

Data Protector will check the path to the specified directories and files.

In case of an error, the error number is displayed in the form *RETVAL*<Error_number>, otherwise *RETVAL*0 is displayed.

Testing the Integration

Once you have created and saved a backup specification, you should test it before running a backup. The test verifies both parts of the integration, the Lotus Notes/Domino Server side and the Data Protector side. The configuration is tested as well.

The procedure consists of checking the Lotus Notes/Domino Server and the Data Protector part of the integration to ensure that communication between Domino Server and Data Protector is established, such that the data transfer works properly.

Integrating Lotus Notes/Domino Server and Data Protector Configuring the Integration

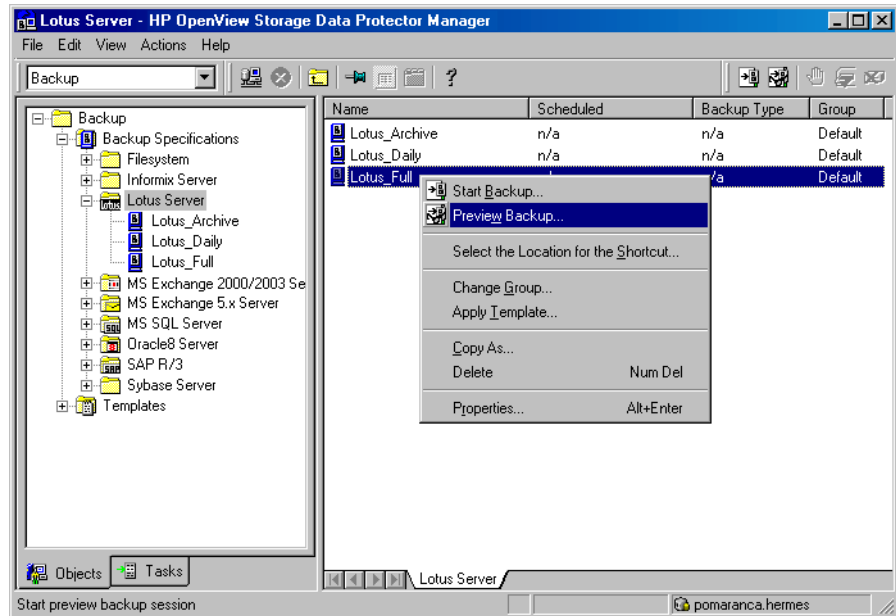
Test your backup specifications thoroughly by previewing them, then running them on file devices and then finally on the actual devices you intend to use. To test your backup specifications, you can use either the Data Protector GUI or the Data Protector CLI.

Testing Using the Data Protector GUI

Follow the procedure below to test the backup of a Lotus Notes/Domino Server backup specification:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand Backup, and then double-click Backup Specifications. Expand Lotus Server and right-click the backup specification you want to preview.
3. Click Preview Backup.

Figure 3-4 Previewing a Backup



Observe the generated messages. The “Session completed successfully” message is displayed at the end of a successful backup session of the selected backup specification.

Testing Using the Command Line

A test can be executed from the command line on the Lotus Notes/Domino Server system or on any Data Protector client system within the same Data Protector cell, provided that the system has the Data Protector User Interface installed.

Execute the following command:

- On Windows:

```
<Data_Protector_home>\bin\omnib -lotus_list  
<backup_specification_name> -test_bar
```

- On HP-UX:

```
/opt/omni/bin/omnib -lotus_list  
<backup_specification_name> -test_bar
```

- On other UNIX:

```
/usr/omni/bin/omnib -lotus_list  
<backup_specification_name> -test_bar
```

What Happens?

The given procedure performs a backup preview that tests:

- Communication between the Lotus Notes/Domino Server and Data Protector.
- The syntax of the Lotus Notes/Domino backup specification.
- If used devices are correctly specified.
- If the needed media are in the devices.

The command tests only the Data Protector part of the configuration.

Backing Up Lotus Notes/Domino Server

Before You Begin Before performing a backup of Lotus Notes/Domino Server, make sure that archive transaction logging is enabled. Refer the *HP OpenView Storage Data Protector Software Release Notes* or http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, devices, limitations, and other information.

What to Back Up The Lotus Integration Agent provides functions for backing up and restoring Notes data in the Lotus Notes/Domino Server data directory.

Lotus Notes/Domino Server databases consist of the following files:

- NSF (Notes Storage Facility) files.
- NTF (Notes Template Facility) files.
These files are templates for creating new NSF databases.
- BOX files.
The mail router uses these files.
- Transaction log files, named SXXXXXXX.TXN, where XXXXXXXX is a 7 digit number that is automatically incremented for every new transaction file (the maximum size of this file is 64 MB).

When the online backup and database are under transaction log, Lotus Integration Agent backs up transactions made during a backup. The Agent saves the changed information to a newly created file `<db_name>.CI`. This file is also backed up and after the backup is complete, it is deleted. During a restore, the Agent applies all the changed information from the `.CI` file to restored database. Following this, the recovery is performed.

Backup functions use the log files to perform archive backups. Lotus Notes/Domino Server automatically recycles archived transaction logs after backup.

IMPORTANT

It is important that archived transaction log files are backed up often enough, so that log files do not exceed the defined amount of disk space.

Domino Templates (NTF)

NTF files (Domino templates) are templates for creating new NSF databases which, in contrast with NSF files, never change. To speed up a full Lotus Notes/Domino Server backup, it is recommended to create a separate backup specification for NTF files and back them up. When you create a backup specification for a full Lotus Notes/Domino Server backup, add NTF files to the private exclusion list to exclude them from the full backup. For more information on exclusion lists, refer to the *HP OpenView Storage Data Protector Administrator's Guide*. Note that NTF files are not backed up during the incremental backup because they do not change.

The Lotus Integration Agent is the Data Protector software component that backs up and restores Lotus Notes/Domino databases, Domino templates, and transaction logs. Besides the Notes/Domino databases and archived transaction log files (Notes data) there are a lot of non-database files which need to be backed up to provide a complete data protection solution for a Notes/Domino Server. Domino non-database data include:

- notes.ini
- desktop.dsk
- All *.id files

You can back up this data using the Data Protector filesystem backup solutions. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for detailed information.

Configuring a Lotus Notes/Domino Server Backup

To configure a Lotus Notes/Domino Server backup, perform the following steps:

1. Configure the devices you plan to use for the backup. See the *HP OpenView Storage Data Protector Administrator's Guide* or online Help for instructions.
2. Configure media pools and media for the backup. See the *HP*

OpenView Storage Data Protector Administrator's Guide or online Help for instructions.

3. Create a Lotus Notes/Domino Server backup specification, specifying what to back up, which devices to use, and how to back it up.

Refer to the following section for the procedure for creating a backup specification.

Creating a Backup Specification

All Lotus Notes/Domino Server backup specifications are collected under "Lotus Server" in the Scoping Pane.

To create a Lotus Notes/Domino Server backup specification, proceed as follows:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand Backup, and then double-click Backup Specifications.
3. In the Results Area, right-click Lotus Server and then click Add Backup. The Create New Backup dialog box is displayed.
4. Select the Blank Lotus Notes Backup template, and then click OK to start a backup wizard.
5. In the Client drop-down list, select the Lotus Notes/Domino Server system. If the application is cluster-aware, select the virtual server of Lotus Notes/Domino Server resource group.

In the Application database drop-down list, select the name of the Lotus Notes/Domino Server that you want to back up. If the Lotus Notes/Domino Server has not yet been configured, type the name of the Notes/Domino Server manually.

On UNIX, also enter the name of the user who is the owner of the backup and the name of the user group. This was configured during the installation of the application.

Click Next.

Figure 3-5 Specifying a Client Name and Selecting an Application Database on Windows

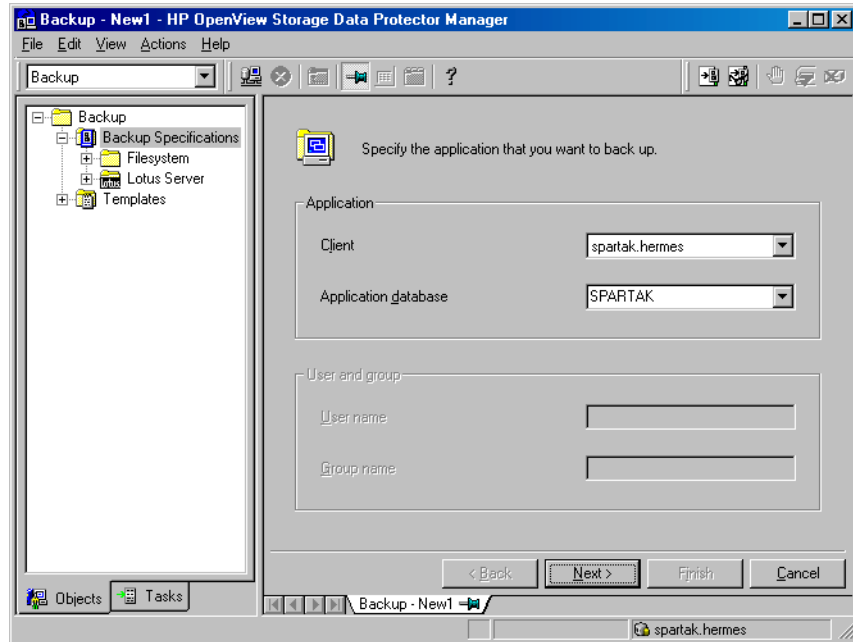
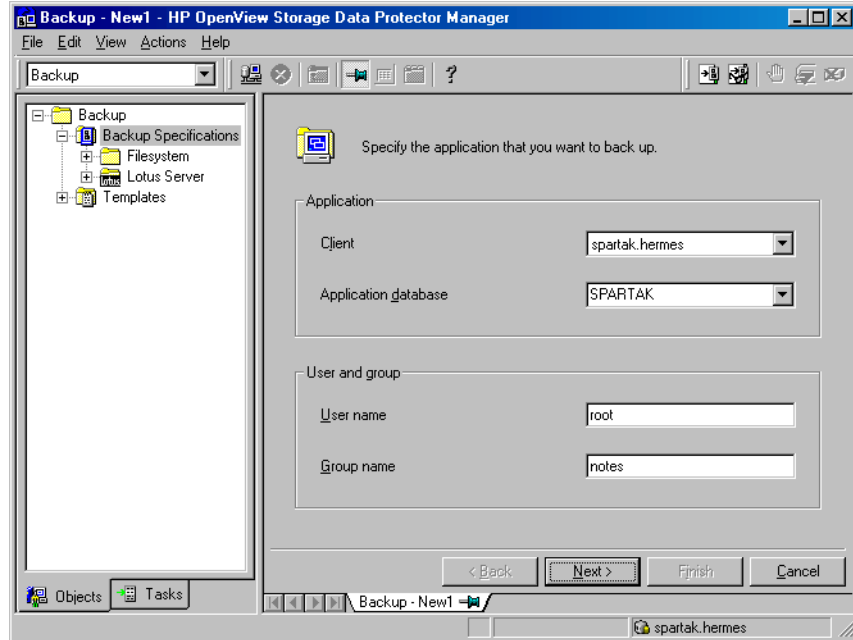


Figure 3-6 Specifying a Client Name and Selecting an Application Database on UNIX



6. If you are configuring the Lotus Integration for the specified Notes/Domino Server for the first time, a window Configure Lotus Notes is displayed.

Specify the full pathname to the `notes.ini` file located on the Lotus Notes/Domino client system.

On UNIX, specify also the full pathname to the Lotus Notes/Domino home directory, Lotus Notes/Domino data directory and Lotus Notes/Domino executables directory.

Click Next.

Figure 3-7 Specifying the Pathname to the Notes.ini File on Windows

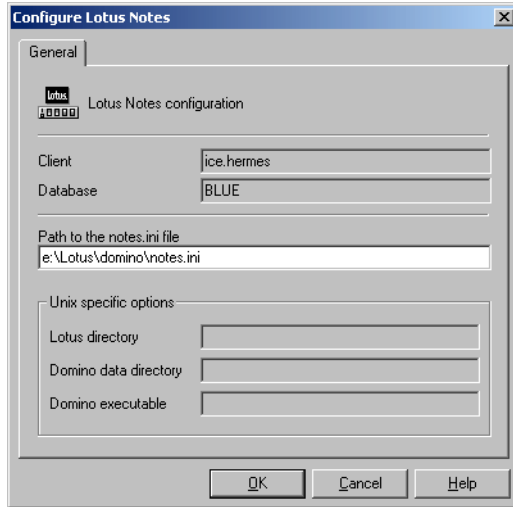
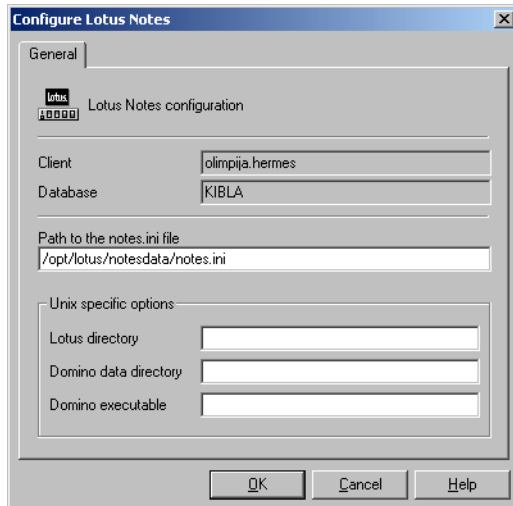
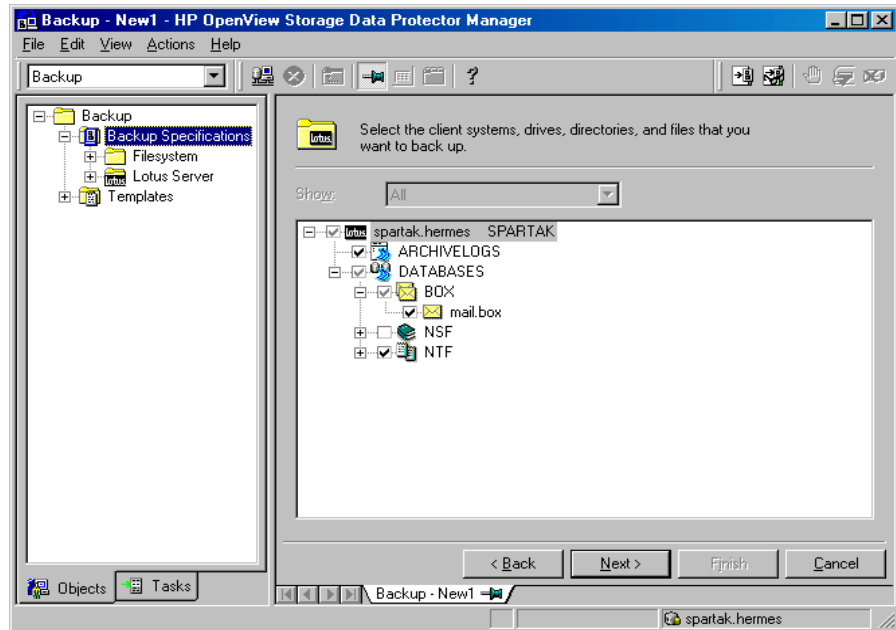


Figure 3-8 Specifying the Pathname to the Notes.ini File on UNIX



7. Select the Lotus Notes/Domino Server objects you want to back up. Click Next.

Figure 3-9 **Selecting Objects for a Backup**

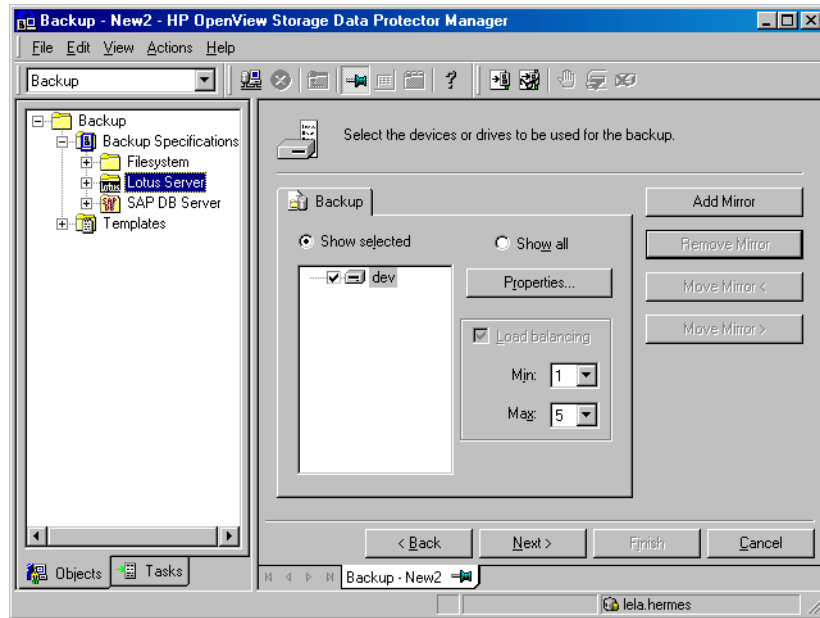


8. Select the device(s) you want to use for the backup. Click *Properties* to set the device concurrency, media pool, and preallocation policy. For more information on these options, click *Help*.

You can also specify whether you want to create additional copies (mirrors) of the backup during the backup session. Specify the desired number of mirrors by clicking the *Add mirror* and *Remove mirror* buttons. Select separate devices for the backup and for each mirror.

For detailed information on the object mirror functionality, see the *HP OpenView Storage Data Protector Administrator's Guide*.

Figure 3-10 **Selecting Backup Devices**



9. Click Next to select backup options and to schedule your backup.

Refer to online Help or the *HP OpenView Storage Data Protector Administrator's Guide* for details about options common to all Data Protector backup specifications.

Refer to “Lotus Notes/Domino Server Specific Backup Options” on page 183 for details about Lotus Notes/Domino Server specific options.

10. Once you have defined all backup options and optionally scheduled the backup, name and save the newly created backup specification.

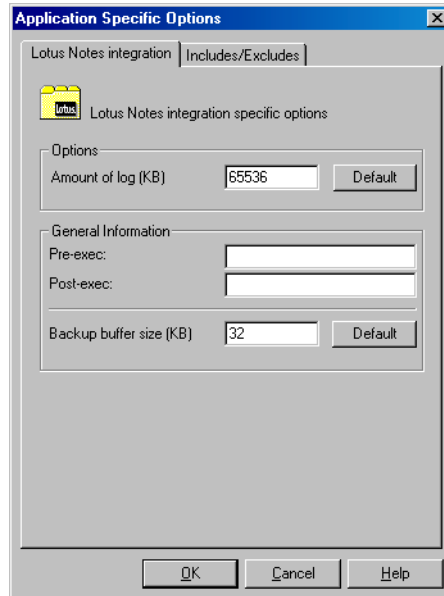
Once saved, the backup specification can be tested by clicking Start Preview, or started by clicking Start Backup.

Lotus Notes/Domino Server Specific Backup Options

This section describes backup options specific to the Data Protector Lotus Integration.

You can access these options in the Options property page of a backup specification. Click the Advanced button next to the Application Specific Options. Refer to “Application Specific Options” on page 184.

Figure 3-11 Application Specific Options



The following options can be selected from this window:

Amount of log Defines the size of the amount of log needed for the database recovery. If the database has less amount of log than specified, the incremental backup skips the database. If the database exceeds the specified amount of log, the full backup of the database is performed.

Pre-exec Specifies a command with arguments or a script that will be started on the Lotus Notes/Domino Server client before the backup starts. The command/script is started by Data Protector `ldbar.exe` and has to reside in the `<Data_Protector_home>/bin` (Windows systems), `/opt/omni/bin` (HP-UX systems), or `/usr/omni/bin` (other UNIX systems) directory. Only the filename must be provided in the backup specification.

Post-exec Specifies a command with arguments or a script that will be started on the Lotus Notes/Domino Server client after the backup. The command/script is started by Data Protector `ldbar.exe` and has to reside in the `<Data_Protector_home>\bin` (Windows systems), `/opt/omni/bin` (HP-UX systems), or `/usr/omni/bin` (other UNIX systems) directory. Only the filename must be provided in the backup specification.

Backup buffer size This is the size of the Lotus Integration buffer which is used to transfer data to Data Protector.

The application specific options are applied to all backup objects that have been selected in the backup specification.

Running an Online Backup

To run an online backup of a Lotus Notes/Domino Server object, use any of the following methods:

- Schedule the backup of an existing Lotus Notes/Domino Server backup specification using the Data Protector Scheduler.
- Start an interactive backup using the Data Protector GUI.

Scheduling a Backup

For more detailed information on scheduling, refer to the online Help index keyword “scheduled backups”.

Scheduling a backup specification means setting the time, date, and type of a backup that starts unattended once the scheduling options are defined and saved in the backup specification.

A backup schedule can be tailored according to your business needs. If you have to keep the databases online continuously, then you should back it up frequently, including the backup of the archived transaction logs, which are required in case you need a recovery to a particular point in time.

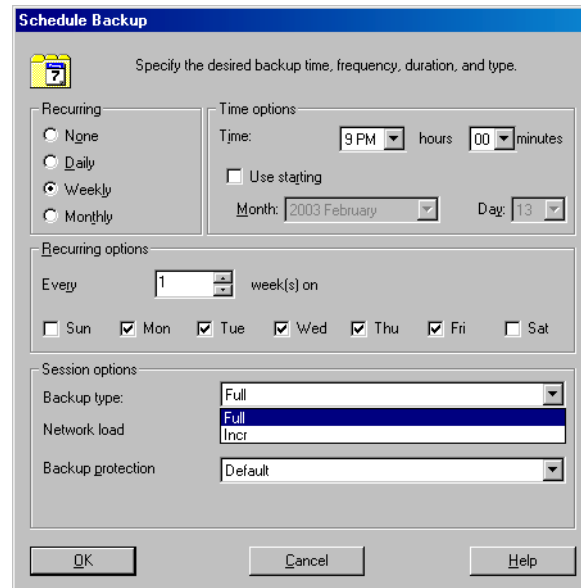
To schedule a Lotus Notes/Domino Server backup specification, perform the following steps:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.

2. In the Scoping Pane, expand Backup, then Backup Specifications. Click Lotus Server.
A list of backup specifications is displayed in the Results Area.
3. Double-click the backup specification you want to schedule and click the Schedule tab to open the Schedule property page.
4. In the Schedule property page, select a date in the calendar and click Add to open the Schedule Backup dialog box.
5. Specify Recurring, Time options, Recurring options, and Session options. See Figure 3-12 on page 186.
6. Click OK to return to the Schedule property page.
7. Click Apply to save the changes.

Figure 3-12

Scheduling Backups



Starting an Interactive Backup

An interactive backup can be performed any time after the backup specification has been created and saved.

To start an interactive backup of a Lotus Notes/Domino Server backup object, perform the following steps:

1. In the HP OpenView Storage Data Protector Manager, switch to the Backup context.
2. In the Scoping Pane, expand the Backup, and then the Backup Specifications items.

Expand Lotus Server. A list of backup specifications appears.

3. Right-click the backup specification you want to back up, and then select Start Backup from the pop-up menu.

The Start Backup dialog box appears.

Select the backup type and network load.

Refer to online Help for a description of network load.

4. Click OK.

Messages appear in the Results Area as the backup session proceeds. Upon successful completion of the backup session, the Session completed successfully message is displayed.

Restoring Lotus Notes/Domino Server Data

You can restore Lotus Notes/Domino Server objects using the Data Protector GUI.

Databases are restored directly to the host with the installed Notes/Domino Server using `ldbar.exe`. Through the Lotus Integration Agent you are able to bring database offline, put the databases online, and put perform database recoveries after restores. In the case that you perform a recovery, transaction logs are also restored if needed. This step (restoring archive logs) is performed automatically during the recovery process.

Database restore can be done while the server is online. You can specify the restore location. So you can restore the database to the same location as it was backed up from (so in case the database is corrupted or deleted you can replace it) or you can restore the database to a location other than the original and you keep the original database intact.

After restore of the Notes/Domino database, the database is not active. If you access it, it will be automatically brought online. But in this case the recovery is not performed. In most cases you would like to get the last possible consistent state of the databases or to do recovers to a specific point in time. In this situation you must use the recover option.

IMPORTANT

If restore location resides the database with the same file name as restored one, then this database is taken offline and deleted.

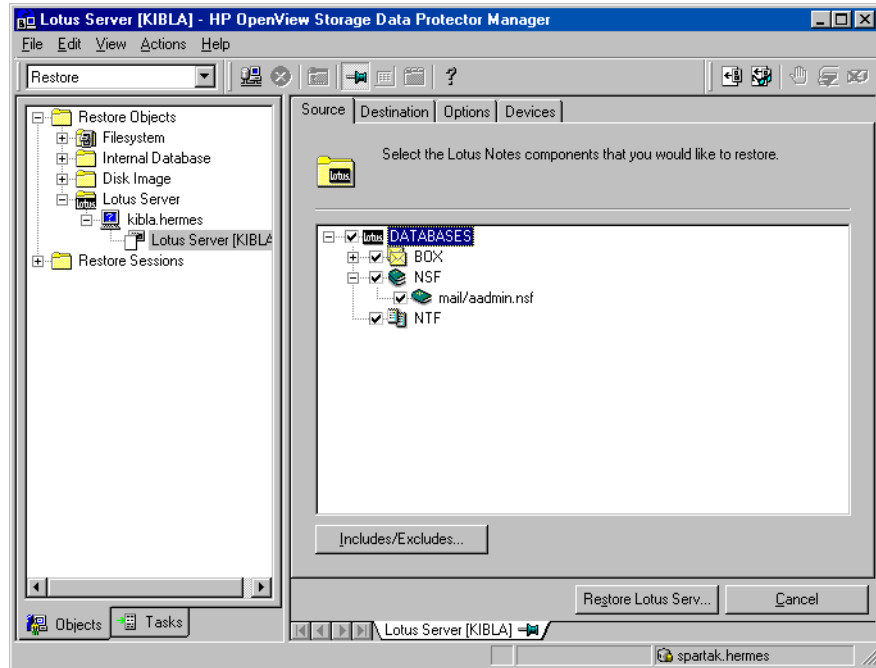
Restore Procedure

Use the following procedure to restore the Lotus Notes/Domino Server objects:

1. In HP OpenView Storage Data Protector Manager, switch to the Restore context.
2. In the Scoping Pane, expand Lotus Server and then the name of the client system from which you want to restore.

3. Browse for and select the backed up Lotus Notes/Domino Server objects you want to restore.

Figure 3-13 Restore Objects



Backup version can be selected in the Options property page. Click Browse to select a different version of backup.

NOTE

In the source property page all the backed up databases are listed. If you are restoring multiple databases from a specific backup session, ensure that the databases selected for restore were backed up in the selected backup session. If this criteria is not met, a warning 'object not found in the database' appears at the restore time. Restoring from different backup sessions demands separate restore sessions. The only exception

Integrating Lotus Notes/Domino Server and Data Protector
Restoring Lotus Notes/Domino Server Data

is when the backup session is not specified. In such cases, the Lotus Integration Agent finds the latest backup version of each database for restore.

Figure 3-14 Selecting Restore Options on Windows

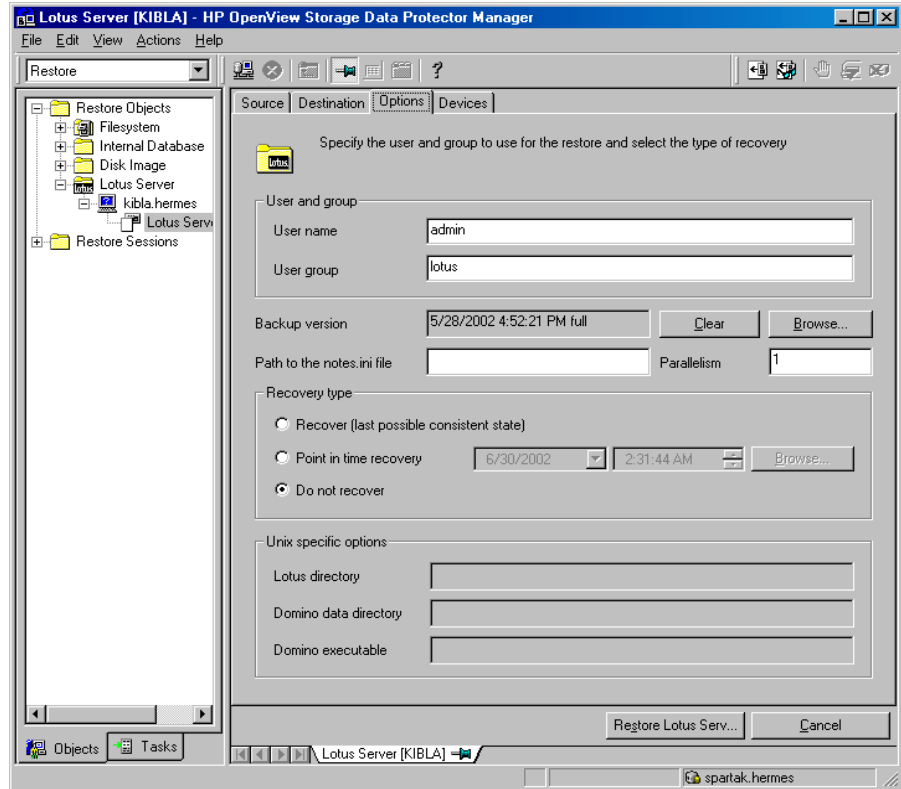
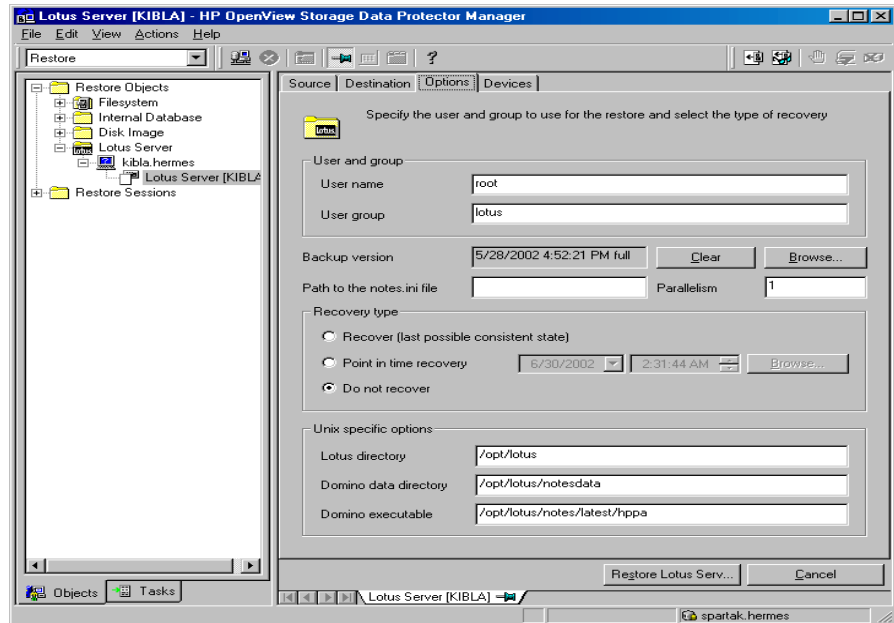


Figure 3-15 Selecting Restore Options on UNIX



4. Select the restore options from the Options property page. Refer to “Restore Options” on page 193.

The devices and media for restore are automatically selected.

Note that you can change the device used for the restore. Therefore, you have the possibility of using a different device for a restore than the one that was used for the backup. Refer to the “Restoring Under Another Device” section of the *HP OpenView Storage Data Protector Administrator’s Guide* for more information on how to perform a restore using another device.

5. Click Restore Lotus Server. Review your selection, and then click Finish to start a restore session.

The restore session messages are displayed in the Results Area.

Restore Options

The following destination and restore options are specific to the Data Protector Lotus Integration.

Destination Options

Destination options are the following:

- Target client

By default, the target Data Protector Lotus client is the Lotus Notes/Domino Server from which the application data was backed up. If the target client is a Windows system, then UNIX specific options are disabled. If the target client is a UNIX system, manually enter the Lotus Notes/Domino home directory, Lotus Notes/Domino data directory, and the Lotus Notes/Domino executables directory. The new target Lotus Notes/Domino Server must be a part of the Data Protector cell and have the Lotus Integration software component installed.

Nevertheless, the databases can be restored to a Lotus Notes/Domino Server other than the one the backup was made from. The new target Lotus Notes/Domino Server must be a part of the Data Protector cell and have the Lotus Integration software component installed.

- Restore Location

- ✓ Restore to original location

This is the default option. You can restore the databases to the same directory from which it was backed up (it can be on the original client system or on some other client system which you selected).

- ✓ Restore to new location

This option enables you to restore your data to another directory. When defining the restore location you can specify the relative directory to the Notes/Domino data directory where you want to restore your data.

Example

Lotus Notes/Domino data directory is located in
C:\Lotus\Domino\BLUE\ (Windows systems) or
/opt/lotus/notesdata/BLUE (UNIX systems).

To restore a database to the `C:\Lotus\Domino\BLUE\restore_dir\` (Windows systems) or `/opt/lotus/notesdata/BLUE/restore_dir/` directory, specify the `restore_dir` directory. The restored database filenames are the same as they were at backup time.

Restore Options

You can specify the following restore options:

- User and group

Enter the Lotus Notes/Domino user name and group, for example, "notes", "notes".

- Backup version

By default, a restore is done from the last full backup of a database. Click the `Browse` button to define a backup version other than the last one.

- Path to the `notes.ini` file

Specify the full path to the Lotus Notes/Domino Server `notes.ini` file.

- Parallelism

Specify how many Lotus Integration Agents will start the restore. By default, this value is set to 1.

- Recovery type

— Recover (last possible consistent state)

This is the default option. Select this option to restore the database to the last possible consistent state. This also includes restore of archived transaction logs if needed during recovery.

— Point in time recovery

You can specify a point in time to which the database state should be restored. Click `Browse` to specify the desired date and time for the point in time recovery. In this case, only transactions written before the specified date and time are applied to the database.

— Do not recover

Restoring Lotus Notes/Domino Server Data

If this option is selected, the restore of the specified database is performed from the last backup or from the specified backup version. This option only restores databases without trying to recover the database. Any transactions made during or after backup are not reflected in the restored database.

- UNIX specific options

These options are only enabled if the target system is a UNIX system. To perform a restore, the following options must be specified:

- Lotus directory

Specify the full path to the Lotus Notes/Domino Server home directory.

- Lotus Notes/Domino data directory

Specify the full path to the Lotus Notes/Domino data directory.

- Domino executables

Specify the full path to the Lotus Notes/Domino executables.

Monitoring a Lotus Notes/Domino Server Backup and Restore

The Data Protector GUI enables you to monitor current or previous backup and restore sessions. Note that you must have the appropriate privileges to view previous sessions.

Monitoring is automatically activated when you start a restore or backup.

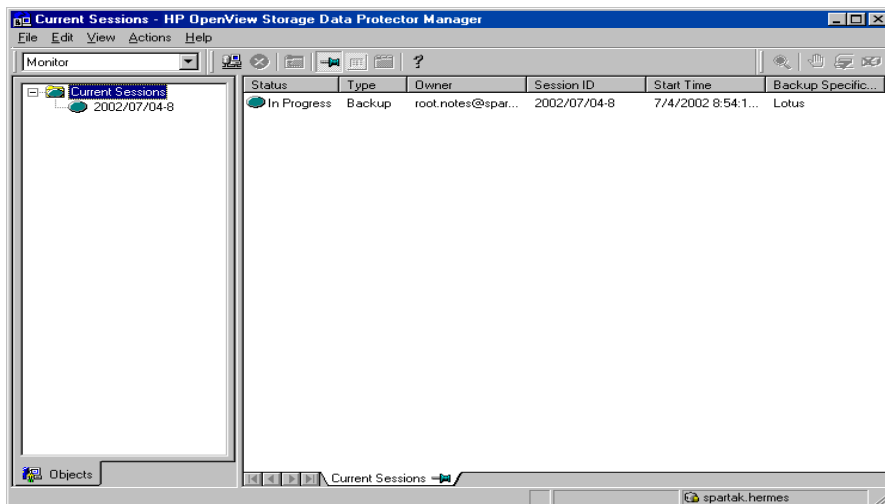
Monitoring Current Sessions

To monitor a currently running session using the Data Protector GUI, proceed as follows:

1. In the Context List, click Monitor.
In the Results Area, all currently running sessions are listed. See Figure 3-16.
2. Double-click the session you want to monitor.

Figure 3-16

Monitoring Current Sessions



Clearing Sessions To remove all completed or aborted sessions from the Results Area of the Monitor context, proceed as follows:

1. In the Scoping Pane, click `Current Sessions`.
2. In the Actions menu, select `Clear Sessions`. Or click the `Clear Sessions` icon on the toolbar.

To remove a particular completed or aborted session from the current sessions list, right-click the session and select `Remove From List`.

NOTE

All completed or aborted sessions are automatically removed from the Results Area of the Monitor context if you restart the Data Protector GUI.

For detailed information on a completed or aborted session, see “Viewing Previous Sessions”.

Viewing Previous Sessions

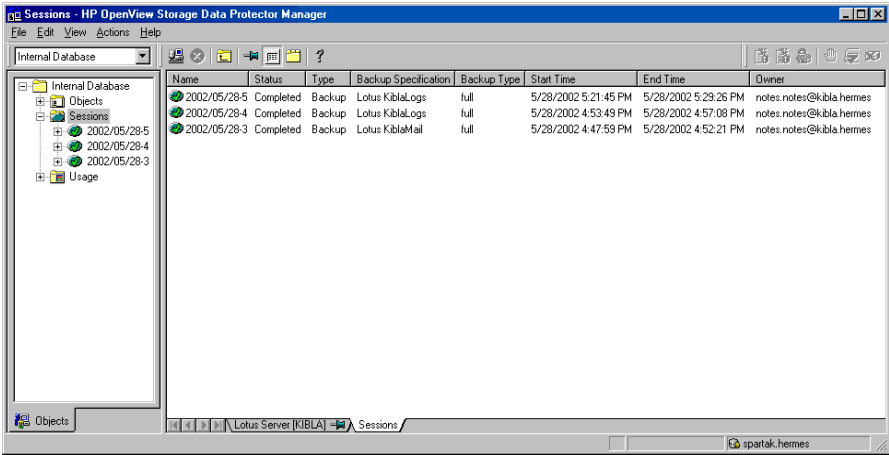
To view a previous session using the Data Protector GUI, proceed as follows:

1. In the Context List, click `Internal Database`.
2. In the Scoping Pane, expand `Sessions` to display all the sessions stored in the IDB.

The sessions are sorted by date. Each session is identified by a session ID consisting of a date in the YY/MM/DD format and a unique number.

3. Right-click the session and select `Properties` to view details on the session.
4. Click the `General`, `Messages` or `Media` tab to display general information on the session, session messages, or information on the media used for this session, respectively. See Figure 3-17.

Figure 3-17 Viewing Previous Sessions



Troubleshooting

This section is divided into the following subsections:

- General troubleshooting
- Checking prerequisites related to the Lotus Notes/Domino Server side of the integration
- Configuration problems
- Backup problems
- Restore problems
- Recovery problems

General Troubleshooting

1. Ensure that the latest official Data Protector patches are installed. Refer to “Verifying Which Data Protector Patches Are Installed” in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Refer to the *HP OpenView Storage Data Protector Software Release Notes* or

http://www.openview.hp.com/products/datapro/spec_0001.html for an up-to-date list of supported versions, platforms, and other information.

2. Refer to the *HP OpenView Storage Data Protector Software Release Notes* for a description of general Data Protector limitations, problems and workarounds, as well as the list of related Data Protector patches.

The following sections provide some checking procedures you should perform before you call Data Protector support. In this way you may either resolve the problem yourself or identify the area where the difficulties are occurring.

Follow the given procedures to troubleshoot your configuration, backup or restore problems.

Checking Prerequisites Related to the Lotus Notes/Domino Server Side of the Integration

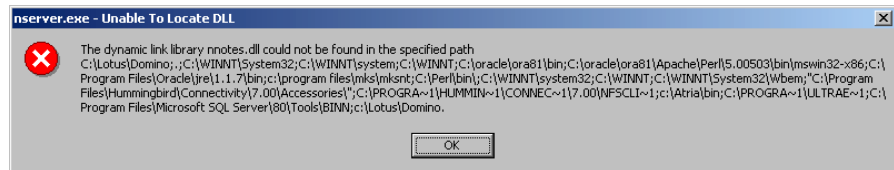
For more detailed information about how to perform any of the following procedures, refer to the Lotus Notes/Domino Server documentation.

Windows

1. Check if the nNotes.dll library is linked.

If the nNotes.dll is not linked, you can experience the following error:

Figure 3-18 Unable to Locate the nNotes.dll Library



2. Check if the nNotes.dll library is in the environment path.

If the nNotes.dll library is not in the environment path, add it. The nNotes.dll is located in the <Lotus_home>\domino directory by default.

UNIX

1. Check the environment variables.

Prior to any Lotus C API call from Data Protector Lotus Integration Agent, the Lotus C API has to be initialized. To successfully initialize it, the following environment variables must be set:

```
LOTUS=/opt/lotus
```

```
NOTES_DATA_DIR=/local/notesdata
```

```
Notes_ExecDirectory=<Lotus_home>/notes/latest/ibmpow
```

```
PATH=$PATH:$LOTUS:$NOTES_DATA_DIR:$Notes_ExecDirectory:/opt/lotus/bin
```

```
PATH=$PATH:$Notes_ExecDirectory/res/C
```

These variables are usually exported by Lotus Integration Agent or utility prior to Lotus Notes C API initialization. If you experience problems with Lotus C API initialization, please try to export these

variables manually or put them in `.omnirc` file. For more information on how to use `.omnirc` file, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

2. Check if the soft link to the Lotus Notes/Domino `libnotes` library exists.

If the soft link to the `libnotes` library does not exist, you can experience the following error while running Lotus Notes utility from the command line:

```
#!/util_notes.exe
/usr/lib/dld.sl: Can't find path for shared library:
libnotes.sl
/usr/lib/dld.sl: No such file or directory
Abort (coredump)
```

Check if the soft link from `/opt/omni/lib/libnotes.sl` (HP-UX systems) or `/usr/omni/lib/libnotes_r.a` (AIX systems) to the Lotus Notes/Domino `libnotes` library exists. The name of the link must be the same as `libnotes` library name in the Lotus Notes/Domino Exec directory.

NOTE

The soft link must be checked on all Lotus Notes/Domino clients that you have in your cell.

Example

- On HP-UX systems, the following link must exist in the `/opt/omni/lib` directory:

```
libnotes.sl ->
/opt/lotus/notes/latest/hppa/libnotes.sl
```

- On AIX systems, the following link must exist in the `/usr/omni/lib` directory:

```
libnotes_r.a ->
/opt/lotus/notes/latesst/ibmpow/libnotes_r.a
```

After setting the soft link, check if the soft link works:

- On HP-UX system, run:

```
/opt/omni/lbin/util_notes.exe -app
```

If the following output is displayed, the libnotes library is not linked properly. Please check the link again.

```
/usr/lib/dld.sl: Can't find path for shared library:  
libnotes.sl
```

```
/usr/lib/dld.sl: No such file or directory
```

If the soft link is set correctly, the *RETVAL*0 message is displayed.

- On AIX system, run:

```
/usr/omni/bin/util_notes.exe -app
```

If the following output is displayed, the libnotes library is not linked properly. Please check the link again.

```
exec():0509-036 Cannot load program ./util_notes.exe  
because of the following errors:
```

```
0509-022 Cannot load library libnotes_r.a
```

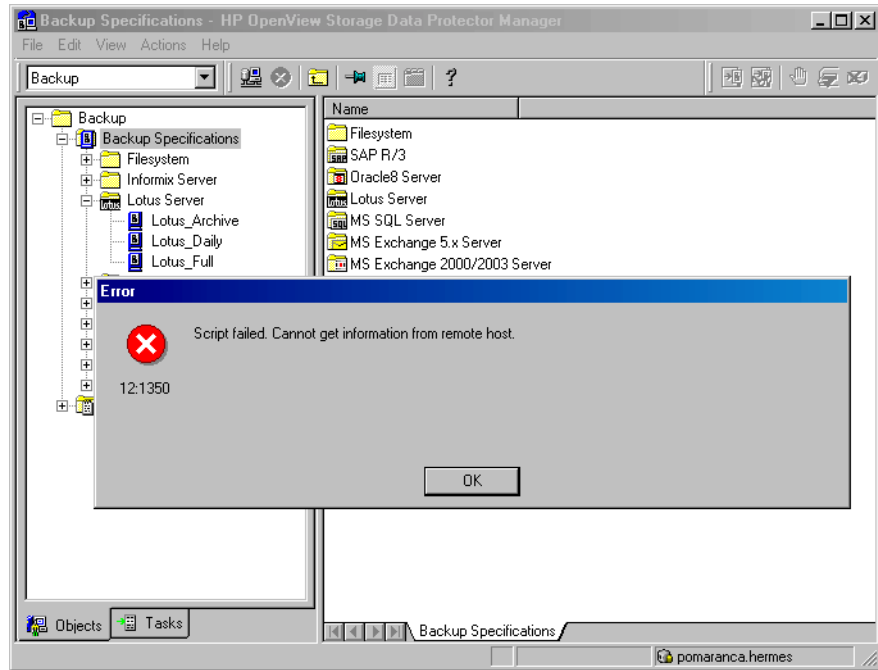
```
0509-026 System error: A file or directory in the path  
does not exist.
```

If the soft link is set correctly, the *RETVAL*0 message is displayed.

3. Script failed error.

You can get the following error message while configuring or starting a backup using the Data Protector GUI

Figure 3-19 Script Failed Error



To solve this problem, see the procedure described in “Checking Prerequisites Related to the Lotus Notes/Domino Server Side of the Integration” on page 199.

Configuration Problems

IMPORTANT

If you have encountered any errors up to this point when performing procedures described in the previous section, refer to Lotus Notes/Domino Server support. The respective tests have to be done before you even start checking the Data Protector Lotus Notes/Domino Server configuration.

1. **Verify that the Data Protector software has been installed properly.**

Refer to “Verifying Data Protector Client Installation” in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for details.

2. **On Windows, verify the inet startup parameters.**

Check the Data Protector Inet service startup parameters on the Lotus Notes/Domino Server system. Proceed as follows:

- a. In the Control Panel, go to Administrative Tools, Services.
- b. In the Services window, select Data Protector Inet, Startup.
- c. The service has to run under a specified user account. Make sure that the same user is also added to the Data Protector admin user group.

Figure 3-20 Checking the Inet Start-Up Parameters



3. Check the Windows Registry Entry for the Data Protector Cell Manager.

To check if the Cell Manager is correctly set on the Lotus Notes/Domino Server system, check the Windows registry entry:

```
\HKEY_LOCAL_MACHINE\Software\Hewlett-Packard\OpenView\OmniBack II\Site
```

4. Check the omnirc environment settings.

Examine the environment settings in the omnirc file, which is located in the `<Data_Protector_home>` (Windows systems) or `/opt/omni` (UNIX systems) directory.

Backup Problems

At this stage, you should have performed all the verification steps described in the previous sections. After this, proceed as follows:

1. Check your Lotus Notes/Domino Server configuration.

Windows

On the Lotus Notes/Domino Server system, run the following command:

```
<Data_Protector_home>\bin\util_notes.exe -CHKCONF  
-SERVER:<SRV_NAME>
```

*RETVAL*0 indicates a successful configuration.

UNIX

Login as a Lotus Notes/Domino group dba user to the Lotus Notes/Domino Server system and run the following command:

```
/opt/omni/lbin/util_notes.exe -CHKCONF -SERVER:<SRV_NAME>
```

In case of an error, the error number is displayed in the form *RETVAL*`<Error_number>`.

To get the error description, run the following command:

```
/opt/omni/lbin/omnigetmsg <set_number> <Error_number>
```

*RETVAL*0 indicates a successful configuration.

2. Perform a filesystem backup of the Lotus Notes/Domino Server system.

Perform a filesystem backup of the Lotus Notes/Domino Server system so that you can eliminate the chance of any potential communication problems between the Lotus Notes/Domino and the Data Protector Cell Manager system.

Do not start troubleshooting an online database backup unless you have successfully completed a filesystem backup of the Lotus Notes/Domino Server system.

Refer to online Help or the *HP OpenView Storage Data Protector Administrator's Guide* for details about how to do a filesystem backup.

If the Lotus Notes/Domino Server part of the filesystem backup fails, examine the system errors reported in the `<Data_Protector_home>\log\debug.log` (Windows systems) or `/var/opt/omni/log/debug.log` (UNIX systems) file, which is located on the Data Protector Lotus Notes/Domino client system. Try to restart the Lotus Notes/Domino Server and observe the server messages.

If the Data Protector part of the filesystem backup fails, examine the system errors reported in the `<Data_Protector_home>\log\debug.log` (Windows system) or `/var/opt/omni/log/debug.log` (UNIX system) file, which is located on the Data Protector Cell Manager system.

If the filesystem backup succeeds, the problem is probably insufficient memory, disk space or other OS resource of the client running the Data Protector User Interface.

3. Verify Data Protector internal data transfer using the testbar utility.

- a. Verify that the Cell Manager name is correctly defined on the Lotus Notes/Domino Server system. Check the `<Data_Protector_home>\Config\client\cell_server` (Windows systems), `/etc/opt/omni/client/cell_server` (HP-UX systems), or `/usr/omni/config/cell/cell_server` (other UNIX systems) file, which contains the name of the Cell Manager system.
- b. On Windows, restart the `OmniInet` service as an administrator.

- c. Run the following command:
 - On Windows:

```
<Data_Protector_home>\bin\testbar -type:Lotus  
-appname:<SRV_NAME> -bar:<backup_specification_name>  
-perform:backup
```
 - On HP-UX:

```
/opt/omni/bin/utilns/testbar -type:Lotus  
-appname:<SRV_NAME> -bar:<backup_specification_name>  
-perform:backup
```
 - On other UNIX:

```
/usr/omni/bin/utilns/testbar -type:Lotus  
-appname:<SRV_NAME> -bar:<backup_specification_name>  
-perform:backup
```
 - d. In the HP OpenView Storage Data Protector Manager, switch to the Monitor context, and examine the errors reported by the testbar utility by clicking the Details button.
 - e. Create an Lotus Notes/Domino Server backup specification to back up to the null device or file. If the backup succeeds, the problem may be related to the backup devices. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for instructions on troubleshooting devices.
4. **Start a backup session using ldbar.exe .**

You can start a test backup session using the Data Protector command line interface, where the backup options have to be specified as the ldbar.exe command line options.

Run the following command from the

<Data_Protector_home>\bin (Windows system) or
/opt/omni/bin (UNIX system) directory on a Data Protector Lotus client system:

- On Windows:

```
ldbarm.exe -perform:backup -db:<DB_NAME> -server:<SRV_NAME>  
-ini:<path to notes.ini file>  
-bar:<backup_specification_name>
```

- On UNIX:

```
ldbar.exe -perform:backup -db:<DB_NAME> -server:<SRV_NAME>  
-ini:<path to notes.ini file>  
-bar:<backup_specification_name> -homedir:<path to Lotus  
home> -datadir:<path to Domino data> -execdir:<path to Domino  
executables>
```

For other `ldbar.exe` parameters, refer to the command help by running `ldbar.exe -help`.

NOTE

The `-bar` option is mandatory since the `ldbar.exe` reads the device options from the backup specification as opposed to other options in the respective backup specification, which are ignored. The command line options are used instead.

5. If the Lotus Notes/Domino Server freezes during backup.

During the backup session, it can happen that Lotus Notes/Domino Server freezes with the following error:

```
Fatal Error signal = 0x0000000b PID/TID = xxxx/l  
Freezing all server threads ...
```

This can happen in the following cases:

- The Lotus Notes C API initialization failed and caused the server to freeze.

In this case, kill the `ldbar.exe` processes when following the recovering procedure below.

- On UNIX, if the Lotus Notes/Domino Server is not online and the Lotus Notes/Domino daemon `logasio` is not running, then while the Lotus Integration Agent is initializing Lotus C API, the `logasio` daemon automatically starts. Since the environment for `notes` user is not set because the `.profile` is not executed, the `logasio` server could fail to start.

In this case, kill the `logasio` processes when following the recovering procedure below.

Proceed as follows:

- a. On UNIX, log into the Lotus Notes/Domino client system as a root user.

- b. On Windows, kill all the `ldbar.exe` processes using Task Manager.
- c. On UNIX, kill all the either `ldbar.exe` or `logasio` processes:

```
ps -ef | grep <processes_name> | grep -v 'grep' | awk {'print $2'} | xargs kill -9
```

where `<processes_name>` is `ldbar.exe` or `logasio`.
- d. If the Lotus Notes/Domino Server is running, restart it. Before restarting, make sure that none of the Domino processes are still running.
- e. Log in as a `notes` user and run the following command to see if the server recovered:
 - On windows:

```
<Data_Protector_home>\bin\util_notes.exe -box -ini:<path to notes.ini file>
```
 - On UNIX:

```
/opt/omni/bin/util_notes.exe -box -ini:<path to notes.ini file>
```If everything is working properly, the `*RETVAl*0` message is displayed.

NOTE

On UNIX, this is caused by corrupted shared memory and semaphores that the program does not clean up. Even if you do not have any troubles after the crash, it is good practice to clean up before restarting any process.

6. Check errors during the backup session.

Observe the messages reported during the backup session. In cases when the error is related to the Lotus Notes/Domino Server, the following type of error may be displayed:

```
Lotus ERROR [error #]: <Error description>
```

Examine the error description and take appropriate actions.

Example of Lotus Error Message

```
[Critical] From: OB2BAR@ice.hermes "BLUE" Time: 1.10.01 16:26:48
```

Lotus ERROR [3748]: Attempt to backup a database that is currently being backed up.

- 7. On UNIX, the Lotus Notes/Domino backup cannot be performed when the Lotus Notes/Domino Server and Windows Terminal Services coexist on the same host and the Lotus Notes/Domino Server is started from the terminal client program.**

The Windows Terminal Services should not be used to manage the Lotus Notes/Domino Server. However, the Lotus Notes/Domino backup can be performed when using the terminal service client program to start the Data Protector GUI on the host where the Lotus Notes/Domino Server is running. The server can be managed locally or with a VNC program.

Restore Problems

At this stage, you should have performed all the verification steps described in the previous sections. After this, proceed as follows:

- 1. Perform a filesystem restore.**

Check whether the filesystem restore of the problematic client works. It is much easier to troubleshoot a filesystem restore.

- 2. Check whether the Data Protector Lotus Integration Agent `ldbar.exe` is installed on the system.**
- 3. Check the restore to another client.**

To restore to another system, ensure that the Lotus Notes/Domino Server is installed and that it has the same non-database files as the Lotus Notes/Domino Server whose backup is to be restored. Those files must be first restored from a filesystem backup.

- 4. Examine system errors.**

If the Lotus Notes/Domino Server restore fails, examine the system errors reported in the `<Data_Protector_home>\log\debug.log` (Windows system) or `/var/opt/omni/log/debug.log` (UNIX system) file, which is located on the Data Protector Lotus Notes/Domino client system.

5. **Test a restore session using `ldbar.exe` command.**

Run the following command from the
<Data_Protector_home>\bin (Windows systems) or
/opt/omni/bin (UNIX systems) directory on the Data Protector
Lotus Notes/Domino Server system:

```
ldbar.exe -perform:restore -db:<DB_NAME>  
-server:<SRV_NAME> -ini:<path to notes.ini file>
```

For other `ldbar.exe` parameters, refer to command help by running
`ldbar.exe -help`.

6. **Check errors during the restore session.**

Observe the messages reported during the restore session. In case the error is related to the Lotus Notes/Domino Server, the following type of error can be displayed:

```
Lotus ERROR [error #]: <Error description>
```

Examine the error description and take appropriate actions.

Example of Lotus Error Message

```
[Minor] From: OB2BAR@ice.hermes "BLUE" Time: 30.9.01  
21:56:24
```

```
Lotus ERROR [5098]: The database is in use and cannot be  
taken offline.
```

Recovery Problems

At this stage, you should have performed all the verification steps described in the previous sections. After this, proceed as follows:

1. **Recovery of restored Lotus Notes/Domino NSF database failed.**

You can experience the following error at the recovery process:

```
[Critical] From: OB2BAR@ice.hermes "BLUE" Time: 19.10.01  
17:24:23
```

```
Lotus ERROR [5114]:Recovery Manager: Recovery only  
supported for Backup Files.
```

This error indicates that at least one database from the restore list was accessed, for example: by Lotus Notes/Domino Server, any user or any process, before the recovery ended.

Proceed as follows:

- a. Restart the Lotus Notes/Domino Server and perform the restore again.
- b. Restore the failed database to a location other than the one it was backed up from.

2. Check the recovery time parameter setting.

The recovery time parameter must be set as follows:

yyyy/mm/dd.hh:mm:ss

The recovery time parameter must be in the above mentioned format, otherwise the recovery time can be misunderstood. It is very important that time format is accurate and that you use a 24 hour format.

Example

2001/01/25.18:15:00

3. Recovery failed with a Lotus ERROR [520] error.

The following error message indicates that the recovery has failed.

```
[Critical] From: OB2BAR@ice.hermes "BLUE" Time: 1.10.01  
9:04:23
```

Lotus ERROR [520]:

This can happen, if you have restored several databases but some of them were not under transaction logging at the backup time. Therefore no database was in the list for recovery. This is the case when you are recovering NTF database types or an NSF database that is not recoverable.

To resolve the problem, try to restore only one database, for which you are sure that it is recoverable, and observe messages. It might be that one database in the restore list is corrupt (was corrupted at backup time) and therefore the Lotus C API recovery call fails.

NOTE

No description is listed for error number 520. This is because the internal error text of Lotus C API. There are several error codes that are internal type and have no description listed.

Before You Call Support

If you have performed the troubleshooting procedures without solving your problem, you should gather the following information for the Data Protector support before you make your call:

1. Provide details about your hardware and software configuration, including official patches you use, the Lotus Notes/Domino Server version, etc...
2. Provide a detailed description about the action performed that failed. If you have backup problems, attach the backup specification.
3. Provide the information from the `<Data_Protector_home>\log\debug.log`. Describe what happened after the failure.
4. Copy the session output to a file.

Glossary

access rights

See **user rights**.

ACSLs (*StorageTek specific term*)

The Automated Cartridge System Library Server (ACSLs) software that manages the Automated Cartridge System (ACS).

Active Directory (*Windows specific term*)

The directory service in a Windows network. It contains information about resources on the network and makes them accessible to users and applications. The directory services provide a consistent way to name, describe, locate, access and manage resources regardless of the physical system they reside on.

AML (*EMASS/GRAU specific term*)

Automated Mixed-Media library.

application agent

A component needed on a client to back up or restore online database integrations.

See also **Disk Agent**.

application system (*ZDB specific term*)

A system the application or database runs on. The application or database data is located on source volumes.

See also **backup system** and **source volume**.

archived redo log (*Oracle specific term*)

Also called offline redo log. If the Oracle database operates in the ARCHIVELOG mode, as each online redo log is filled, it is copied to one (or more) archived log destination(s). This copy is the Archived Redo Log. The presence or absence of an Archived Redo Log is determined by the mode that the database is using:

- ARCHIVELOG - The filled online redo log files are archived before they are reused. The database can be recovered from an instance and disk failure. The “hot” backup can be performed only when the database is running in this mode.
- NOARCHIVELOG - The filled online redo log files are not archived.

See also **online redo log**.

archive logging (*Lotus Domino Server specific term*)

Lotus Domino Server database mode where transaction log files are overwritten only after they have been backed up.

ASR Set

A collection of files stored on several diskettes, required for proper reconfiguration of the replacement disk

Glossary

(disk partitioning and logical volume configuration) and automatic recovery of the original system configuration and user data that was backed up during the full client backup.

These files are stored as an ASR archive file on the Cell Manager (in `<Data_Protector_home>\Config\Server\dr\asr` on a Windows Cell Manager or in `/etc/opt/omni/server/dr/asr/` on a UNIX Cell Manager) as well as on the backup medium. The ASR archive file is extracted to three diskettes for 32-bit Windows systems or four diskettes for 64-bit Windows systems after a disaster occurs. You need these diskettes to perform ASR.

autochanger

See **library**

autoloader

See **library**

BACKINT (*SAP R/3 specific term*)

SAP R/3 backup programs can call the Data Protector `backint` interface program via an open interface, which enables them to communicate with Data Protector software. For backup and restore, SAP R/3 programs issue orders for the Data Protector `backint` interface.

backup API

The Oracle interface between the Oracle backup/restore utility and the backup/restore media management layer. The

interface defines a set of routines to allow the reading and writing of data to the backup media, the creation, searching and removing the backup files.

backup chain

This relates to a situation where full and incremental backups are performed. Based on the level of the incremental backups used (Incr, Incr 1, Incr 2, and so on), simple or rather complex dependencies of incrementals to previous incrementals can exist. The backup chain are all backups, starting from the full backup plus all the dependent incrementals up to the desired point in time.

backup device

A device configured for use with Data Protector, which can write data to and read data from storage media. This can be, for example, a standalone DDS/DAT drive or a library.

backup generation

One backup generation includes one full backup and all incremental backups until the next full backup.

backup ID

An identifier of an integration object that equals the session ID of the backup of this object. The backup ID is preserved when an object is copied, exported, or imported.

Glossary

backup object

A backup unit that contains all items backed up from one disk volume (logical disk or mount point). The backed up items can be any number of files, directories, or the entire disk or mount point. Additionally, a backup object can be a database entity or a disk image (rawdisk).

A backup object is defined by:

- Client name: hostname of the Data Protector client where the backup object resides.
- Mount point: the access point in a directory structure (drive on Windows and mount point on UNIX) on the client where the backup object is located.
- Description: uniquely defines backup objects with identical client name and mount point.
- Type: backup object type (for example filesystem or Oracle).

backup owner

Each backup object in the IDB has an owner. The default owner of a backup is the user who starts the backup session.

backup session

A process that creates a copy of data on storage media. The activities are

specified in a backup specification or an interactive session. All clients configured in one backup specification are backed up together in one backup session using the same backup type (full or incremental). The result of a backup session is a set of media, which was written to, also called the backup or media set.

*See also **incremental backup** and **full backup**.*

backup set

A complete set of integration objects associated with a backup.

backup set (*Oracle specific term*)

A logical grouping of backed up files that are created using the RMAN backup command. A backup set is a complete set of files associated with a backup. The files can be multiplexed to increase performance. A backup set contains either datafiles or archived logs, but not both together.

backup specification

A list of objects to be backed up, together with a set of devices or drives to be used, backup options for all objects in the specification, days and time that you want backups to be performed. The objects are entire disks/volumes or parts of them such as files, directories, or even the Windows

Glossary

Registry for example. File selection lists such as include-lists and exclude-lists can be specified.

backup system (*ZDB specific term*)

A system connected to target volumes of one or multiple application systems. The backup system is typically connected to a backup device to perform the backup of the data in a replica.

See also **application system, target volume, and replica.**

backup types

See **incremental backup, differential backup, transaction backup, full backup and delta backup.**

backup view

Data Protector provides different views for backup specifications: By Type - according to the type of data available for backups/templates. Default view. By Group - according to the group to which backup specifications/templates belong. By Name - according to the name of backup specifications/templates. By Manager - if you are running MoM, you can also set the Backup view according to the Cell Manager to which backup specifications/templates belong.

BC (*EMC Symmetrix specific term*)

Business Continuity are processes that allow customers to access and manage

instant copies of EMC Symmetrix standard devices.

See also **BCV.**

BC (*HP StorageWorks Disk Array XP specific term*)

The Business Copy XP allows to maintain internal copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data backup or data duplication. The copies (secondary volumes or S-VOLs) can be separated from the primary volumes (P-VOLs) and connected to a different system for various purposes, such as backup and development. For backup purposes, P-VOLs should be connected to the application system, and one of the S-VOL mirror sets to the backup system. *See also* **HP StorageWorks Disk Array XP LDEV, CA, Main Control Unit, application system, and backup system.**

BC Process (*EMC Symmetrix specific term*)

A protected storage environment solution that has defined specially configured EMC Symmetrix devices as mirrors or Business Continuity Volumes to protect data on EMC Symmetrix standard devices.

See also **BCV.**

BC VA (*HP StorageWorks Virtual Array specific term*)

Business Copy VA allows you to

Glossary

maintain internal copies of HP StorageWorks Virtual Array LUNs for data backup or data duplication within the same virtual array. The copies (child or Business Copy LUNs) can be used for various purposes, such as backup, data analysis or development. When used for backup purposes, the original (parent) LUNs are connected to the application system and the Business Copy (child) LUNs are connected to the backup system.

See also **HP StorageWorks Virtual Array LUN, application system, and backup system.**

BCV (*EMC Symmetrix specific term*) Business Continuance Volumes, or BCV devices, are dedicated SLDs that are pre-configured in the ICDA on which the business continuation operation runs. BCV devices are assigned separate SCSI addresses, differing from the addresses used by the SLDs they mirror. The BCV devices are used as splittable mirrors of the primary EMC Symmetrix SLDs that need to be protected.

See also **BC** and **BC Process.**

Boolean operators

The Boolean operators for the full text search functionality of the online Help system are AND, OR, NOT, and NEAR. Used when searching, they enable you to define your query precisely by creating a relationship between search terms. If no operator is specified in a

multi-word search, AND is used by default. For example, the query manual disaster recovery is equivalent to manual AND disaster AND recovery.

boot volume/disk/partition

A volume/disk/partition with files required for the initial step of the boot process. Microsoft terminology defines the boot volume/disk/partition as a volume/disk/partition containing the operating system files.

BRARCHIVE (*SAP R/3 specific term*)

An SAP R/3 backup tool that allows you to archive redo log files. BRARCHIVE also saves all the logs and profiles of the archiving process.

See also **SAPDBA, BRBACKUP** and **BRRESTORE.**

BRBACKUP (*SAP R/3 specific term*)

An SAP R/3 backup tool that allows an online or offline backup of the control file, of individual data files, or of all tablespaces and, if necessary, of the online redo log files.

See also **SAPDBA, BRARCHIVE** and **BRRESTORE.**

BRRESTORE (*SAP R/3 specific term*)

An SAP R/3 tool that can be used to restore files of the following type:

- Database data files, control files, and online redo log files saved with BRBACKUP

Glossary

- Redo log files archived with BRARCHIVE
- Non-database files saved with BRBACKUP

You can specify files, tablespaces, complete backups, log sequence numbers of redo log files, or the session ID of the backup.

See also **SAPDBA**, **BRBACKUP** and **BRARCHIVE**.

BSM

The Data Protector Backup Session Manager controls the backup session. This process always runs on the Cell Manager system.

CA (*HP StorageWorks Disk Array XP specific term*)

Continuous Access XP allows you to create and maintain remote copies of HP StorageWorks Disk Array XP LDEVs for purposes such as data duplication, backup, and disaster recovery. CA operations involve the main (primary) disk arrays and the remote (secondary) disk arrays. The main disk arrays contain the CA primary volumes (P-VOLs), which contain the original data and are connected to the application system. The remote disk arrays contain the CA secondary volumes (S-VOLs) connected to the backup system. *See also* **BC** (*HP StorageWorks Disk*

Array XP specific term), **Main Control Unit** and **HP StorageWorks Disk Array XP LDEV**.

CAP (*StorageTek specific term*)

Cartridge Access Port is a port built into the door panel of a library. The purpose is to enter or eject media.

catalog protection

Defines how long information about backed up data (such as file names and file versions) is kept in the IDB.

See also **data protection**.

CDB

The Catalog Database is a part of the IDB that contains information about backups, object copies, restores, media management sessions, and backed up data. Depending on the selected logging level, it also contains file names and file versions. This part of the database is always local to the cell.

See also **MMDB**.

CDF file (*UNIX specific term*)

A Context Dependent File is a file consisting of several files grouped under the same pathname. The system ordinarily selects one of the files using the context of the process. This mechanism allows machine dependent executables, system data, and device files to work correctly from all hosts in a cluster while using the same pathname.

Glossary

cell

A set of systems that are under the control of a Cell Manager. The cell typically represents the systems on a site or an organizational entity, which are connected to the same LAN. Central control is available to administer the backup and restore policies and tasks.

Cell Manager

The main system in the cell where the essential Data Protector software is installed and from which all backup and restore activities are managed. The GUI used for management tasks can be located on a different system. Each cell has one Cell Manager system.

centralized licensing

Data Protector allows you to configure centralized licensing for the whole enterprise environment consisting of several cells. All Data Protector licenses are installed and kept on the Enterprise Cell Manager system. You can then allocate licenses to specific cells to suit your needs.

See also MoM.

Centralized Media Management Database (CMMDB)

See CMMDB.

channel (*Oracle specific term*)

An Oracle Recovery Manager resource allocation. Every allocated channel starts a new Oracle process, which

performs backup, restore, and recovery actions. The type of channel allocated determines the type of media used:

- type “disk”
- type ‘SBT_TAPE’

If the specified channel is type ‘SBT_TAPE’ and Oracle is integrated with Data Protector, the server process will attempt to read backups from or write data files to Data Protector.

circular logging (*Microsoft Exchange Server and Lotus Domino Server specific term*)

Circular logging is a Microsoft Exchange Server database and Lotus Domino Server database mode, in which the transaction log file contents are periodically overwritten after the corresponding data is committed to the database. Circular logging reduces disk storage space requirements.

client backup

A backup of all filesystems mounted on a client. Filesystems mounted on the client after the backup specification was created are not automatically detected.

client backup with disk discovery

A backup of all filesystems mounted on a client. When the backup starts, Data Protector discovers the disks on the clients. Client backup with disk

Glossary

discovery simplifies backup configuration and improves backup coverage of systems that often mount or dismount disks.

client or client system

Any system configured with any Data Protector functionality and configured in a cell.

cluster-aware application

It is an application that supports the cluster Application Programming Interface. Each cluster-aware application declares its own critical resources (disk volumes (on Microsoft Cluster Server), volume groups (on MC/ServiceGuard), application services, IP names and addresses ...).

CMD Script for OnLine Server

(Informix specific term)

Windows CMD script that is created in INFORMIXDIR when Informix OnLine Server is configured. The CMD script is a set of system commands that export environment variables for OnLine Server.

CMMDB

The Data Protector Centralized Media Management Database (CMMDB) is the result of merging MMDBs from several cells in the MoM environment. It allows you to share high-end devices and media across multiple cells in a MoM environment. One cell can control the

robotics, serving the devices that are connected to systems in other cells. The CMMDB must reside on the MoM Manager. A reliable network connection between the MoM cell and the other Data Protector cells is highly recommended
See also MoM.

COM+ Registration Database

(Windows specific term)

The COM+ Registration Database and the Windows Registry store COM+ application attributes, class attributes, and computer-level attributes. This guarantees consistency among these attributes and provides common operation on top of these attributes.

command-line interface

A set of DOS and UNIX like commands that you can use in shell scripts to perform Data Protector configuration, backup, restore, and management tasks.

Command View (CV) EVA *(HP*

StorageWorks EVA specific term)

The user interface that allows you to configure, manage, and monitor your HP StorageWorks EVA storage system. It is used to perform various storage management tasks, for example, creating virtual disk families, managing storage system hardware, creating snapclones and snapshots of virtual disks. The Command View EVA software runs on the HP OpenView

Glossary

Storage Management Appliance, and is accessed by a Web browser.

See also **HP StorageWorks EVA Agent (legacy)** and **HP StorageWorks EVA SMI-S Agent**.

concurrency

See **Disk Agent concurrency**.

control file (*Oracle and SAP R/3 specific term*)

An Oracle data file that contains entries specifying the physical structure of the database. It provides database consistency information used for recovery.

CRS

The Cell Request Server process (service) runs on the Data Protector Cell Manager. It starts and controls the backup and restore sessions. The service is started as soon as Data Protector is installed on the Cell Manager.

CRS runs under the account root on UNIX systems, and under any Windows account. By default, it runs under the account of the user, specified at installation time.

CSM

The Data Protector Copy Session Manager process controls the object copy session and runs on the Cell Manager system.

data file (*Oracle and SAP R/3 specific term*)

A physical file created by Oracle that contains data structures such as tables and indexes. A data file can only belong to one Oracle database.

data protection

Defines how long the backed up data on media remains protected, that is, Data Protector will not overwrite it. When the protection expires, Data Protector will be able to reuse the media in one of the next backup sessions.

See also **catalog protection**.

Data Protector Event Log

A central repository of all Data Protector related notifications. By default, all notifications are sent to the Event Log. The Event Log is accessible only to Data Protector users in the Admin group and to Data Protector users who are granted the Reporting and notifications user rights. You can view or delete all events in the Event Log.

Data Protector user account

You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group

Glossary

membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

data stream

Sequence of data transferred over the communication channel.

database library

A Data Protector set of routines that enables data transfer between Data Protector and a server of an online database integration, for example, the Oracle Server.

database parallelism

More than one database is backed up at a time if the number of available devices allows you to perform backups in parallel.

database server

A computer with a large database stored on it, such as the SAP R/3 or Microsoft SQL database. A server has a database that can be accessed by clients.

Dboject (*Informix specific term*)

An Informix physical database object. It can be a blob space, db space, or logical-log file.

DC directory

The Detail Catalog (DC) directory consists of DC binary files, which store information about file versions. It represents the DCBF part of the IDB,

which occupies approximately 80% of the IDB. The default DC directory is called the dcbf directory and is located in the `<Data_Protector_home>\db40` directory on a Windows Cell Manager and in the `/var/opt/omni/server/db40` directory on a UNIX Cell Manager. You can create more DC directories and locate them as appropriate to you. Up to 10 DC directories are supported per cell. The default maximum size of a DC directory is 4 GB.

DCBF

The Detail Catalog Binary Files (DCBF) part of the IDB stores information about file versions and attributes. It occupies approximately 80% of the IDB. One DC binary file is created for each Data Protector medium used for backup.

delta backup

A delta backup is a backup containing all the changes made to the database from the last backup of any type. *See also* **backup types**

device

A physical unit which contains either just a drive or a more complex unit such as a library.

device chain

A device chain consists of several standalone devices configured for sequential use. When a medium in one

Glossary

device gets full, the backup automatically continues on a medium in the next device in the device chain.

device group (*EMC Symmetrix specific term*)

A logical unit representing several EMC Symmetrix devices. A device cannot belong to more than a single device group. All devices in a device group must be on the same EMC Symmetrix unit. You can use a device group to identify and work with a subset of the available EMC Symmetrix devices.

device streaming

A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for more data, reverses the tape a little and resumes to write to the tape, and so on. In other words, if the data rate written to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. Streaming significantly improves the performance of the device and use of space.

DHCP server

A system running the Dynamic Host Configuration Protocol (DHCP) providing dynamic configuration of IP addresses and related information.

differential backup

An incremental backup (incr) based on any previous Data Protector backup (full or any incremental), which must still be protected.

See **incremental backup**.

differential backup (*MS SQL specific term*)

A database backup that records only the data changes made to the database after the last full database backup.

See also **backup types**.

differential database backup

A differential database backup records only those data changes made to the database after the last full database backup.

direct backup

A SAN-based backup solution in which data movement directly from disk to tape (or to other secondary storage) is facilitated by the SCSI Extended Copy (Xcopy) command. Direct backup lessens the backup I/O load on systems in a SAN environment. The data movement is facilitated directly from disk to tape (or to other secondary storage) by the SCSI Extended Copy (XCOPY) command. The command is provided by any element of the infrastructure including bridges, switches, tape libraries, and disk subsystems.

See also **XCOPY engine**.

Glossary

directory junction (*Windows specific term*)

Directory junctions use the reparse point concept of Windows. An NTFS 5 directory junction allows you to redirect a directory/file request to another location.

Directory Store (DS) (*Microsoft Exchange specific term*)

A part of the Microsoft Exchange Server directory. The Microsoft Exchange Server directory contains objects used by Microsoft Exchange applications in order to find and access services, mailboxes, recipients, public folders, and other addressable objects within the messaging system.

See also **Information Store (MDB)**.

disaster recovery

A process to restore a client's main system disk to a state close to the time when a (full) backup was performed.

Disk Agent

A component needed on a client to back it up and restore it. The Disk Agent controls reading from and writing to a disk. During a backup session, the Disk Agent reads data from a disk and sends it to the Media Agent, which then moves it to the device. During a restore session the Disk Agent receives data from the Media Agent and writes it to the disk.

Disk Agent concurrency

The number of Disk Agents that are allowed to send data to one Media Agent concurrently.

disk discovery

The detection of disks during client backup with disk discovery. During this backup, Data Protector discovers (detects) the disks that are present on the client — even though they might not have been present on the system when the backup was configured — and backs them up. This is particularly useful in dynamic environments, where configurations change rapidly. After the disks are expanded, each inherits all options from its master client object. Even if pre- and post-exec commands are specified once, they are started many times, once per each object.

disk group (*Veritas Volume Manager specific term*)

The basic unit of data storage in VxVM system. A disk group can consist of one or more physical volumes. There can be more than one disk group on the system.

disk image (rawdisk) backup

A high-speed backup where Data Protector backs up files as bitmap images. A disk image (rawdisk) backup does not track the files and directory structure stored on the disk, but stores a disk image structure on byte level. You

Glossary

can perform a disk image backup of either specific disk sections or a complete disk.

disk quota

A concept to manage disk space consumption for all or a subset of users on a computer system. This concept is used by several operating system platforms.

disk staging

The process of backing up data in several phases to improve the performance of backups and restores, reduce costs of storing the backed up data, and increase the data availability and accessibility for restore. The backup stages consist of backing up data to one media type first (for example disk) and later copying it to a different media type (for example tape).

Distributed File System (DFS)

A service that connects file shares into a single namespace. The file shares can reside on the same or on different computers. DFS provides client access to the resources in a location-transparent manner.

DMZ

The Demilitarized Zone (DMZ) is a network inserted as a "neutral zone" between a company's private network (intranet) and the outside public network

(Internet). It prevents outside users from getting direct access to company servers in the intranet.

DNS server

In the DNS client-server model, this is the server containing information about a portion of the DNS database that makes computer names available to client resolvers querying for name resolution across the Internet.

domain controller

A server in a network that is responsible for user security and verifying passwords within a group of other servers.

DR image

Data required for temporary disaster recovery operating system (DR OS) installation and configuration.

DR OS

A disaster recovery operating system is an operating system environment in which disaster recovery runs. It provides Data Protector a basic runtime environment (disk, network, tape, and filesystem access). The OS has to be installed and configured before the Data Protector disaster recovery can be performed. DR OS not only hosts the Data Protector disaster recovery process but is also a part of the restored system because it replaces its own configuration data with the original configuration data.

Glossary

drive

A physical unit that receives data from a computer system and can write it onto a magnetic medium (typically a tape drive). It can also read the data from the medium and send it to the computer system.

drive index

A number that identifies the mechanical position of a drive inside a library device. This number is used by the robotic control to access a drive.

dynamic client

See **client backup with disk discovery**.

EMC Symmetrix Agent (SYMA)

(EMC Symmetrix specific term)

See **Symmetrix Agent (SYMA)**

emergency boot file *(Informix specific term)*

An Informix configuration file that resides in the <INFORMIXDIR>\etc directory (on HP-UX) or <INFORMIXDIR>/etc directory (on Windows) and is called ixbar.<server_id>, where <INFORMIXDIR> is the OnLine Server home directory and <server_id> is the value of the SERVERNUM configuration parameter. Each line of the emergency boot file corresponds to one backup object.

Enterprise Backup Environment

Several cells can be grouped together and managed from a central cell. The enterprise backup environment includes all clients located in several Data Protector cells which are managed and administered from a central cell using the Manager-of-Managers concept. See also **MoM**.

Event Logs

Files in which Windows logs all events, such as the starting or stopping of services and the logging on and off of users. Data Protector can back up Windows Event Logs as part of the Windows configuration backup.

exchanger

Also referred to as SCSI Exchanger. See also **library**.

exporting media

A process that removes all data about backup sessions, such as systems, objects, and file names, which reside on the media from the IDB. Information about the media and their relation to a pool is also removed from the IDB. The data on the media remains unchanged. See also **importing media**.

Glossary

Extensible Storage Engine (ESE)

(Microsoft Exchange Server 2000/2003 specific term)

A database technology used as a storage system for information exchange in Microsoft Exchange Server 2000/2003.

failover

Transferring of the most important cluster data, called group (on Windows) or package (on Unix) from one cluster node to another. A failover can occur mostly because of software or hardware failures or maintenance on the primary node.

FC bridge

See **Fibre Channel bridge**

Fibre Channel

An ANSI standard for high-speed computer interconnection. Using either optical or copper cables, it allows the high speed bidirectional transmission of large data files and can be deployed between sites kilometers apart. Fibre Channel connects nodes using three physical topologies: point-to-point, loop, and switched.

Fibre Channel bridge

A Fibre Channel bridge or multiplexer provides the ability to migrate existing parallel SCSI devices, like RAID arrays, solid state disks (SSD), and tape libraries to a Fibre Channel

environment. On one side of the bridge or multiplexer there is a Fibre Channel interface while on the other side there are parallel SCSI ports. The bridge or multiplexer enables SCSI packets to be moved between the Fibre Channel and parallel SCSI devices.

file depot

A file containing the data from a backup to a file library device.

file jukebox device

A device residing on disk consisting of multiple slots used to store file media.

file library device

A device which resides on a disk emulating a library with several media, hence containing multiple files, referred to as file depots.

File Replication Service (FRS)

A Windows service that replicates the domain controller store logon scripts and group policies. FRS also enables replication of Distributed File System (DFS) shares between systems and allows any server to perform replication activity.

file version

The same file can be backed up multiple times in case of full backups and incremental backups (if the file changed). If the log level ALL is selected for backup, Data Protector

Glossary

retains one entry in the IDB for the filename itself and one for each version (date/time) of the file.

filesystem

The organization of files on a hard disk. A filesystem is backed up so that the file attributes and the file contents are stored on the backup media.

first level mirror (*HP StorageWorks Disk Array XP specific term*)

HP StorageWorks Disk Array XP allows up to three mirror copies of a Primary Volume and each of these copies can have additional two copies. The three mirror copies are called first level mirrors.

See also **Primary Volume**, and **MU numbers**.

fnames.dat

The fnames.dat files of the IDB contain information on the names of the backed up files. Typically, these files occupy about 20% of the IDB, if filenames are stored.

formatting

A process that erases any data contained on a medium and prepares it for use with Data Protector. Information about media (media ID, description, and location) is saved in the IDB as well as on the respective media (media header). Data Protector media with protected data are

not formatted until the protection expires or the media are unprotected/recycled.

free pool

An auxiliary source of media for use by media pools when they run out of media. The media pools must be configured to use free pools.

full backup

A backup in which all selected objects are backed up, whether or not they have been recently modified.

See also **backup types**.

full database backup

A backup of all data in a database, not only the data that has been changed after the last (full or incremental) backup of the database. A full database backup does not depend on any other backup.

full mailbox backup

A full mailbox backup is a backup of the entire mailbox content.

global options file

A file that allows you to customize Data Protector. It explains the global options, which cover various aspects of Data Protector, typically time-outs and limits, and affect the entire Data Protector cell. The file is located in the /etc/opt/omni/server/options directory on HP-UX and Solaris systems and in the

Glossary

<Data_Protector_home>\Config\Server\Options directory on Windows systems.

group (*Microsoft Cluster Server specific term*)

A collection of resources (for example disk volumes, application services, IP names and addresses) that are needed to run a specific cluster-aware applications.

GUI

A cross-platform (HP-UX, Solaris, and Windows) graphical user interface, provided by Data Protector for easy access to all configuration, administration, and operation tasks.

hard recovery (*Microsoft Exchange Server specific term*)

A Microsoft Exchange Server database recovery that is performed after a restore by the database engine, using transaction log files.

heartbeat

A cluster data set with a time stamp carrying information about the operational status of a particular cluster node. This data set or packet is distributed among all cluster nodes.

Hierarchical Storage Management (HSM)

A method for optimizing the use of expensive hard disk storage by migrating less frequently used data to

less expensive optical platters. When needed, the data is migrated back to hard disk storage. This balances the need for fast retrieval from hard disk with the lower cost of optical platters.

Holidays file

A file that contains information about holidays. You can set different holidays by editing the Holidays file: /etc/opt/omni/server/Holidays on the UNIX Cell Manager and <Data_Protector_home>\Config\Server\holidays on the Windows Cell Manager.

host backup

See **client backup with disk discovery**.

hosting system

A working Data Protector client used for Disk Delivery Disaster Recovery with a Data Protector Disk Agent installed.

HP ITO

See **OVO**.

HP OpC

See **OVO**.

HP OpenView SMART Plug-In (SPI)

A fully integrated, out-of-the-box solution which "plugs into" HP OpenView Operations, extending the managed domain. Through the Data Protector integration, which is implemented as an HP OpenView

Glossary

SMART Plug-In, a user can have an arbitrary number of Data Protector Cell Managers monitored as an extension to HP OpenView Operations (OVO).

HP OVO

See **OVO**.

HP StorageWorks Disk Array XP LDEV

A logical partition of a physical disk within an HP StorageWorks Disk Array XP. LDEVs are entities that can be replicated in the Continuous Access XP (CA) and Business Copy XP (BC) configurations, or can be used as standalone entities.

See also **BC** (*HP StorageWorks Disk Array XP specific term*), **CA** (*HP StorageWorks Disk Array XP specific term*), and **replica**.

HP StorageWorks EVA Agent (legacy)

A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array integration operating on HP StorageWorks EVA with Command View (CV) EVA software v3.1 or lower, and the EVA VCS firmware v3.01x or lower.

See also **Command View (CV) EVA** and **HP StorageWorks EVA SMI-S Agent**.

HP StorageWorks EVA SMI-S Agent

A Data Protector software module that executes all tasks required for the HP StorageWorks Enterprise Virtual Array integration operating on HP StorageWorks EVA with Command View (CV) EVA software starting with v3.2. With the EVA SMI-S Agent, the control over the array is established through HP StorageWorks SMI-S EVA provider, which directs communication between incoming requests and CV EVA.

See also **Command View (CV) EVA**, **HP StorageWorks SMI-S EVA provider**, and **HP StorageWorks EVA Agent (legacy)**.

HP StorageWorks SMI-S EVA provider

An interface used for controlling HP StorageWorks Enterprise Virtual Array. SMI-S EVA provider runs as a separate service on the HP OpenView Storage Management Appliance system and acts as a gateway between incoming requests and Command View EVA. With the Data Protector HP StorageWorks EVA integration, SMI-S EVA provider accepts standardized requests from the EVA SMI-S Agent, communicates with Command View EVA for information or method invocation, and returns standardized responses.

See also **HP StorageWorks EVA SMI-**

Glossary

S Agent and Command View (CV) EVA.

HP StorageWorks Virtual Array LUN

A logical partition of a physical disk within an HP StorageWorks Virtual Array. LUNs are entities that can be replicated in the HP StorageWorks Business Copy VA configuration, or can be used as standalone entities.
See also BC VA and replica.

HP VPO
See OVO.

ICDA (*EMC Symmetrix specific term*)
EMC's Symmetrix Integrated Cached Disk Arrays (ICDA) is a disk array device that combines a set of physical disks, a number of FWD SCSI channels, an internal cache memory, and control and diagnostic software commonly referred to as the microcode.

IDB
The Data Protector Internal Database is an embedded database located on the Cell Manager that keeps information regarding which data is backed up, on which media it is backed up, how backup and restore sessions are run, and which devices and libraries are configured.

importing media

A process that re-reads all data about backup sessions which are on the medium back into the IDB. This then allows for fast and convenient access to the data on the media.
See also exporting media.

incremental backup

A backup that selects only files that have changed since a previous backup. Several levels of incremental backup are available, allowing selective backup of only files that have changed since the last incremental backup.
See also backup types.

incremental backup (*Microsoft Exchange Server specific term*)

A backup of the Microsoft Exchange Server data that has changed since the last full or incremental backup. With the incremental backup, only the transaction log files are backed up.
See also backup types.

incremental mailbox backup

An incremental mailbox backup backs up all the changes made to the mailbox after the last backup of any type.

incremental1 mailbox backup

An incremental1 mailbox backup backs up all the changes made to the mailbox after the last full backup.

Glossary

incremental (re)-establish (*EMC Symmetrix specific term*)

A BCV or SRDF control operation. In BCV control operations, an incremental establish causes the BCV device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.

In SRDF control operations, an incremental establish causes the target (R2) device to be synchronized incrementally and to function as an EMC Symmetrix mirrored medium. The EMC Symmetrix devices must have been previously paired.

incremental restore (*EMC Symmetrix specific term*)

A BCV or SRDF control operation. In BCV control operations, an incremental restore reassigns a BCV device as the next available mirror of the standard device in the pair. However, the standard devices are updated with only the data that was written to the BCV device during the time of the original pair split, and the data that was written to the standard device during the split is overwritten with data from the BCV mirror. In SRDF control operations, an incremental restore reassigns a target (R2) device as the next available mirror of the source (R1) device in the pair. However, the source (R1) devices are updated with only the data that was

written to the target (R2) device during the time of the original pair split, and the data that was written to the source (R1) device during the split is overwritten with data from the target (R2) mirror.

Inet

A process that runs on each UNIX system or service that runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and for starting other processes needed for backup and restore. The Inet service is started as soon as Data Protector is installed on a system. The Inet process is started by the inetd daemon.

Information Store (*Microsoft Exchange Server 2000/2003 specific term*)

The Microsoft Exchange Server 2000/2003 service that is responsible for storage management. Information Store in Microsoft Exchange Server 2000/2003 manages two kinds of stores: mailbox stores and public folder stores. A mailbox store consists of mailboxes that belong to individual users. A public folder store contains public folders and messages that are shared among several users.

See also **Key Management Service** and **Site Replication Service**.

Glossary

Information Store (*Microsoft Exchange Server 5.5 specific term*)

This is the default message store provider for the Microsoft Exchange Server 5.5. Information Store consists of the following stores:

- public information store
- private information store
- personal folder store
- offline information store.

The public information store contains public folders and messages that can be shared among multiple users and applications. A single public store is shared by all users within an Exchange Server 5.5 organization, even if multiple Exchange Servers are used. The private information store consists of mail boxes that can belong to users or to applications. The mail boxes reside on the server running the Exchange Server 5.5.

See also **Directory Store (DS)**.

initializing

See **formatting**.

Installation Server

A computer system that holds a repository of the Data Protector software packages for a specific architecture. The Installation Server is

used for remote installation of Data Protector clients. In mixed environments at least two Installation Servers are needed: one for UNIX systems and one for Windows systems.

instant recovery (*ZDB specific term*)

A process in which a replica, produced by a ZDB-to-disk or a ZDB-to-disk+tape sessions, is used to restore the contents of the source volumes to their states at the time at which the replica was created, avoiding the need to perform a restore from tape. Depending on the application/database concerned, this may be all that is required, or other steps, such as the application of transaction log files, may be required for full recovery.

See also **replica**, **zero downtime backup (ZDB)**, **ZDB to disk**, and **ZDB to disk+tape**.

integrated security (*MS SQL specific term*)

Integrated security allows the Microsoft SQL Server to use Windows authentication mechanisms to validate Microsoft SQL Server logins for all connections. Using integrated security means that users have one password for both Windows and Microsoft SQL Server. Integrated security should be used in environments where all clients support trusted connections. Connections validated by Windows Server and accepted by Microsoft SQL

Glossary

Server are referred to as trusted connections. Only trusted connections are allowed.

integration object

A backup object of a Data Protector integration, such as Oracle or SAP DB.

Internet Information Server (IIS)

(Windows specific term)

Microsoft Internet Information Server is a network file and application server that supports multiple protocols. Primarily, IIS transmits information in Hypertext Markup Language (HTML) pages by using the Hypertext Transport Protocol (HTTP).

IP address

Internet Protocol address is a numeric address of a system used to uniquely identify the system on the network. The IP address consists of four groups of numbers separated by periods (full stops).

ISQL *(Sybase specific term)*

A Sybase utility used to perform system administration tasks on Sybase SQL Server.

ITO

See **OVO**.

jukebox

See **library**.

jukebox device

A device consisting of multiple slots used to store either optical or file media. When being used to store file media, the jukebox device is known as the “file jukebox device”.

Key Management Service *(Microsoft Exchange Server 2000/2003 specific term)*

The Microsoft Exchange Server 2000/2003 service that provides encryption functionality for enhanced security. See also **Information Store** and **Site Replication Service**.

LBO *(EMC Symmetrix specific term)*

A Logical Backup Object (LBO) is an object of data storage/retrieval in the EMC Symmetrix environment. It is stored/retrieved by EMC Symmetrix as one entity and can only be restored as a whole.

library

Also called autochanger, jukebox, autoloader, or exchanger. A library contains media in repository slots. Each slot holds one medium (for example, DDS/DAT). Media are moved between slots and drives by a robotic mechanism, allowing random access to media. The library can contain multiple drives.

lights-out operation or **unattended operation**

A backup or restore operation that takes

Glossary

place outside of normal business hours without an operator. This implies that no operator personnel is present to work with the backup application or service mount requests, for example.

LISTENER.ORA (*Oracle specific term*)

An Oracle configuration file that describes one or more Transparent Network Substrate (TNS) listeners on a server.

load balancing

By default, Data Protector automatically balances the usage of devices selected for backup, so that they are used evenly. Load balancing optimizes the device usage by balancing the number of objects written to each device. Since load balancing is done automatically during backup time, you do not need to manage how the data is actually backed up. You just specify the devices to be used. If you do not want to use load balancing, you can select which device will be used for each object in the backup specification. Data Protector will access the devices in the specified order.

local and remote recovery

Remote recovery is performed if all Media Agent hosts specified in the SRD file are accessible. If any of them fails, the disaster recovery process fails over to the local mode. This means that the

target system is searched for locally attached devices. If only one device is found, it is automatically used. Otherwise, Data Protector prompts you to select the device, which will be used for restore.

lock name

You can configure the same physical device several times with different characteristics, by using different device names.

The lock name is a user specified string that is used for locking all such device configurations to prevent collision if several such devices (device names) are used concurrently. Use an identical lock name for all device definitions which use the same physical device.

log_full shell script (*Informix UNIX specific term*)

A script provided by ON-Bar that you can use to start backing up logical-log files when OnLine Server issues a log-full event alarm. The Informix ALARMPROGRAM configuration parameter defaults to the `<INFORMIXDIR>/etc/log_full.sh`, where `<INFORMIXDIR>` is the OnLine Server home directory. If you do not want logical logs to be backed up continuously, set the ALARMPROGRAM configuration parameter to `<INFORMIXDIR>/etc/no_log.sh`.

Glossary

logging level

The logging level determines the amount of details on files and directories written to the IDB during backup or object copying. You can always restore your data, regardless of the logging level used during backup. Data Protector provides four logging levels: Log All, Log Directories, Log Files, and No Log. The different logging level settings influence the IDB growth, backup speed, and the convenience of browsing data for restore.

logical-log files

This applies to online database backup. Logical-log files are files in which modified data is first stored before being flushed to disk. In the event of a failure, these logical-log files are used to roll forward all transactions that have been committed as well as roll back any transactions that have not been committed.

login ID (*MS SQL Server specific term*)

The name a user uses to log on to Microsoft SQL Server. A login ID is valid if Microsoft SQL Server has an entry for that user in the system table syslogin.

login information to the Oracle

Target Database (*Oracle and SAP R/3 specific term*)

The format of the login information is <user_name>/<password>@<service>, where:

- <user_name> is the name by which a user is known to Oracle Server and to other users. Every user name is associated with a password and both have to be entered to connect to an Oracle Target Database. This user must have been granted Oracle SYSDBA or SYSOPER rights.
- <password> is a string used for data security and known only to its owner. Passwords are entered to connect to an operating system or software application. The password has to be the same as the password specified in the Oracle password file (orapwd), which is used for authentication of users performing database administration.
- <service> is the name used to identify an SQL*Net server process for the target database.

login information to the Recovery

Catalog Database (*Oracle specific term*)

The format of the login information to the Recovery (Oracle) Catalog Database is <user_name>/

Glossary

<password>@<service>, where the description of the user name, password, and service name is the same as in the Oracle SQL*Net V2 login information to the Oracle target database. In this case, <service> is the name of the service to the Recovery Catalog Database, not the Oracle target database.

Note that the Oracle user specified here has to be the owner of the Oracle Recovery (Oracle) Catalog.

Lotus C API (*Lotus Domino Server specific term*)

An interface for the exchange of backup and recovery information between Lotus Domino Server and a backup solution, like Data Protector.

LVM

A Logical Volume Manager is a subsystem for structuring and mapping physical disk space to logical volumes on UNIX systems. An LVM system consists of several volume groups, where each volume group has several volumes.

Magic Packet

See **Wake ONLAN**.

mailbox (*Microsoft Exchange Server specific term*)

The location to which e-mail is delivered, which is set up by the administrator for each user. If a set of

personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

Mailbox Store (*Microsoft Exchange Server 2000/2003 specific term*)

A part of the Information Store that maintains information about user mailboxes. A mailbox store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

Main Control Unit (MCU) (*HP StorageWorks Disk Array XP specific term*)

An HP StorageWorks XP disk array that contains the primary volumes for the Continuous Access configuration and acts as a master device.

See also **BC** (*HP StorageWorks Disk Array XP specific term*), **CA** (*HP StorageWorks Disk Array XP specific term*), and **HP StorageWorks Disk Array XP LDEV**.

Manager-of-Managers (MoM)

See **Enterprise Cell Manager**.

Media Agent

A process that controls reading from and writing to a device, which reads from or writes to a medium (typically a tape). During a backup session, a Media Agent receives data from the Disk Agent and sends it to the device for writing it to the medium. During a restore session, a Media Agent locates data on the backup

Glossary

medium and sends it to the Disk Agent. The Disk Agent then writes the data to the disk. A Media Agent also manages the robotics control of a library.

MAPI (*Microsoft Exchange specific term*)

The MAPI (Messaging Application Programming Interface) is the programming interface that lets applications and messaging clients interact with messaging and information systems.

media allocation policy

Determines in which sequence media are used for backup. The Strict allocation policy directs Data Protector to prompt for a specific medium. The Loose policy directs Data Protector to prompt for any suitable medium. The Formatted First policy directs Data Protector to give preference to unknown media, even if unprotected media are available in the library.

media condition

The quality of a medium as derived from the media condition factors. Heavy usage and age result in an increased number of read and write errors with tape media. Media need to be replaced when they are marked as POOR.

media condition factors

The user-assigned age threshold and overwrite threshold used to determine the state of a medium.

media ID

A unique identifier assigned to a medium by Data Protector.

media label

A user-defined identifier used to describe a medium.

media location

A user-defined physical location of a medium, such as "building 4" or "off-site storage".

media management session

A session performing some action on a medium, such as initializing, scanning the content, verifying data on a medium, or copying a medium.

media pool

A set of media of the same type (such as DDS) used and tracked as a group. Media are formatted and assigned to a media pool.

media set

The result of a backup session is data backed up on a group of media called media set. Depending on the media usage policy, several sessions can share the same media.

Glossary

media type

The physical type of media, such as DDS or DLT.

media usage policy

The media usage policy controls how new backups are added to the already used media. It can be Appendable, Non-Appendable, or Appendable for incrementals only.

merging

This defines one mode to resolve file conflicts during restore. If the file to be restored already exists at the destination, the one with the more recent modification date is kept. Files not present on the disk are always restored. *See also* **overwrite**.

MFS

The Migrating File System enables a standard JFS filesystem with migration capabilities (on HP-UX 11.00). The MFS is accessed via a standard filesystem interface (DMAPI), it is mounted to a directory the same way as any HP-UX filesystem. In an MFS, only the superblock, the inode and the 'extended attribute' information remain permanently on the hard disk and are never migrated. *See also* **VBFS**.

Microsoft Exchange Server

A "client-server" messaging and a workgroup system that offers a

transparent connection to many different communication systems. It provides users with an electronic mail system, individual and group scheduling, online forms, and workflow automation tools. It provides a developer with a platform on which to build custom information-sharing and messaging-service applications.

Microsoft Management Console (MMC) (*Windows specific term*)

An administration model for Windows-based environments. It provides a simple, consistent, and integrated administration user interface allowing management of many applications through the same GUI, provided that the applications adhere to the MMC model.

Microsoft SQL Server 7.0/2000

A database management system designed to meet the requirements of distributed "client-server" computing.

Microsoft Volume Shadow Copy service (VSS)

A software service that provides a unified communication interface to coordinate backup and restore of a VSS-aware application regardless of its specific features. This service collaborates with the backup application, writers, shadow copy providers, and the operating system kernel to implement the management of volume shadow copies and shadow copy

Glossary

sets.

See also **shadow copy**, **shadow copy provider**, **writer**.

mirror (*EMC Symmetrix and HP StorageWorks Disk Array XP specific term*)

See **target volume**.

mirror rotation (*HP StorageWorks Disk Array XP specific term*)

See **replica set rotation**.

MMD

The Media Management Daemon process (service) runs on the Data Protector Cell Manager and controls media management and device operations. The process is started when Data Protector is installed on the Cell Manager.

MMDB

The Media Management Database (MMDB) is a part of the IDB that contains information about media, media pools, devices, libraries, library drives, and slots configured in the cell, as well as the Data Protector media used for backup. In an enterprise backup environment, this part of the database can be common to all cells.

See also **CMMDB**, **CDB**.

MoM

Several cells can be grouped together and managed from a central cell. The

management system of the central cell is the Manager-of-Managers (MoM). The MoM allows you to configure and manage multiple cells from a central point.

mount request

A screen prompt that tells you to insert a specific medium into a device. Once you respond to the mount request by providing the required medium and confirm the mount request, the session continues.

mount point

The access point in a directory structure for a disk or logical volume, for example /opt or d:. On UNIX, the mount points are displayed using the bdf or df command.

MSM

The Data Protector Media Session Manager, which runs on the Cell Manager and controls media sessions, such as copying media.

MU number (*HP StorageWorks Disk Array XP specific term*)

A Mirror Unit number is an integer number (0, 1 or 2), used to indicate a first level mirror.

See also **first level mirror**.

multi-drive server

A license that allows you to run an unlimited number of Media Agents on a

Glossary

single system. This license, which is bound to the IP address of the Cell Manager, is no longer available.

obdrindex.dat

An IDB file with information about IDB backups, media, and devices used for the backup. This information can significantly simplify IDB recovery. It is recommended to relocate the file, together with IDB transaction logs, on a separate physical disk from other IDB directories, and, additionally, to make a copy of the file and locate it where you want.

OBDR capable device

A device that can emulate a CD-ROM drive loaded with a bootable disk and can thus be used as a backup or boot device for disaster recovery purposes.

object

See **backup object**

object copy

A copy of a specific object version that is created during an object copy session or a backup session with object mirroring.

object copy session

A process that creates an additional copy of the backed up data on a different media set. During an object copy

session, the selected backed up objects are copied from the source to the target media.

object copying

The process of copying selected object versions to a specific media set. You can select object versions from one or several backup sessions to be copied.

Object ID (*Windows specific term*)

The object IDs (OIDs) enable access to NTFS 5 files no matter where in the system the files reside. Data Protector treats the OIDs as alternate streams of the files.

object mirror

A copy of a backup object created using object mirroring. Object mirrors are often referred to as object copies.

object mirroring

The process of writing the same data to several media sets during a backup session. Data Protector enables you to mirror all or some backup objects to one or more media sets.

offline backup

A backup during which an application database cannot be used by the application.

- For simple backup methods (non ZDB), the database is generally put into a quiescent state that allows use

Glossary

by the backup system, but not the application, for the whole backup period (~minutes/hours). For instance, for backup to tape, until streaming of data to the tape is finished.

- For ZDB methods, the database is also put into the quiescent state, but for the period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

See also **zero downtime backup (ZDB)** and **online backup**.

offline recovery

Offline recovery is performed if the Cell Manager is not accessible, for example, due to network problems. Only standalone and SCSI library devices can be used for offline recovery. Recovery of the Cell Manager is always offline.

offline redo log

See **archived redo log**

OmniStorage

Software providing transparent migration of less frequently used data to the optical library while keeping more frequently used data on the hard disk. HP OmniStorage runs on HP-UX systems.

On-Bar (*Informix specific term*)

A backup and restore system for OnLine Server. ON-Bar enables you to create a copy of your OnLine Server data and later restore the data. The ON-Bar backup and restore system involves the following components:

- onbar utility
- Data Protector, as the backup solution
- XBSA interface
- ON-Bar catalog tables, which are used to back up dobjects and track instances of dobjects through multiple backups.

onbar utility (*Informix specific term*)

The Informix utility that communicates backup and restore requests to OnLine Server. The utility uses XBSA to exchange control data and back up and restore data with Data Protector.

ONCONFIG (*Informix specific term*)

An environment variable that specifies the name of the active ONCONFIG configuration file. If the ONCONFIG environment variable is not present, OnLine uses the configuration values from the file `<INFORMIXDIR>/etc/onconfig` (on HP-UX) or `<INFORMIXDIR>\etc\onconfig` (on Windows).

Glossary

online backup

A backup performed while a database application remains available for use. The database is placed into a special backup mode of operation for the time period that the backup application requires access to the original data objects. During this period, the database is fully operational, but there may be a small performance impact and log files may grow very quickly.

- For simple backup methods (non ZDB), backup mode is required for the whole backup period (~minutes/ hours). For instance, for backup to tape, until streaming of data to tape is finished.
- For ZDB methods, backup mode is required for the short period of the data replication process only (~seconds). Normal database operation can then be resumed for the rest of the backup process.

In some cases, transaction logs may also have to be backed up to allow a consistent database to be restored. *See also* **zero downtime backup (ZDB)** and **offline backup**.

online redo log (*Oracle specific term*)

Redo logs that have not been archived, but are either available to the instance for recording database activity or are

filled and waiting to be archived or reused.

See also **archived redo log**.

OnLine Server (*Informix specific term*)

Refers to INFORMIX-OnLine Dynamic Server.

OpC

See **OVO**.

Oracle instance (*Oracle specific term*)

Each installation of an Oracle database on one or more systems. One computer system can have several instances of a database running.

ORACLE_SID (*Oracle specific term*)

A unique name for an Oracle Server instance. To switch among Oracle Servers, specify the desired `<ORACLE_SID>`. The `<ORACLE_SID>` is included in the `CONNECT DATA` parts of the connect descriptor in a `TNSNAMES.ORA` file and in the definition of the TNS listener in the `LISTENER.ORA` file.

original system

The system configuration backed up by Data Protector before a computer disaster hits the system.

overwrite

An option that defines one mode to resolve file conflicts during restore. All

Glossary

files are restored from a backup even if they are older than existing files.

See also **merging**.

OVO

HP OpenView Operations for Unix provides powerful capabilities for operations management of a large number of systems and applications on a network. Data Protector provides an integration into this management product. This integration is implemented as a SMART Plug-In for OVO management servers on HP-UX and Solaris. Earlier versions of OVO were called IT/Operation, Operations Center and Vantage Point Operations.

See also **merging**.

ownership

The ownership of a backup determines who can restore from the backup. The user who starts an interactive backup is the session owner. If a user starts an existing backup specification without modifying it, the session is not considered interactive. In that case, if the backup owner has been defined in the backup specification, they remain the session owner. Otherwise, the session owner becomes the user who started the backup in question. For the scheduled backups, by default, the session owner is for the UNIX Cell Manager: `root.sys@<Cell Manager>`, and for the Windows Cell Manager, the user that was specified during the

installation of the Cell Manager. It is possible to modify the ownership, so that the specific user becomes the session owner.

P1S file

P1S file contains information on how to format and partition all disks installed in the system during Enhanced Automated Disaster Recovery (EADR). It is created during full backup and is saved on backup medium and on Cell Manager into

`<Data_Protector_home>\Config\Server\dr\p1s` directory on a Windows Cell Manager or in `/etc/opt/omni/server/dr/p1s` directory on a UNIX Cell Manager with the filename `recovery.p1s`.

package (*MC/ServiceGuard and Veritas Cluster specific term*)

A collection of resources (for example volume groups, application services, IP names and addresses) that are needed to run a specific cluster-aware application.

pair status (*HP StorageWorks Disk Array XP specific term*)

A mirrored pair of disks can have various status values depending on the action performed on it. The three most important status values are:

Glossary

- **COPY** - The mirrored pair is currently resynchronizing. Data is transferred from one disk to the other. The disks do not contain the same data.
- **PAIR** - The mirrored pair is completely synchronized and both disks (the primary volume and the mirrored volume) contain identical data.
- **SUSPENDED** - The link between the mirrored disks is suspended. That means that both disks are accessed and updated independently. However, the mirror relationship is still maintained and the pair can be resynchronized without transferring the complete disk.

parallel restore

Restoring backed up data to multiple disks at the same time (that is, in parallel) by running multiple Disk Agents, that receive data from one Media Agent. For the parallel restore to work, select data that is located on different disks or logical volumes and during backup, the data from the different objects must have been sent to the same device using a concurrency of 2 or more. During a parallel restore, the data for multiple objects selected for restore is read from media at the same time, thereby improving performance.

parallelism

The concept of reading multiple data streams from an online database.

physical device

A physical unit that contains either a drive or a more complex unit such as a library.

post-exec

A backup option that executes a command or script after the backup of an object or after the entire session completes. Post-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.

See also **pre-exec**.

pre- and post-exec commands

Pre- and post-exec commands are used to perform additional action before and after a backup or restore session. They are not supplied by Data Protector. You need to create your own commands. They can be written as executables or batch files on Windows and as shell scripts on UNIX.

prealloc list

A subset of media in a media pool that specifies the order in which media are used for backup.

Glossary

pre-exec

A backup option that executes a command or script before the backup of an object or before the entire session is started. Pre-exec commands are not supplied by Data Protector. You need to create your own. They can be written as executables or batch files on Windows and as shell scripts on UNIX.

See also **post-exec**.

Primary Volume (P-VOL) *(HP*

StorageWorks Disk Array XP specific term)

Standard HP StorageWorks Disk Array XP LDEVs that act as a primary volume for the CA and BC configurations. The P-VOL is located in the MCU.

See also **Secondary Volume (S-VOL)**.

Private Information Store *(Microsoft*

Exchange Server 5.5 specific term)

A part of the Information Store that maintains information in user mailboxes. A mailbox store consists of a binary rich-text .edb file.

protection

See **data protection** and also **catalog protection**.

public folder store *(Microsoft*

Exchange Server 2000/2003 specific term)

The part of the Information Store that maintains information in public folders.

A public folder store consists of a binary rich-text .edb file and a streaming native internet content .stm file.

public/private backed up data

When configuring a backup, you can select whether the backed up data will be:

- public, that is visible (and accessible for restore) to all Data Protector users
- private, that is, visible (and accessible for restore) only to the owner of the backup and administrators

RAID

Redundant Array of Inexpensive Disks.

RAID Manager Library *(HP*

StorageWorks Disk Array XP specific term)

The RAID Manager Library is used internally by Data Protector on Solaris systems to allow access to HP StorageWorks Disk Array XP configuration, status, and performance data and to key HP StorageWorks Disk Array XP features through the use of function calls translated into a sequence of low level SCSI commands.

RAID Manager XP *(HP StorageWorks*

Disk Array XP specific term)
The RAID Manager XP application

Glossary

provides an extensive list of commands to report and control the status of the CA and BC applications. The commands communicate through a RAID Manager instance with the HP StorageWorks Disk Array XP Disk Control Unit. This instance translates the commands into a sequence of low level SCSI commands.

rawdisk backup

See **disk image backup**.

RCU (*HP StorageWorks specific term*)

The Remote Control Unit acts as a slave of an MCU in a CA configuration. In bidirectional configurations, the RCU can act as an MCU.

RDBMS

Relational Database Management System.

RDF1/RDF2 (*EMC Symmetrix specific term*)

A type of SRDF device group. Only RDF devices can be assigned to an RDF group. An RDF1 group type contains source (R1) devices and an RDF2 group type contains target (R2) devices.

RDS

The Raima Database Server process (service) runs on the Data Protector Cell Manager and manages the IDB. The process is started when Data Protector is installed on the Cell Manager.

Recovery Catalog (*Oracle specific term*)

A set of Oracle tables and views that are used by Recovery Manager to store information about Oracle databases. This information is used by Recovery Manager to manage the backup, restore, and recovery of Oracle databases. The recovery catalog contains information about:

- The physical schema of the Oracle target database
- Data file and archived log backup sets
- Data file copies
- Archived Redo Logs
- Stored scripts.

Recovery Catalog Database (*Oracle specific term*)

An Oracle database that contains a recovery catalog schema. You should not store the recovery catalog in your target database.

RecoveryInfo

When backing up Windows configuration files, Data Protector collects the information about the current system configuration (information on disk layout, volume,

Glossary

and network configuration). This information is needed for disaster recovery.

Recovery Manager (RMAN) (*Oracle specific term*)

An Oracle command-line interface that directs an Oracle Server process to back up, restore, or recover the database it is connected to. RMAN uses either the recovery catalog or the control file to store information about backups. This information can be used later in restore sessions.

recycle

A process that removes the data protection from all backed up data on a medium, allowing Data Protector to overwrite it during one of the next backups. Data that belongs to the same session(s) but resides on other media is also unprotected. Recycling does not actually alter the data on the medium.

redo log (*Oracle specific term*)

Every Oracle database has a set of two or more redo log files. The set of redo log files for the database is known as the database's redo log. Oracle uses the redo log to record all changes made to data.

Remote Control Unit (RCU) (*HP StorageWorks Disk Array XP specific term*)

The Remote Control Unit (RCU) acts as a slave of an MCU in a CA

configuration. In bidirectional configurations, the RCU can act as an MCU.

Removable Storage Management Database (*Windows specific term*)

A Windows service used for managing removable media (such as tapes and disks) and storage devices (libraries). Removable Storage allows applications to access and share the same media resources.

reparse point (*Windows specific term*)

A system-controlled attribute that can be associated with any directory or file. The value of a reparse attribute can have user-controlled data. The format of the data is understood by the application that stored the data and a filesystem filter that was installed to interpret the data and process such files. Whenever the filesystem encounters a file with a reparse point, it attempts to find the filesystem filter associated with the data format.

replica (*ZDB specific term*)

An image, at a particular point in time, of the data in source volumes that contain user-specified backup objects. Depending on the hardware/software with which it is created, the image may be an independent exact duplicate (clone) of the storage blocks at the physical disk level (for example, a split mirror), or a virtual copy (for example, a

Glossary

snapshot). From a host's perspective, on a basic UNIX or Windows system, the complete physical disk containing a backup object is replicated. However, if a volume manager is used on UNIX, the whole volume/disk group containing a backup object is replicated.

See also **snapshot**, **snapshot creation**, **split mirror**, and **split mirror creation**.

replica set (*ZDB specific term*)

A group of replicas, all created using the same backup specification.

See also **replica** and **replica set rotation**.

replica set rotation (*ZDB specific term*)

The use of a replica set for regular backup production: Each time the same backup specification requiring the use of a replica set is run, a new replica is created and added to the set, until the maximum number for the set is reached. After that, the oldest replica in the set is replaced, maintaining the maximum number of replicas in the set.

See also **replica** and **replica set**.

restore session

A process that copies data from backup media to a client.

RMAN (*Oracle specific term*)

See **Recovery Manager**.

RSM

The Data Protector Restore Session Manager controls the restore session. This process always runs on the Cell Manager system.

RSM (*Windows specific term*)

Removable Storage Manager (RSM) includes a media management service that facilitates communication among applications, robotic changers, and media libraries. It enables multiple applications to share local robotic media libraries and tape or disk drives and to manage removable media.

SAPDBA (*SAP R/3 specific term*)

An SAP R/3 user interface that integrates the BRBACKUP, BRARCHIVE, and BRRESTORE tools.

scan

A function that identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library).

scanning

A function which identifies the media in a device. This synchronizes the MMDB with the media that are actually present at the selected locations (for example, slots in a library). It is useful to perform a scan and check the actual media in the

Glossary

device if someone has manually manipulated media without using Data Protector to eject or enter, for example.

Scheduler

A function that controls when and how often automatic backups occur. By setting up a schedule, you automate the start of backups.

Secondary Volume (S-VOL) (*HP StorageWorks Disk Array XP specific term*)

Secondary Volumes, or S-VOLs, are XP LDEVs that act as a secondary CA or BC mirror of another LDEV (a P-VOL). In the case of CA, S-VOLs can be used as failover devices in a MetroCluster configuration. The S-VOLs are assigned separate SCSI addresses, different from the addresses used by the P-VOLs. *See also* **Primary Volume (P-VOL)**.

session

See **backup session, media management session, and restore session**.

session ID

An identifier of a backup, restore, object copy, or media management session, consisting of the date when the session ran and a unique number.

session key

This environment variable for the Pre- and Post-exec script is a Data Protector

unique identification of any session, including preview sessions. The session key is not recorded in the database, and it is used for specifying options for the omnimnt, omnistat and omniabort CLI commands.

shadow copy (*MS VSS specific term*)

A volume that represents a duplicate of the original volume at a certain point in time. The data is then backed up from the shadow copy and not from the original volume. The original volume continues to change as the backup process continues, but the shadow copy of the volume remains constant.

See also **Microsoft Volume Shadow Copy service**.

shadow copy provider (*MS VSS specific term*)

An entity that performs the work on creating and representing the volume shadow copies. Providers own the shadow copy data and expose the shadow copies. Providers can be software (for example, system providers) or hardware (local disks, disk arrays).

See also **shadow copy**.

shadow copy set (*MS VSS specific term*)

A collection of shadow copies created at the same point in time.

See also **shadow copy**.

Glossary

shared disks

A Windows disk on another system that has been made available to other users on the network. Systems with shared disks can be backed up without a Data Protector Disk Agent installed.

SIBF

The Serverless Integrations Binary Files (SIBF) is a part of the IDB that stores raw NDMP meta data. This data is necessary to perform restore of NDMP objects.

Site Replication Service (*Microsoft Exchange Server 2000/2003 specific term*)

The Microsoft Exchange Server 2000/2003 service that permits compatibility with Microsoft Exchange Server 5.5 by emulating the Exchange Server 5.5 directory service.

See also **Information Store** and **Key Management Service**.

slot

A mechanical position in a library. Each slot can hold a medium, such as a DLT tape. Data Protector references each slot with a number. To read a medium, a robotic mechanism moves the medium from a slot into the drive.

SMB

See **split mirror backup**.

SMBF

The Session Messages Binary Files (SMBF) part of the IDB stores session messages generated during backup, object copy, restore, and media management sessions. One binary file is created per session. The files are grouped by year and month.

snapshot (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

A form of replica produced using snapshot creation techniques. A range of snapshot types is available, with different characteristics, depending on the arrays/techniques used. Such replicas are dynamic and may be either virtual copies, still reliant upon the contents of the source volumes, or independent exact duplicates (clones), depending on the snapshot type and the time since creation.

See also **replica** and **snapshot creation**.

snapshot backup (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

snapshot creation (*HP StorageWorks VA and HP StorageWorks EVA specific term*)

A replica creation technique, in which copies of source volumes are created using storage virtualization techniques. The replicas are considered to be created

Glossary

at one particular point-in-time, without pre-configuration, and are immediately available for use. However background copying processes normally continue after creation.

See also **snapshot**.

source (R1) device (*EMC Symmetrix specific term*)

An EMC Symmetrix device that participates in SRDF operations with a target (R2) device. All writes to this device are mirrored to a target (R2) device in a remote EMC Symmetrix unit. An R1 device must be assigned to an RDF1 group type.

See also **target (R2) device**.

source volume (*ZDB specific term*)

A storage volume containing data to be replicated.

sparse file A file that contains data with portions of empty blocks. Examples are:
-A matrix in which some or much of the data contains zeros
-files from image applications
-high-speed databases
If sparse file processing is not enabled during restore, it might be impossible to restore this file.

split mirror (*EMC Symmetrix and HP StorageWorks Disk Array XP specific term*)

A replica created using split mirror techniques. Such a replica provides an independent, exact duplicate, or clone,

of the contents of the source volumes.

See also **replica** and **split mirror creation**.

split mirror backup (*EMC Symmetrix specific term*)

See **ZDB to tape**.

split mirror backup (*HP StorageWorks Disk Array XP specific term*)

See **ZDB to tape**, **ZDB to disk**, and **ZDB to disk+tape**.

split mirror creation (*EMC Symmetrix and HP StorageWorks Disk Array XP specific term*)

A replica creation technique, in which a pre-configured set of target volumes (a mirror) is kept synchronized with a set of source volumes until the time at which a replica of the contents of the source volumes is required. Then, the synchronization is stopped (the mirror is split) and a split mirror replica of the source volumes at the time of the split remains in the target volumes.

See also **split mirror**.

split mirror restore (*EMC Symmetrix and HP StorageWorks Disk Array XP specific term*)

A process in which data backed up in a ZDB-to-tape or a ZDB-to-disk+tape session is restored from tape media to a split mirror replica, which is then synchronized to the source volumes. Individual backup objects or complete

Glossary

sessions can be restored using this method.

See also **ZDB to tape, ZDB to disk+tape, and replica.**

sqlhosts file (*Informix specific term*)

An Informix connectivity-information file that contains the names of each of the database servers and any aliases to which the clients on a host computer can connect.

SRD file

The Data Protector System Recovery Data (SRD) file contains system information required for installing and configuring the operating system in case of a disaster. The SRD file is an ASCII file, generated when a CONFIGURATION backup is performed on a Windows client and stored on the Cell Manager.

SRDF (*EMC Symmetrix specific term*)

The EMC Symmetrix Remote Data Facility is a business continuation process that enables effective, real-time data replication of SLDs between dislocated processing environments. These environments could be situated within the same root computer environment or separated by long distances.

SSE Agent (*HP StorageWorks Disk Array XP specific term*)

A Data Protector software module that

executes all tasks required for a split mirror backup integration. It communicates with the HP StorageWorks Disk Array XP storing system using the RAID Manager XP utility (HP-UX and Windows systems) or RAID Manager Library (Solaris systems).

sst.conf file

The file `/usr/kernel/drv/sst.conf` is required on each Data Protector Sun Solaris client to which a multi-drive library device is connected. It must contain an entry for the SCSI address of the robotic mechanism of each library device connected to the client.

st.conf file

The file `/kernel/drv/st.conf` is required on each Data Protector Solaris client with a backup device connected. It must contain device information and a SCSI address for each backup drive connected to that client. A single SCSI entry is required for a single-drive device and multiple SCSI entries are required for a multi-drive library device.

stackers

Devices with multiple slots for media storage usually with only one drive. A stacker selects media from the stack sequentially. In contrast, a library can randomly select media from its repository.

Glossary

standalone file device

A file device is a file in a specified directory to which you back up data.

standard security (*MS SQL specific term*)

Standard security uses the login validation process of the Microsoft SQL Server for all connections. Standard security is useful in network environments with a variety of clients, some of which may not support trusted connections. It also provides backward compatibility for older versions of the Microsoft SQL Server.

See also **integrated security**.

Storage Group

(*Microsoft Exchange Server 2000/2003 specific term*)

A collection of databases (stores) that share a common set of transaction log files. Exchange manages each storage group with a separate server process.

StorageTek ACS library

(*StorageTek specific term*)

Automated Cartridge System is a library system (also known as Silo) consisting of one Library Management Unit (LMU) and one to 24 Library Storage Modules (LSM) connected to the unit.

storage volume (*ZDB specific term*)

A storage volume represents an object that may be presented to an operating system or some other entity (for

example, a virtualization mechanism) upon which volume management systems, file systems, or other objects may exist. The volume management systems, file systems are built on this storage. Typically, these can be created or exist within a storage system such as a disk array.

switchover

See **failover**

Sybase Backup Server API (*Sybase specific term*)

An industry-standard interface developed for the exchange of backup and recovery information between a Sybase SQL Server and a backup solution like Data Protector.

Sybase SQL Server (*Sybase specific term*)

The server in the Sybase “client-server” architecture. Sybase SQL Server manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

Symmetrix Agent (SYMA) (*EMC Symmetrix specific term*)

The Data Protector software module that prepares the EMC Symmetrix environment for backup and restore operations.

Glossary

System Backup to Tape (*Oracle specific term*)

An Oracle interface that handles the actions required to load, label, and unload correct backup devices when Oracle issues a backup or restore request.

system databases (*Sybase specific term*)

The four system databases on a newly installed Sybase SQL Server are the:

- master database (master)
- temporary database (tempdb)
- system procedure database (sybssystemprocs)
- model database (model).

system disk

A system disk is a disk containing operating system files. Microsoft terminology defines the system disk as a disk containing the files required for initial step of boot process.

system partition

A system partition is a partition containing operating system files. Microsoft terminology defines a system partition as a partition containing the files required for initial step of boot process.

System State (*Windows specific term*)

The System State data comprises the Registry, COM+ Class Registration database, system startup files, and the Certificate Services database (if the server is a certificate server). If the server is a domain controller, Active Directory directory services and the Sysvol directory are also contained in the System State data. If the server is running the Cluster service, the System State data also includes resource registry checkpoints and the quorum resource recovery log, which contains the most recent cluster database information.

system volume/disk/partition

A volume/disk/partition containing operating system files. Microsoft terminology defines the system volume/disk/partition as the volume/disk/partition containing files required for the initial step of the boot process.

SysVol (*Windows specific term*)

A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

tablespace

A part of a database structure. Each database is logically divided into one or more tablespaces. Each tablespace has data files or raw volumes exclusively associated with it.

Glossary

tapeless backup (*ZDB specific term*)
See **ZDB to disk**.

target database (*Oracle specific term*)
In RMAN, the target database is the database that you are backing up or restoring.

target (R2) device (*EMC Symmetrix specific term*)
An EMC Symmetrix device that participates in SRDF operations with a source (R1) device. It resides in the remote EMC Symmetrix unit. It is paired with a source (R1) device in the local EMC Symmetrix unit and receives all write data from its mirrored pair. This device is not accessed by user applications during normal I/O operations. An R2 device must be assigned to an RDF2 group type.
See also **source (R1) device**

target system (*Disaster Recovery specific term*)
A system after a computer disaster has occurred. The target system is typically in a non-bootable state and the goal of disaster recovery is to restore this system to the original system configuration. The difference between a crashed system and a target system is that a target system has all faulty hardware replaced.

target volume (*ZDB specific term*)
A storage volume to which data is replicated.

Terminal Services (*Windows specific term*)
Windows Terminal Services provide a multi-session environment that allows clients to access a virtual Windows desktop session and Windows-based programs running on the server.

thread (*MS SQL Server 7.0/2000 specific term*)
An executable entity that belongs to only one process. It comprises a program counter, a user-mode stack, a kernel-mode stack, and a set of register values. Several threads can run at a time within one process.

TimeFinder (*EMC Symmetrix specific term*)
A business continuation process that creates an instant copy of single or multiple Symmetrix Logical Devices (SLDs). The instant copy is created on specially preconfigured SLDs called BCVs and is accessible via a separate device address to the system(s).

TLU
Tape Library Unit.

TNSNAMES.ORA (*Oracle and SAP R/3 specific term*)
A network configuration file that

Glossary

contains connect descriptors mapped to service names. The file may be maintained centrally or locally, for use by all or individual clients.

transaction

A mechanism for ensuring that a set of actions is treated as a single unit of work. Databases use transactions to keep track of database changes.

transaction backup

Transaction backups generally use fewer resources than database backups, so they can be created more frequently than database backups. By applying transaction backups, you can recover the database to a specific point in time prior to when a problem occurred.

transaction backup (*Sybase and SQL specific term*)

A backup of the transaction log providing a record of changes made since the last full or transaction backup.

transaction log backup

Transaction log backups generally use fewer resources than database backups so they can be created more frequently than database backups. By applying transaction log backups, you can recover the database to a specific point in time.

transaction log files

Files that record transactions of the database modifications, and provide fault tolerance in case of a database disaster.

transaction logs (*Data Protector specific term*)

Keeps track of IDB changes. The archiving of transaction logs should be enabled to prevent you from losing the transaction log files that are created after the last IDB backup and are necessary for IDB recovery.

transaction log table (*Sybase specific term*)

A system table in which all changes to the database are automatically recorded.

transportable snapshot (*MS VSS specific term*)

A shadow copy that is created on the application system and can be presented to the backup system which performs the backup.

See also **Microsoft Volume Shadow Copy service (VSS)**.

TSANDS.CFG file (*Novell NetWare specific term*)

A file that allows you to specify the names of containers where you want backups to begin. It is text file located in the SYS:SYSTEM\TSA directory on the server where TSANDS.NLM is loaded.

Glossary

unattended operation

See lights-out operation.

user account

You can use Data Protector only if you have a Data Protector user account, which restricts unauthorized access to Data Protector and to backed up data. Data Protector administrators create this account specifying a user logon name, the systems from which the user can log on, and a Data Protector user group membership. This is checked whenever the user starts the Data Protector user interface or performs specific tasks.

user disk quotas

NTFS quota-management support enables an enhanced tracking mechanism and control over disk space usage on shared storage volumes. Data Protector backs up user disk quotas on the whole system and for all configured users at a time.

user group

Each Data Protector user is member of a User Group. Each User Group has a set of user rights that are given to every user in that User Group. The number of User Groups with their associated user rights can be defined as desired. Data Protector provides three default user groups: admin, operator, and user.

user profile (*Windows specific term*)

Configuration information retained on a user basis. This information includes desktop settings, screen colors, network connections, and so on. When the user logs on, the user profile is loaded and the Windows environment is set accordingly.

user rights

User rights or access rights are the permissions needed to perform specific Data Protector tasks. Configuring a backup, starting a backup session, or starting a restore session are typical user rights. Users have the access rights of the user group to which they belong.

vaulting media

The process of storing media to a safe and remote place. The media are brought back to the data center when they are needed for restore or are ready for reuse in subsequent backups. The vaulting procedure depends on your company's backup strategy and policies for data protection/reliability.

VBFS (*OmniStorage specific term*)

A Very Big File System is an extension of the standard HP-UX file system on HP-UX 9.x. It is mounted to a directory the same way as any HP-UX file system. In a VBFS, only the superblock, the inode and the 'extended attribute'

Glossary

information remain permanently on the hard disk and are never migrated.
See also **MFS**.

verify

A function that lets you check whether the Data Protector data on a specified medium is readable. Additionally, consistency within each block can be checked if the backup was performed with the cyclic redundancy check (CRC) option ON.

Virtual Controller Software (VCS)

(HP StorageWorks EVA specific term)

The firmware that manages all aspects of storage system operation, including communication with Command View EVA through the HSV controllers.
See also **Command View (CV) EVA**.

Virtual Device Interface (MS SQL Server 7.0/2000 specific term)

This is a SQL Server 7.0/2000 programming interface that allows fast backup and restore of large databases.

virtual disk (HP StorageWorks EVA specific term)

A unit of storage allocated from an HP StorageWorks Enterprise Virtual Array storage pool. Virtual disks are the entities that are replicated using the HP StorageWorks Enterprise Virtual Array

snapshot functionality.

See also **source volume** and **target volume**.

virtual server

A virtual machine in a cluster environment defined in a domain by a network IP name and address. Its address is cached by the cluster software and mapped to the cluster node that is currently running the virtual server resources. This way all requests for a particular virtual server are cached by a specific cluster node.

volser (ADIC and STK specific term)

A VOLume SERial number is a label on the medium to identify the physical tape used in very large libraries. A volser is a naming convention specific to ADIC/ GRAU and StorageTek devices.

volume group

A unit of data storage in an LVM system. A volume group can consist of one or more physical volumes. There can be more than one volume group on the system.

volume mountpoint (Windows specific term)

An empty directory on a volume that can be used to mount another volume. The volume mount point acts as a gateway to the target volume. Provided that the volume is mounted, users and applications can refer to the data on the

Glossary

mounted volume by the full (merged) filesystem path as if both volumes are one integral part.

Volume Shadow Copy service

See **Microsoft Volume Shadow Copy service**.

VPO

See **OVO**.

VSS

See **Microsoft Volume Shadow Copy service**.

VxFS

Veritas Journal Filesystem.

VxVM (Veritas Volume Manager)

A Veritas Volume Manager is a system for managing disk space on Solaris platforms. A VxVM system consists of an arbitrary group of one or more physical volumes organized into logical disk groups.

Wake ONLAN

Remote power-up support for systems running in power-save mode from some other system on the same LAN.

Web reporting

The Data Protector functionality that allows you to view reports on backup status and Data Protector configuration using the Web interface.

wildcard character

A keyboard character that can be used to represent one or many characters. The asterisk (*), for example, typically represents one or more characters, and the question mark (?) typically represents a single character. Wildcard characters are often used in operating systems as a means of specifying more than one file by name.

Windows CONFIGURATION backup

Data Protector allows you to back up Windows CONFIGURATION, including Windows Registry, user profiles, Event Logs, and WINS and DHCP server data (if configured on a system) in one step.

Windows Registry

A centralized database used by Windows to store configuration information for the operating system and the installed applications.

WINS server A system running Windows Internet Name Service software that resolves Windows networking computer names to IP addresses. Data Protector can back up WINS server data as part of the Windows configuration.

Glossary

writer

(MS VSS specific term)

A process that initiates change of data on the original volume. Writers are typically applications or system services that write persistent information on a volume. Writers also participate in the shadow copy synchronization process by assuring data consistency.

XBSA interface *(Informix specific term)*

The onbar utility and Data Protector communicate with each other through the X/Open Backup Specification Services Programmer's Interface (XBSA).

XCopy engine *(direct backup specific term)*

A SCSI-3 copy command that allows you to copy data from a storage device having a SCSI source address to a backup device having a SCSI destination address, thus enabling direct backup. The data flows from a source device (either block or streaming, that is, disk or tape) to the destination device (either block or streaming) through XCopy. This releases the controlling server of reading the data from the storage device into memory and then writing the information to the destination device.

See also **direct backup**.

ZDB

See **zero downtime backup (ZDB)**.

ZDB database *(ZDB specific term)*

A part of the IDB, storing ZDB related information such as source volumes, replicas and security information. The ZDB database is used for ZDB, instant recovery, and split mirror restore.

See also **zero downtime backup (ZDB)**.

ZDB to disk *(ZDB specific term)*

A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time. Multiple replicas, produced using the same backup specification at different times, can be kept in a replica set. A replica from ZDB to disk can be restored using the instant recovery process.

See also **zero downtime backup (ZDB)**, **ZDB to tape**, **ZDB to disk+tape**, **instant recovery**, and **replica set rotation**.

ZDB to disk+tape *(ZDB specific term)*

A form of zero downtime backup where the replica produced is kept on the disk array as a backup of the source volumes at a specific point in time, in the same way as with ZDB to disk. However, data in the replica is also streamed to a backup medium, as with ZDB to tape. If this backup method is used, data backed up in the same session can be restored

Glossary

using the instant recovery process, the standard Data Protector restore from tape, or on split mirror arrays, split mirror restore.

See also **zero downtime backup (ZDB), ZDB to disk, ZDB to tape, instant recovery, replica, and replica set rotation.**

ZDB to tape (*ZDB specific term*)

A form of zero downtime backup where data in the replica produced is streamed to a backup medium, typically tape. Instant recovery is not possible from such a backup, so the replica need not be retained on the disk array after backup completion. The backed-up data can be restored using standard Data Protector restore from tape. On split mirror arrays, split mirror restore can also be used.

See also **zero downtime backup (ZDB), ZDB to disk, instant recovery, ZDB to disk+tape, and replica.**

zero downtime backup (ZDB)

A backup approach in which data replication techniques, provided by a disk array, are used to minimize the impact of backup operations on an application system. A replica of the data to be backed up is created first. All subsequent backup operations are performed on the replicated data rather than the original data, while the application system can be returned to normal operation.

See also **ZDB to disk, ZDB to tape, ZDB to disk+tape, and instant recovery.**

A

- advantages
 - DB2 integration, 106
 - Informix integration, 4
 - Lotus integration, 158
- architecture
 - DB2 integration, 114
 - Informix integration, 7
 - Lotus integration, 162
- archive logging
 - DB2 integration, 111
 - Lotus integration, 167
- archive logs backup
 - DB2 integration, 128

B

- backing up DB2, 128–133
 - archive logs backup, 118, 128
 - backup flow, 112
 - backup methods, 128
 - backup modes, 128
 - backup options, 124
 - backup problems, 150
 - backup specification, creating, 118
 - backup types, 105
 - database objects backup, 118
 - delta backup, 112
 - full backup, 112
 - incremental backup, 112, 129
 - incremental delta backup, 129
 - interactive backup, 131
 - scheduled backup, 129
 - scheduled backup, example, 130
 - starting interactive backup, using CLI, 132
 - starting interactive backup, using GUI, 131
 - temporary table spaces, 128
- backing up Informix, 51–64
 - backup flow, 8
 - backup methods, 51
 - backup modes, 61
 - backup options, 39
 - backup owner, configuring, 17
 - backup problems, UNIX, 91
 - backup problems, Windows, 82
 - backup specification, creating, 32
 - backup types, 3, 41, 51, 58
 - configuration files, 61
 - continuous backup, 63
 - database backup, 51

- full backup, 3, 51
- incremental backup, 3, 51
- interactive backup using CLI, 57
- interactive backup using GUI, 56
- interactive backup using Informix
 - commands, 59
- interactive backup using the log_full.sh
 - script, 62
- onbar utility, 61
- on-demand backup, 63
- online mode, 61
- quiescent mode, 61
- scheduled backup, 54
- scheduled backup, example, 55
- starting interactive backup, using CLI, 57
- starting interactive backup, using GUI, 56
- starting interactive backup, using Informix
 - commands, 59
 - starting interactive backup, using Informix log_full.sh, 62
- backing up Lotus, 176–187
 - backup flow, 161
 - backup options, 183
 - backup problems, 204
 - backup specification, creating, 178
 - backup types, 158
 - BOX files, 176
 - full backup, 158
 - incremental backup, 158
 - interactive backup, 186
 - Notes Storage Facility files, 176
 - Notes Template Facility files, 176
 - scheduled backup, 185
 - transaction log files, 176
- backup flow
 - DB2 integration, 112
 - Informix integration, 8
 - Lotus integration, 161
- backup methods
 - DB2 integration, 128
 - Informix integration, 51
- backup modes
 - DB2 integration, 128
 - Informix integration, 61
- backup options
 - DB2 integration, 124
 - Informix integration, 39
 - Lotus integration, 183
- backup problems

Index

- DB2 integration, 150
- Informix integration, UNIX, 91
- Informix integration, Windows, 82
- Lotus integration, 204
- backup specification
 - DB2 integration, creating, 118
 - DB2 integration, scheduling, 129
 - Informix integration, creating, 32
 - Informix integration, scheduling, 54
 - Lotus integration, creating, 178
 - Lotus integration, scheduling, 185
- backup templates
 - DB2 integration, 118
- backup types
 - DB2 integration, 105
 - Informix integration, 3, 41, 51, 58
 - Lotus integration, 158
- BOX files
 - Lotus integration, 176
- C**
- checking
 - Informix configuration, 28
 - Lotus configuration, 171, 173
- circular logging
 - DB2 integration, 110
 - Lotus integration, 167
- concepts
 - DB2 integration, 109
 - Informix integration, 7
 - Lotus integration, 161
- configuration problems
 - Lotus integration, 202
- configuring DB2, 115–127
 - backup, 117
 - backup specification, 118
 - backup templates, 118
 - instances, 116
 - overview, 115
 - prerequisites, 115
 - users, 115
- configuring Informix, 13–46
 - backup owner, 17
 - backup specification, 32
 - checking configuration, 28
 - configuration options, 20
 - Informix configuration file, 9–12
 - Informix Enterprise Decision Server (EDS), 45

- OnLine Server, 19
 - overview, 13
 - users, 16, 18
 - users, changing, 40
- configuring Lotus, 164–175
 - archive logging, 167
 - backup, 177
 - backup specification, 178
 - checking configuration, 171, 173
 - configuration problems, 202
 - examples, 169
 - global configuration file, 168
 - linking library, 170
 - overview, 164
 - server specific configuration file, 168
 - transaction logging, 164, 166
 - users, 170
 - using CLI, 172
 - using GUI, 171
- conventions, ix
- creating
 - DB2 backup specification, 118
 - Informix backup specification, 32
 - Lotus backup specification, 178
- D**
- DB2 backup, 128–133
 - archive logs backup, 118, 128
 - backup flow, 112
 - backup methods, 128
 - backup modes, 128
 - backup options, 124
 - backup problems, 150
 - backup specification, creating, 118
 - backup types, 105
 - database objects backup, 118
 - delta backup, 112
 - full backup, 112
 - incremental backup, 112, 129
 - incremental delta backup, 129
 - interactive backup, 131
 - modification tracking, 129
 - scheduling, 129
 - scheduling, example, 130
 - starting interactive backup, using CLI, 132
 - starting interactive backup, using GUI, 131
 - temporary table spaces, 128
- DB2 configuration, 115–127
 - backup, 117

- backup specification, 118
- backup templates, 118
- instances, 116
- overview, 115
- prerequisites, 115
- users, 115
- DB2 integration
 - advantages, 106
 - architecture, 114
 - archive logging, 111
 - backing up DB2, 128–133
 - circular logging, 110
 - concepts, 109
 - configuring DB2, 115–127
 - disaster recovery, 111
 - limitations, 108
 - monitoring sessions, 146
 - overview, 105
 - prerequisites, 107
 - recovery methods, rollforward recovery, 111
 - recovery methods, version recovery, 110
 - restoring DB2, 134–145
 - testing, using CLI, 127
 - testing, using GUI, 126
 - troubleshooting DB2, 149–153
 - util_cmd, 143
 - viewing sessions, 147
- DB2 restore, 134–145
 - examples, 142, 143, 145
 - into a new database, 142
 - restore options, 140
 - restore problems, 152
 - restore types, 105, 112
 - to another instance, 144
 - using CLI, 141
 - using GUI, 135
- DB2 troubleshooting, 149–153
 - backup problems, 150
 - restore problems, 152
- delta backup
 - DB2 integration, 112
- disaster recovery
 - DB2 integration, 111
 - Informix integration, 78
- E**
- examples
 - DB2 integration, online restore, 142
 - DB2 integration, scheduling, 130
 - DB2 restore, 143, 145
 - Informix configuration file, 10
 - Informix integration, backup, 59
 - Informix integration, restoring using onbar, 75
 - Informix integration, scheduling, 55
 - Informix integration, testing, 49
 - Informix integration, testing backup specification, 83
 - Lotus integration, creating soft links, 170
 - Lotus integration, global configuration file, 169
 - Lotus integration, server specific configuration f, 169
 - Lotus restore, 192
- F**
- full backup
 - DB2 integration, 112
 - Informix integration, 3, 51
 - Lotus integration, 158
- I**
- incremental backup
 - DB2 integration, 112, 129
 - Informix integration, 3, 51, 59
 - Lotus integration, 158
- incremental delta backup
 - DB2 integration, 129
- Informix backup, 51–64
 - backup flow, 8
 - backup methods, 51
 - backup modes, 61
 - backup options, 39
 - backup owner, configuring, 17
 - backup problems, UNIX, 91
 - backup problems, Windows, 82
 - backup specification, creating, 32
 - backup types, 3, 41, 51, 58
 - configuration files, 61
 - continuous backup, 63
 - database backup, 51
 - full backup, 3, 51
 - incremental backup, 3, 51
 - interactive backup using CLI, 57
 - interactive backup using GUI, 56
 - interactive backup using Informix commands, 59

- interactive backup using the `log_full.sh` script, 62
- onbar utility, 61
- on-demand backup, 63
- online mode, 61
- quiescent mode, 61
- scheduling, 54
- scheduling, example, 55
- starting interactive backup, using CLI, 57
- starting interactive backup, using GUI, 56
- starting interactive backup, using Informix commands, 59
- starting interactive backup, using Informix `log_full.sh`, 62
- Informix configuration, 13–46
 - backup owner, 17
 - backup specification, 32
 - checking configuration, 28
 - configuration options, 20
 - Informix configuration file, 9–12
 - Informix Enterprise Decision Server (EDS), 45
 - OnLine Server, 19
 - overview, 13
 - users, 16, 18
 - users, changing, 40
- Informix integration
 - advantages, 4
 - architecture, 7
 - backing up, 51
 - backing up Informix, 51–64
 - concepts, 7
 - configuring Informix, 13–46
 - disaster recovery, 78
 - Informix configuration file, 9–12
 - limitations, 6
 - monitoring sessions, 79
 - onbar utility, 4
 - overview, 3
 - prerequisites, 6
 - restoring Informix, 65–78
 - testing, 47
 - troubleshooting Informix, 81–102
 - troubleshooting Informix, UNIX, 89–102
 - troubleshooting Informix, Windows, 81–89
 - `util_cmd`, 10
 - viewing sessions, 80
 - whole-system backup, 41
 - XBSA interface, 8
- Informix restore, 65–78
 - finding information for restore, CLI, 66
 - finding information for restore, GUI, 68
 - restore flow, 8
 - restore options, 71
 - restore problems, UNIX, 99
 - restore problems, Windows, 87
 - to another client, 76
 - using another device, 77
 - using GUI, 69
 - using Informix commands, 73
 - using Informix commands, examples, 75
- Informix troubleshooting, 81–102
 - backup problems, UNIX, 91
 - backup problems, Windows, 82
 - cluster, UNIX, 89
 - cluster, Windows, 81
 - configuration, UNIX, 89
 - configuration, Windows, 81
 - restore problems, UNIX, 99
 - restore problems, Windows, 87
 - UNIX, 89–102
 - Windows, 81–89
- instances
 - DB2 integration, configuring, 116
 - Informix integration, 9
- interactive backup
 - DB2 integration, 131, 132
 - Informix integration, using CLI, 57
 - Informix integration, using GUI, 56
 - Informix integration, using Informix commands, 59
 - Informix integration, using the `log_full.sh` script, 62
 - Lotus integration, 186
- L**
 - limitations
 - DB2 integration, 108
 - Informix integration, 6
 - linking library
 - Lotus integration, 170
 - Lotus backup, 176–187
 - backup flow, 161
 - backup options, 183
 - backup problems, 204
 - backup specification, creating, 178
 - backup types, 158
 - BOX files, 176

- full backup, 158
 - incremental backup, 158
 - interactive backup, 186
 - Notes Storage Facility files, 176
 - Notes Template Facility files, 176
 - scheduling, 185
 - transaction log files, 176
 - Lotus configuration, 164–175
 - archive logging, 167
 - backup, 177
 - backup specification, 178
 - checking, 171, 173
 - configuration problems, 202
 - examples, 169
 - global configuration file, 168
 - linking library, 170
 - overview, 164
 - server specific configuration file, 168
 - transaction logging, 164, 166
 - users, 170
 - using CLI, 172
 - using GUI, 171
 - Lotus integration
 - advantages, 158
 - architecture, 162
 - backing up Lotus, 176–187
 - circular logging, 167
 - concepts, 161
 - configuring Lotus, 164–175
 - monitoring sessions, 195
 - overview, 157
 - prerequisites, 160
 - restoring Lotus, 188–194
 - testing, using CLI, 175
 - testing, using GUI, 174
 - troubleshooting Lotus, 198–212
 - util_notes.exe, 172, 173, 200
 - viewing sessions, 196
 - Lotus restore, 188–194
 - examples, 192
 - restore flow, 162
 - restore options, 192
 - restore problems, 209
 - to new location, 192
 - to original location, 192
 - using GUI, 188
 - Lotus troubleshooting, 198–212
 - backup problems, 204
 - configuration problems, 202
 - restore problems, 209
- M**
- modification tracking
 - DB2 integration, 129
 - monitoring
 - DB2 sessions, 146
 - Informix sessions, 79
 - Lotus sessions, 195
- N**
- Notes Storage Facility files
 - Lotus integration, 176
 - Notes Template Facility files
 - Lotus integration, 176
 - NSF *See* Notes Storage Facility files
 - NTF *See* Notes Template Facility files
- O**
- onbar utility
 - backup, 61
 - Informix integration, 4
 - online backup
 - Informix, 61
 - overview
 - DB2 integration, 105
 - Informix integration, 3
 - Lotus integration, 157
- P**
- prerequisites
 - DB2 integration, 107
 - Informix integration, 6
 - Lotus integration, 160
- Q**
- quiescent backups, 61
- R**
- recovery methods
 - DB2 integration, rollforward recovery, 111
 - DB2 integration, version recovery, 110
 - restore flow
 - DB2 integration, 112
 - Informix integration, 8
 - Lotus integration, 162
 - restore methods
 - Informix, 65
-

Index

restore options
 DB2 integration, 140
 Informix integration, 71
 Lotus integration, 192

restore problems
 DB2 integration, 152
 Informix integration, UNIX, 99
 Informix integration, Windows, 87
 Lotus integration, 209

restore types
 DB2 integration, 105

restoring DB2, 134–145
 examples, 142, 143, 145
 into a new database, 142
 restore flow, 112
 restore options, 140
 restore problems, 152
 restore types, 105
 to another instance, 144
 using CLI, 141
 using GUI, 135

restoring Informix, 65–78
 finding information for restore, CLI, 66
 finding information for restore, GUI, 68
 restore flow, 8
 restore options, 71
 restore problems, UNIX, 99
 restore problems, Windows, 87
 to another client, 76
 using another device, 77
 using GUI, 69
 using Informix commands, 73
 using Informix commands, examples, 75

restoring Lotus, 188–194
 restore flow, 162
 restore options, 192
 restore problems, 209
 to new location, 192
 to original location, 192
 using GUI, 188

rollforward recovery
 DB2 integration, 111

running backup *See* starting backup

S

scheduling backup
 DB2 integration, 129
 Informix integration, 54
 Lotus integration, 185

starting backup
 DB2 integration, interactively, 131, 132
 DB2 integration, using CLI, 132
 DB2 integration, using GUI, 131
 Informix integration, interactively, 56, 57, 59, 62
 Informix integration, using CLI, 57
 Informix integration, using GUI, 56
 Informix integration, using Informix commands, 59
 Informix integration, using Informix `log_full.sh`, 62
 Lotus integration, using GUI, 183

T

temporary table spaces
 DB2 integration, 128

testing
 DB2 integration, using CLI, 127
 DB2 integration, using GUI, 126
 Informix integration, 47
 Lotus integration, using CLI, 175
 Lotus integration, using GUI, 174

transaction log files
 Lotus integration, 176

transaction logging
 Lotus integration, 164, 166

troubleshooting DB2, 149–153
 backup problems, 150
 restore problems, 152

troubleshooting Informix, 81–102
 backup problems, UNIX, 91
 backup problems, Windows, 82
 cluster, UNIX, 89
 cluster, Windows, 81
 configuration, UNIX, 89
 configuration, Windows, 81
 restore problems, UNIX, 99
 restore problems, Windows, 87
 UNIX, 89–102
 Windows, 81–89

troubleshooting Lotus, 198–212
 backup problems, 204
 configuration problems, 202
 restore problems, 209

typographical conventions, ix

U

users

- DB2 integration, configuring, 115
- Informix integration, changing, 40
- Informix integration, configuring, 16, 18
- Lotus integration, configuring, 170
- util_cmd
 - DB2 integration, 143
 - Informix integration, 10
- util_notes.exe
 - Lotus integration, 172, 173, 200

V

- version recovery
 - DB2 integration, 110
- viewing
 - DB2 sessions, 147
 - Informix sessions, 80
 - Lotus sessions, 196

W

- whole-system backup
 - Informix integration, 41

X

- XBSA interface
 - Informix integration, 8

