

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

Edition 2



Manufacturing Part Number: None (PDF-only)

Version b.05.03

January 2004

© Copyright 2003-2004 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 2003-2004 Hewlett-Packard Development Company, L.P., all rights reserved.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel386, Intel80386, Intel486, and Intel80486 are U.S. trademarks of Intel Corporation.

Intel Itanium™ Logo: Intel, Intel Inside and Itanium are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries and are used under license.

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

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

MS-DOS® is a U.S. registered trademark of Microsoft Corporation.

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

OpenView® is a registered U.S. trademark of Hewlett-Packard Company.

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

OSF, OSF/1, OSF/Motif, Motif, and Open Software Foundation are trademarks of the Open Software Foundation in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of the Open Group.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

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

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Contents

1. Introduction

About Data Protector	17
Data Protector Architecture	21
Operations in the Cell	23
Backup Sessions	24
Restore Sessions	25
Data Protector Enterprise Environments	26
User Interfaces	27
Data Protector GUI	28
About HP OpenView Operations	29
What Is OVO?	29
What Does OVO Do?	31
Performance and Event Management	31
Service Management	32
Node Management	33
Supports SMART Plug-In and Integration Programs	33
About Administrators and Operators	34
Ready-to-Use Policies	35
Ready-to-Use Tools	37
Service Discovery	38
What Are the Main Components?	39
Management Server	39
Management Console	39
Managed Nodes	40
Policies and Agents	40
Putting It All Together	41
Details on How OVO Works	42
Role of the Agent	43
Automatic Commands and Operator-Initiated Commands	43
What Is the Data Protector Integration?	44
Data Protector Integration Architecture	45

Contents

2. Installing the Data Protector Integration

Supported Platforms and Installation Prerequisites	49
Data Protector Supported Versions	49
OVO Management Server System	50
OVO Patches	51
Software Prerequisites on the OVO Management Server	51
Hardware Prerequisites on the OVO Management Server	51
Managed Node Systems (Data Protector Cell Manager)	51
Supported OVO Agent Versions	52
Supported HP OpenView Performance Agent Versions	52
Additional Software for HP-UX Managed Nodes	53
SNMP Emanate Agent (required).	53
Additional Software for Windows Managed Nodes	54
SNMP Service (required).	54
Disk-Space Requirements.	54
Memory (RAM) Requirements	55
Installing the Data Protector Integration	56
Installation	56
Installation Verification	58
Running the Add Data Protector Cell Application	58
Deploy Instrumentation	60
Agent Configuration	60
SNMP Configuration on UNIX	60
SNMP Configuration on Windows	61
Data Protector User Configuration.	64
Miscellaneous Configuration.	64
Program Identification	64
On UNIX Managed Nodes.	64
On Windows Managed Nodes	64
Deinstalling the Data Protector Integration	66
De-configuration tasks	66

Contents

Undeploy All Data Protector Policies from Managed Nodes	66
Remove Data Protector Policies from the OVO Management Server	67
Remove Data Protector User Roles from the OVO Management Server	68
Remove Data Protector Tools and Directory from the OVO Management Server	69
Remove the Data Protector Service Tree from the OVO Management Server	70
Remove Data Protector DP ALL CELLS and DP ALL MGRS Node Directories from the OVO Management Server	71
Remove the Data Protector Integration	71

3. Using the Data Protector Integration

Data Protector SPI Policies	75
Message Groups	76
Message Format	77
Node Groups	78
Tools Groups	80
DP_Reports Tools Group	80
DP_Tools Tools Group	81
Using Tools and Reports	81
Data Protector Service Tree	83
Users and User Roles	86
Data Protector and Operating System Users	86
Data Protector Integration Users	87
OVO User Roles	87
Data Protector OVO User Roles	88
Data Protector OVO Operators	91
Monitored Objects	96
Permanently Running Processes on the Cell Manager	96

Contents

Databases	97
Media Pool Status	98
Media Pool Size	99
Monitor Status of Long Running Backup Sessions	100
Check Important Configuration Files	101
Windows Systems	101
HP-UX Systems	101
Changing Monitor Parameters	102
Monitored Logfiles	104
Data Protector Default Logfiles	104
omnisv.log	104
inet.log	105
Data Protector Database Logfile	106
purge.log	106
Data Protector Media Logfile	107
media.log	107
Logfiles Not Monitored by Data Protector Integration	108
4. Performance Measurement with the HP OpenView Performance Agent	
Integration Overview	111
Installing Performance Integration Components	113
Installation Steps for Window Nodes	113
Installation Steps for UNIX Nodes	114
Collecting ARM Transactions	116
Modifying the parm File	116
Modifying the ttd.conf File	117
Collecting Data Protector Process Data	119
Modifying the parm File on a Data Protector Cell Manager	119
Modifying the parm File on a Data Protector Media Agent	119
Modifying the parm File on a Data Protector Disk Agent	120

Contents

Modifying the parm File on a Data Protector Installation Server . . .	120
Performance Agent Data Source Integration	121
Compiling the obdsi.spec File	121
Collecting Data on Windows Nodes	122
Installing the Data Protector DSI Log Service	122
Starting the Data Protector DSI Log Service	123
Configuring the Data Protector DSI Log Service	125
Deinstalling the Data Protector DSI Log Service	126
Collecting Data on UNIX Nodes	126
Performance Alarms for the Performance Agent	126

5. Reporter Light Integration

Reporter Light Overview	129
Key Features	129
Standard Reports	129
Reporter Light Integration with Data Protector Architecture	131
Data Flow	132
Installing The Reporter Light Integration	133
Installation Verification	133
De-installation	133
Using the Reporter Light Integration with Data Protector	134
Registering a Data Protector Cell Manager with this Module	134
Troubleshooting Registering Cell Managers for Reporting	135
Gathering Data from Data Protector	137
Generating Reports	137
Viewing Reports	137
Preconfigured Reports	139
Session Trend Report	139
Backup Duration Trend	140
Data Backup Trend Report	140
Number of Files Trend	142

Contents

Backup Session Health Overview	142
Operational Error Status	144
Skipped Files Report.	145
On Demand Report - Number of Files, Data Written and Date. . . .	145

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.

First Edition: April 2003

Second Edition: January 2004

Conventions

The following typographical conventions are used in this manual.

Table 1 **Typographical Conventions**

Font Type	What the Font Type Represents	Example
<i>Italic</i>	Book or manual titles, and man page names	See <i>HP OpenView Smart Plug-In for HP-UX and Solaris: Administrator's Reference</i>
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: login <i>your_name</i> where you supply your login name.
	Parameters to a function	The <i>oper_name</i> parameter returns
Bold	New terms	The monitor agent observes...
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the <code>grep</code> command ...
	Function names	Use the <code>opc_connect()</code> function to ...
	File and directory names	<code>/opt/OV/bin/OpC/</code>
	Process names	Check to see if <code>opcmona</code> is running.
	Window/dialog box names	In the Add Logfile window...
Computer Bold	Text that you must enter	At the prompt, type: <code>ls -l</code>
Keycap	Keyboard keys and Buttons on the user interface.	Press Return Click Operator Click the Apply button

Table 1 **Typographical Conventions (Continued)**

Font Type	What the Font Type Represents	Example
Menu Items	A menu name followed by a colon (:), means select the menu, then the item. When the item is followed by an arrow (→), a cascading menu follows.	Select Actions: → Utilities → Reports...

1 Introduction

This chapter provides an overview of:

- HP OpenView Storage Data Protector
- HP OpenView Operations
- HP OpenView Storage Data Protector Integration

If you are familiar with HP OpenView Storage Data Protector and HP OpenView Operations you may chose to skip these sections.

The section entitled “What Is the Data Protector Integration?” on page 44 provides a short overview of this product, its key features and its architecture.

About Data Protector

HP OpenView Storage Data Protector is a backup solution that provides reliable data protection and high accessibility for your fast growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. The following list describes major Data Protector features:

- **Scalable and Highly Flexible Architecture**

Data Protector can be used in environments ranging from a single system to thousands of systems on several sites. Due to the network component concept of Data Protector, elements of the backup infrastructure can be placed in the topology according to user requirements. The numerous backup options and alternatives to setting up a backup infrastructure allow the implementation of virtually any configuration you want.

- **Easy Central Administration**

Through its easy-to-use graphical user interface (GUI), Data Protector allows you to administer your complete backup environment from a single system. To ease operation, the GUI can be installed on various systems to allow multiple administrators to access Data Protector via their locally installed consoles. Even multiple backup environments can be managed from a single system. The Data Protector command-line interface allows you to manage Data Protector using scripts.

- **High Performance Backup**

Data Protector allows you to back up to several hundred backup devices simultaneously. It supports high-end devices in very large libraries. Various types of backups, such as local, network, full, differential, leveled incremental, online, disk image, and built-in support of parallel data streams, allow you to tune your backups to best fit your requirements.

- **Supporting Mixed Environments**

As Data Protector supports heterogeneous environments, most features are common to the UNIX and Windows platforms. The HP-UX, Solaris and Windows Cell Managers can control all

supported client platforms (UNIX, Windows NT, Windows 2000, Windows XP Professional, Windows Server 2003, and Novell NetWare). The Data Protector user interface can access the entire Data Protector functionality on all supported platforms.

- **Easy Installation for Mixed Environments**

The Installation Server concept simplifies the installation and upgrade procedures. To remotely install UNIX clients, you need an Installation Server running HP-UX or Solaris. To remotely install Windows clients, you need an Installation Server running Windows NT, Windows 2000, Windows XP Professional, or Windows Server 2003. The remote installation can be performed from any client with an installed Data Protector GUI.

- **High Availability Support**

Data Protector enables you to meet the needs for continued business operations around the clock. In today's globally distributed business environment, company-wide information resources and customer service applications must always be available. Data Protector enables you to meet high availability needs by:

- Integrating with clusters (HP-MC/ServiceGuard and Microsoft Cluster Server) to ensure fail-safe operation with the ability to back up virtual nodes.
- Enabling the Data Protector Cell Manager itself to run on a cluster.
- Supporting all popular online database Application Programming Interfaces.
- Integrating with advanced high availability solutions like HP StorageWorks Disk Array XP, HP StorageWorks Virtual Array or EMC Symmetrix.
- Providing various disaster recovery methods for supported Windows and UNIX platforms.

- **Easy Restore**

Data Protector includes an internal database that keeps track of data such as which files from which system are kept on a particular medium. In order to restore any part of a system, browse the files and directories. This provides fast and convenient access to the data to be restored.

- **Automated or Unattended Operation**

With the internal database, Data Protector keeps information about each Data Protector medium and the data on it. Data Protector provides sophisticated media management functionality. For example, it keeps track of how long a particular backup needs to remain available for restoring, and which media can be (re)used for backups.

The support of very large libraries complements this, allowing for unattended operation over several days or weeks (automated media rotation).

Additionally, when new disks are connected to systems, Data Protector can automatically detect (or discover) the disks and back them up. This eliminates the need to adjust backup configurations manually.

- **Service Management**

Data Protector is the first backup and restore management solution to support service management. The integration with Application Response Management (ARM) and Data Source Integration (DSI) enables powerful support of Service Level Management (SLM) and Service Level Agreements (SLA) concepts by providing relevant data to management and planning systems.

- **Monitoring, Reporting and Notification**

Superior web reporting and notification capabilities allow you to easily view the backup status, monitor active backup operations, and customize reports. Reports can be generated using the GUI, or using the `omnirpt` command on systems running UNIX, Windows NT, or Windows 2000, as well as using Java-based online generated web reports.

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.

- **Integration with Online Database Applications**

Data Protector provides online backup of Microsoft Exchange Server 5.5, Microsoft Exchange Server 2000, Microsoft SQL Server 7, Microsoft SQL Server 2000, Oracle7, Oracle8, Informix, SAP R/3, Lotus Domino R5 Server, and Sybase database objects.

- **Integration with Other Products**

Additionally, Data Protector integrates with EMC SRDF and TimeFinder, HP OpenView Operations for UNIX, Microsoft Cluster Server, MC/ServiceGuard, HP OpenView OmniStorage, and other products.

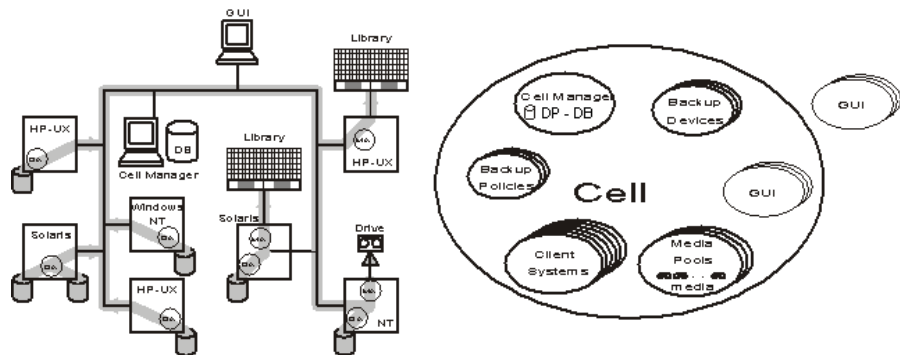
Data Protector Architecture

The Data Protector **cell**, shown in Figure 1-1, is a network environment that has a **Cell Manager**, **client systems**, and **devices**. The Cell Manager is the central control. After installing Data Protector software, you can add systems to be backed up. These systems become Data Protector client systems that are part of the cell. When Data Protector backs up files, it saves them to media in backup devices.

The **Data Protector internal database (IDB)** keeps track of the files you back up so that you can browse and easily recover the entire system or single files.

Data Protector facilitates backup and restore jobs. You can do an immediate (or interactive) backup using the Data Protector user interface. You can also schedule your backups to run unattended.

Figure 1-1 The Data Protector Cell (Physical View and Logical View)



NOTE

The GUI and the Cell Manager systems can run on HP-UX, Solaris, Windows NT, Windows 2000, Windows XP Professional, or Windows Server 2003 operating systems; they do not have to run on the same system nor share the same platform.

Cell Manager

The Cell Manager is the main system in the cell. The Cell Manager:

- Manages the cell from a central point.
- Contains the IDB.

The IDB contains information about backup details such as, backup durations, media IDs, and session IDs.

- Runs core Data Protector software.
- Runs Session Managers that start and stop backup and restore sessions and write session information to the IDB.

Systems to Be Backed Up

Client systems you want to back up must have the Data Protector **Disk Agent** ((DA) also called Backup Agent) installed. To back up online database integrations, install the **Application Agent**. In the rest of the manual, the term Disk Agent will be used for both agents. The Disk Agent reads or writes data from a disk on the system and sends or receives data from the Media Agent. The Disk Agent is also installed on the Cell Manager, thus allowing you to back up data on the Cell Manager, the Data Protector configuration, and the IDB.

Systems with Backup Devices

Client systems with connected backup devices must have the Data Protector Media Agent (MA) installed. Such client systems are also called **Drive Servers**. A backup device can be connected to any system and not only to the Cell Manager. The Media Agent reads or writes data from media in the device and sends or receives data from the Disk Agent.

Systems with a User Interface

You can manage Data Protector from any system on the network on which the Data Protector graphical user interface (GUI) is installed. Therefore, you can have the Cell Manager system in a computer room while managing Data Protector from your desktop system.

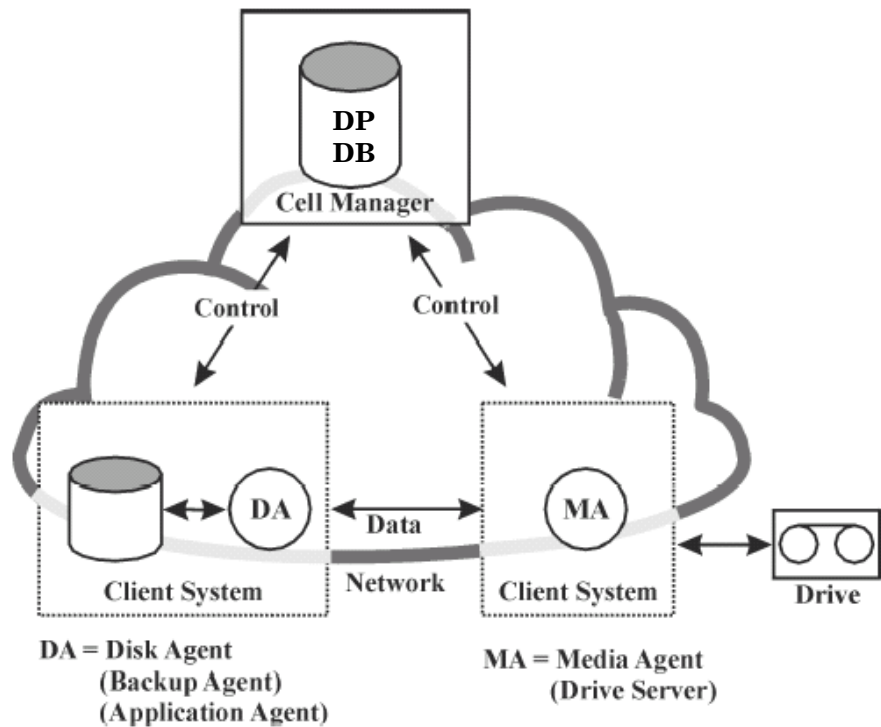
Installation Server

The **Installation Server** holds a repository of the Data Protector software packages for a specific architecture. The Cell Manager is by default also an Installation Server. At least two Installation Servers are needed for mixed environments: one for UNIX systems and one for the Windows systems.

Operations in the Cell

The Data Protector Cell Manager controls backup and restore sessions, which perform all the required actions for a backup or restore, respectively, as shown in Figure 1-2.

Figure 1-2 Backup or Restore Operation



Backup Sessions

What Is a Backup Session?

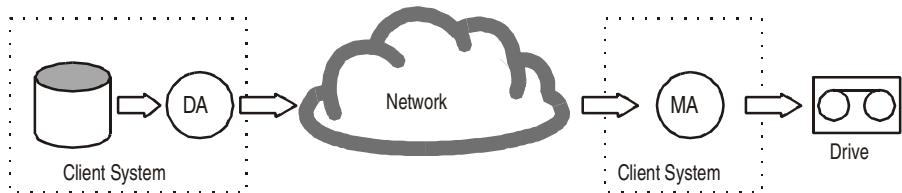
A backup session, shown in Figure 1-3, is a process that creates a copy of data on storage media. It is started either interactively by an operator using the Data Protector user interface, or unattended using the Data Protector Scheduler.

How Does It Work?

The Backup Session Manager process starts Media Agent(s) and Disk Agent(s), controls the session, and stores generated messages to the IDB. Data is read by the Disk Agent and sent to the Media Agent, which saves it to media.

Figure 1-3

Backup Session



A typical backup session is more complex than the one shown in Figure 1-3. A number of Disk Agents read data from multiple disks in parallel and send data to one or more Media Agents. For more information on complex backup sessions, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Restore Sessions

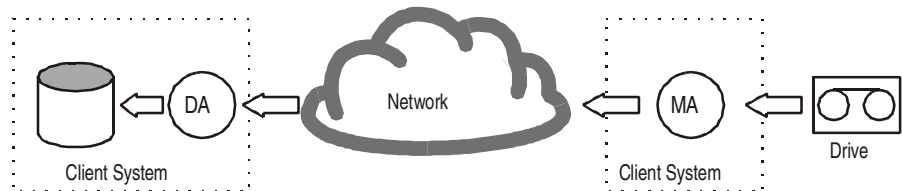
What Is a Restore Session?

A restore session, shown in Figure 1-4, is a process that restores data from previous backups to a disk. The restore session is interactively started by an operator using the Data Protector user interface.

How Does It Work?

After you have selected the files to be restored from a previous backup, you invoke the actual restore. The Restore Session Manager process starts the needed Media Agent(s) and Disk Agent(s), controls the session, and stores messages in the IDB. Data is read by the Media Agent and sent to the Disk Agent, which writes it to disks.

Figure 1-4 Restore Session



A restore session may be more complex than the one shown in Figure 1-4. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for more information on restore sessions.

Data Protector Enterprise Environments

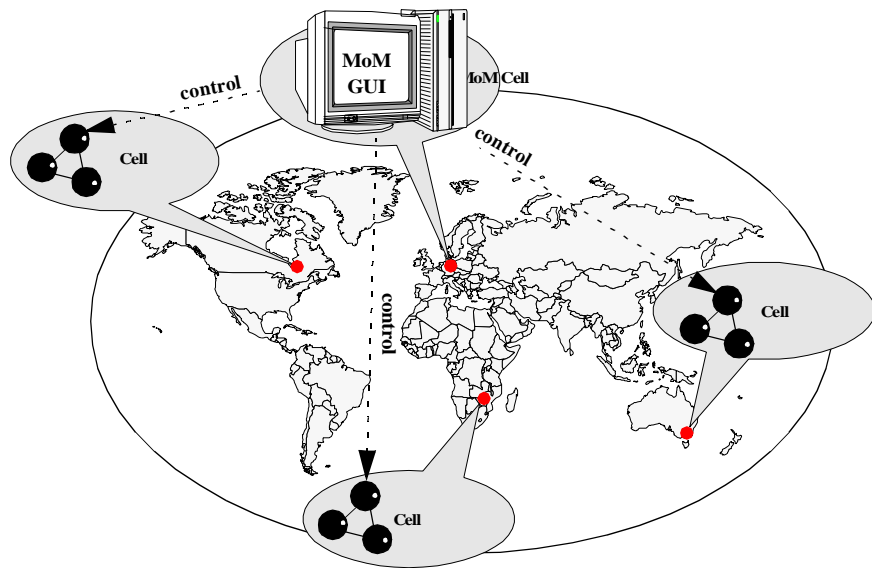
What Is an Enterprise Environment?

A typical enterprise network environment, shown in Figure 1-8, consists of a number of systems from different vendors with different operating systems. The systems may be located in different geographical areas and time zones. All the systems are connected with LAN or WAN networks operating at various communication speeds.

When to Use an Enterprise Environment?

This solution can be used when several geographically separated sites require common backup policies to be used. It can also be used when all departments at the same site want to share the same set of backup devices.

Figure 1-5 Large Data Protector Enterprise Environment



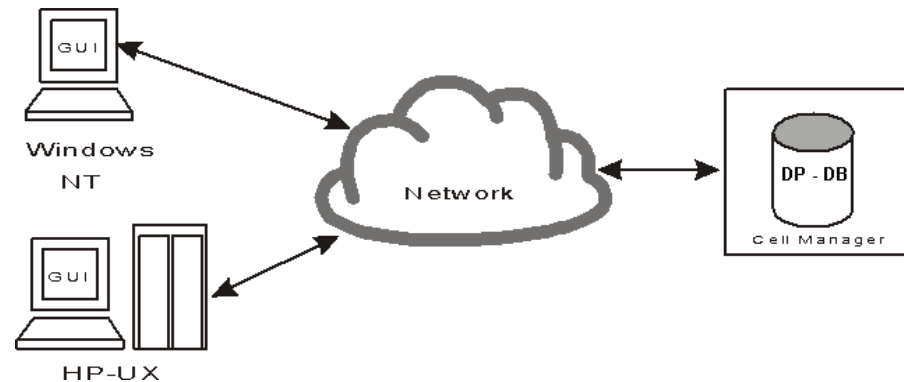
Configuring and managing backups of such a heterogeneous environment is challenging. Data Protector functionality has been designed to highly simplify this task.

User Interfaces

Data Protector provides easy access to all configuration and administration tasks using the Data Protector GUI provided to run under X11/Motif on UNIX platforms and on the Windows platforms. Additionally, a command-line interface is available on UNIX and Windows platforms.

The Data Protector architecture allows you to flexibly install and use the Data Protector user interface. The user interface does not have to be used from the Cell Manager system; you can install it on your desktop system. As depicted in Figure 1-12, the user interface also allows you to transparently manage Data Protector cells with HP-UX, Solaris or Windows Cell Managers.

Figure 1-6 Using the Data Protector User Interface



TIP

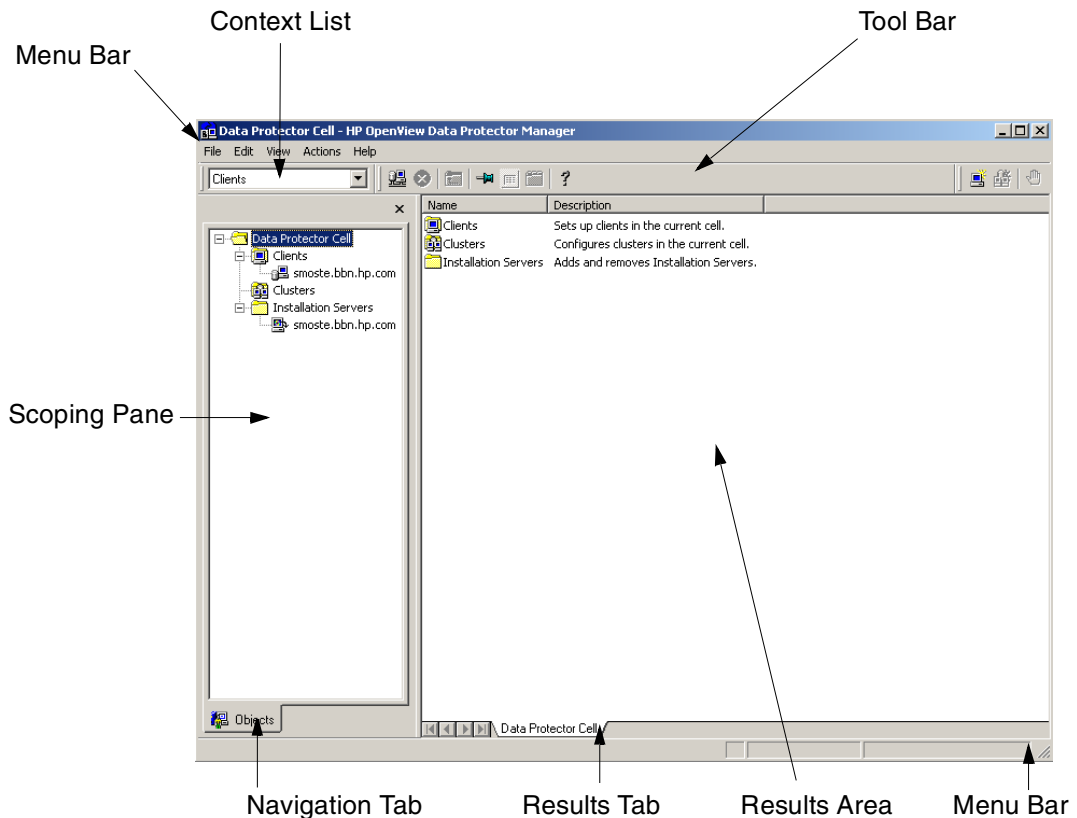
In a typical mixed environment, install the Data Protector user interface on several systems in the environment, thus providing access to Data Protector from several systems.

Data Protector GUI

The Data Protector User Interface is an easy-to-use, powerful graphical user interface. It provides the following main functionality:

- A Results Tab with all the configuration wizards, properties and lists.
- Easy configuration and management of the backup of online database applications that run in Windows environments, such as Microsoft SQL 7, Microsoft Exchange 2000, SAP R/3, and Oracle8 or that run in the UNIX environments, such as SAP R/3, Oracle8, and Informix.
- A context-sensitive online Help system called the Help Navigator.

Figure 1-7 Graphical User Interface



About HP OpenView Operations

The following sections introduce the main concepts behind HP OpenView Operations (OVO), and answers the questions:

- What Is OVO?
- What Does OVO Do?
- About Administrators and Operators
- Ready-to-Use Policies
- Ready-to-Use Tools
- Service Discovery
- What Are the Main Components?
- Putting It All Together

What Is OVO?

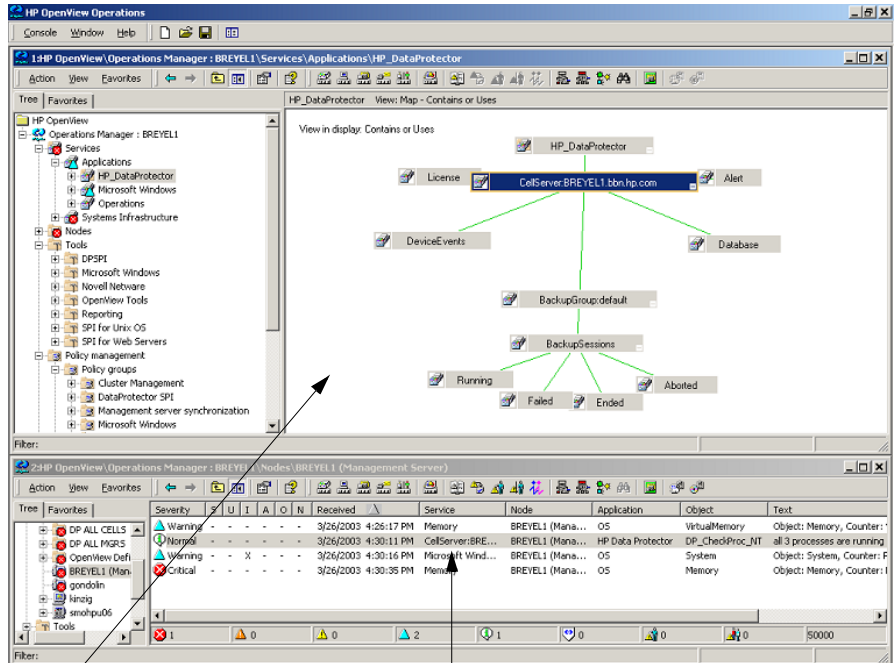
HP OpenView Operations for Windows is a distributed client/server IT operations solution that enables an IT organization to manage their customer's enterprise by individual business services first and then manages all elements dependent on that service. Operations provides solutions for identifying, diagnosing, prioritizing, and responding to these problems in your Windows or UNIX environment.

Operations enables you to build management models. Management models are graphical representations of your service elements called service maps. This specialized interface allows association of the network's physical infrastructure with logical business services. The service map displays an entire business service view in a tree hierarchy to illustrate the relationships and dependencies between map components.

You can "drill down" on a particular service component by clicking on that service component and dragging it to the center of the screen. As you drag a service component you'll notice that the map orientation changes so that the particular service component selected is the highest point of the tree, with the lower level dependencies displayed accordingly.

This assists you in identifying the root cause of a particular problem. In addition, the service map is color-coded to show warning or problem severity as well as scalability for the managed customer environment.

Figure 1-8 Example of a Data Protector Service in a Map View



Map view relates problems to the business.

Active messages browser helps operators detect and respond to problems

NOTE

OVO for Windows is a snap-in to the Microsoft Management Console (MMC), a common console framework for management applications. MMC does not provide any management behavior.

What Does OVO Do?

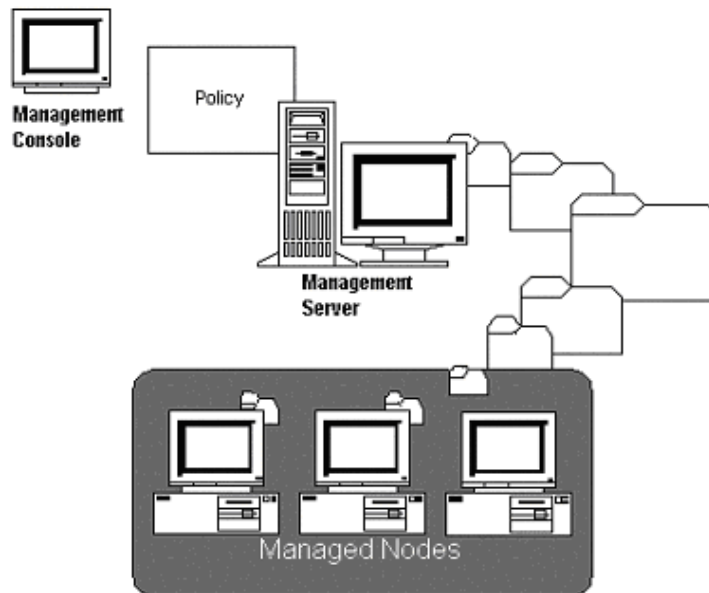
OVO manages your information technology environment and e-services by managing the nodes and services running on the managed nodes. It provides graphical user interfaces to configure:

- Policies
- Nodes
- Services
- Tools

These components work together to automate the detection, evaluation, and response to events and simplify the process of analyzing and resolving problems.

Performance and Event Management

Figure 1-9 Deploying OVO Agents and Configurations



OVO automatically deploys the intelligent agents and configurations that are required for specific types of policies.

OVO uses agents and policies to help manage nodes and e-services. Instead of a one-size-fits-all agent with a range of services that often go unused, it installs only the software components that are needed for the policy and agent to perform their jobs. OVO provides:

- *Single deployment of the enterprise agent for both performance and event management.*

With OVO, both performance and event management are provided through easy-to-use policies.

- *Central deployment of the agent from the management server to all managed nodes.*

With OVO, you can install one or more policies to many managed nodes from a single console, and OVO automatically installs the necessary software and agents to the managed nodes.

- *A policy manager.*

With OVO, you can use the Policy Manager to store and group policies.

Service Management

OVO displays service component dependencies

OVO displays in a map view the relationships between service components and the delivered subservice. Network elements, computer systems, databases, and applications are mapped to the service to clarify relationships and dependencies. By showing which components comprise a given service, OVO shows you which services are at risk when one or more components fail. To relate problems to a particular business, you configure a relationship between three primary components:

- service component (the service running on the managed node).
- service hierarchy or model you create in the Service Editor.
- policies installed on the managed node.

OVO helps resolve problems quickly

With OVO, you can provide answers to the following questions:

- Which of your customer's services are healthy or unhealthy?
- Which service components are affecting the health of a given service?

- What is the severity of an event?
- Which component is the cause of one or more unhealthy services?
- What actions will assist in diagnosing or fixing a given problem?

You can use the map view on the management console to quickly pinpoint problems. For example, to facilitate isolation of a problem, you can display faulty service components in a root cause view. Then you can use the tools and information associated with displayed messages to evaluate and respond to the problem. You can also configure OVO to automatically execute tasks to correct a problem condition.

Node Management

OVO automatically discovers Windows NT nodes in your Windows network and UNIX nodes in a DNS environment. Discovered nodes can then be managed by configuring them in an editor. The editor also gives you the opportunity to create a hierarchical tree structure to best represent your network layout.

Nodes that are not automatically discovered can be added manually to the list of managed nodes. When a node is managed, you can deploy policies to that node, which allow you to track and monitor events and to collect performance data.

With OVO you can configure policies to respond to specific events occurring on managed nodes. Your configurations in a policy tell the OVO agent what to look for and what to do when the event occurs. The agent conducts many of the problem detection, evaluation, fixes, and message sending tasks automatically. In this way many problems are handled before you (as administrator or operator) are notified of a problem.

For example, OVO can notify you when your disk storage is at risk and respond accordingly to the problem. OVO also combines Application Response Monitoring and events for application performance monitoring. For example, OVO can be configured to notify you when a transaction response time exceeds its service level objective, or if the application's consumption of a resource exceeds a given threshold.

Supports SMART Plug-In and Integration Programs

OVO provides a flexible architecture, which supports the use of SMART Plug-In (SPI) programs and integrations such as the HP OpenView Storage Data Protector Integration. These are prepackaged application-specific management programs which provide the

knowledge, configuration information, and tools to enable management of specific applications such as Data Protector. For more information about SPIs for OVO, contact your HP representative.

About Administrators and Operators

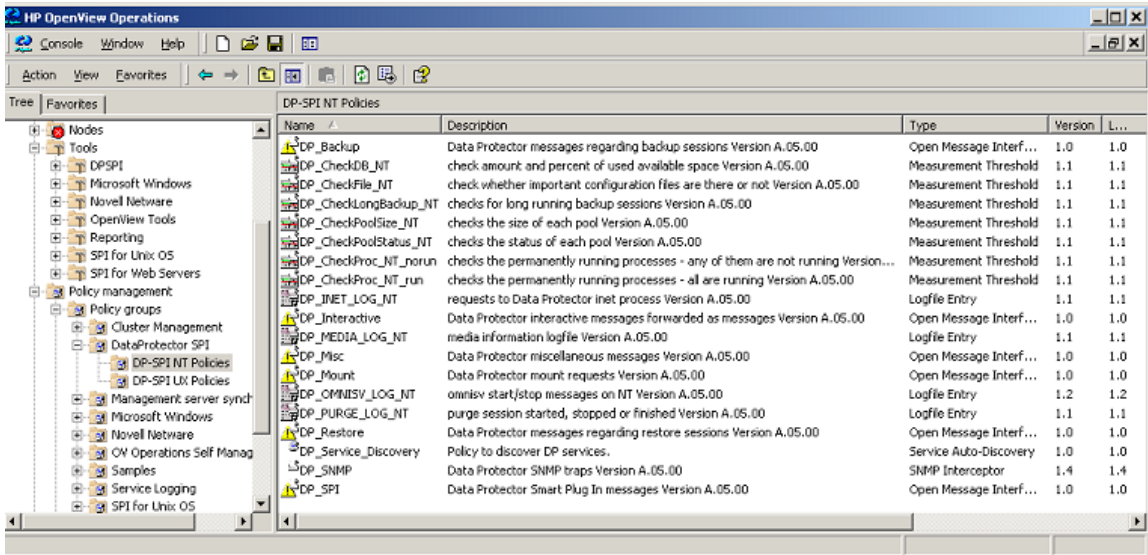
For security purposes, OVO users are grouped by the tasks they are allowed to perform. OVO designates the following two user categories:

- **Administrators** are those who plan the product implementation, install and configure the product, maintain the product configuration, and develop and deploy policies as necessary.
- **Operators** are those who monitor the status of a service or managed node using predefined views, troubleshoot problems using appropriate filters, and resolve problems using appropriate tools as defined by the administrator.

The concepts of designating and setting up domains, administrators, and user groups are based primarily on how an administrator configures Microsoft's security and User Role settings. Discussion of the relationship between Microsoft security and user groups is outside the scope of this guide. For more information on configuring user groups, see the *HP OpenView OVO for Windows Installation and Administrative Tasks Guide*.

Ready-to-Use Policies

Figure 1-10 Data Protector SPI Policy Group



Factory-configured policies, tools, and other intelligent agents are installed when you install OVO on your management server. These include:

- **OVO Microsoft® Windows policy group** provides agents, service discovery functionality, preconfigured policies for Windows systems. It also provides tools and other intelligent software for automated monitoring of Windows services. When you install OVO, the Microsoft Windows policy group is also installed on your console under the Policy Management tree. No additional configuration is required.

The SMART Plug-In for Microsoft Windows can provide you with additional, preconfigured policies for other Windows services. For more details, contact your HP representative.

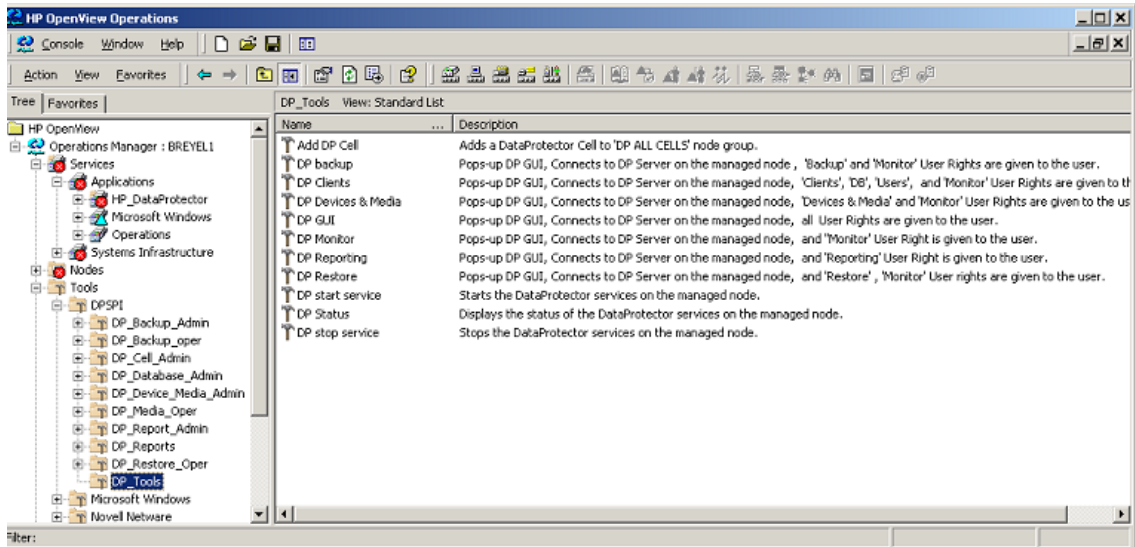
- **Application monitoring policies** provide the Application Response Measurement (ARM) 2.0 agent, preconfigured policies, and other software for collecting basic transaction metrics. You can also use these policies to monitor your ARM 2.0-instrumented

applications by service level. For more information on these policies, refer to Application Response Monitoring under the online help book-level section, “Administering Your Environment.”

- **Operations and performance monitoring policies** are policies in the Microsoft Windows policy group that you can deploy immediately, which helps to automate operations and performance monitoring of your managed Windows environment. For more information on these policies, see the online help section “Managing Windows Services,” which you can find under the online help book-level section “Administering Your Environment.”
- **OVO Self Manager** automatically installs when you install OVO on your management server. It monitors the health of the OVO agents as well as the health of the management server. For example, if one of the agents is not functioning, you would get a message in your message browser about the agent.
- **HP-UX and Sun Solaris node policies** are policies in the Microsoft Windows policy group that you can deploy to manage the operations and performance of your HP-UX and Sun Solaris nodes. These policies also include tools to view information from remote UNIX nodes and to open telnet connections. For more information on these policies, see the section “Managing Windows Services,” which you can find under the online help book-level section “Administering Your Environment.”

Ready-to-Use Tools

Figure 1-11 Data Protector Tools in the DP_Tools Tool Group



OVO includes powerful tools that:

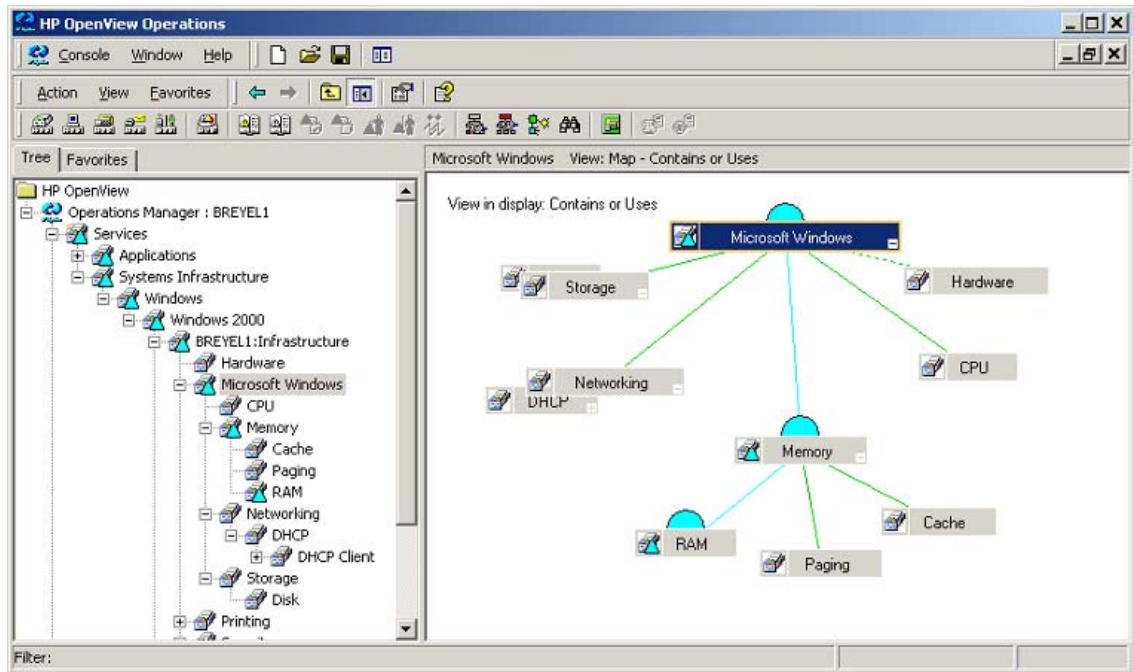
- enable operators to perform actions on remote managed nodes without the need to physically log on.
- can be configured to run on many nodes simultaneously.

This can be useful in checking on usage prior to a backup, and then in performing a backup on all managed nodes selected for the tool.

Ready-to-use tools are listed under the Tools tree. For detailed information about the Microsoft Windows tools, see the online help topic “Managing Microsoft Windows Services.” For detailed information about UNIX tools, see the online help topic “Managing UNIX Services.”

Service Discovery

Figure 1-12 Example of a Microsoft Windows Services Service Map



OVO includes service discovery, which locates and identifies operating services on Windows NT/2000 nodes. Service discovery searches your managed nodes for service elements that match the applications or objects that policies in the Microsoft Windows Auto-Deploy group manage. After discovering services, OVO:

- Creates a map of services for each node.
- Deploys a policy to the appropriate node.
- Displays the service discovery map in the map view.

To keep the hierarchy up to date, OVO provides a Synchronize Services command in the Tools, OpenView Tools, and Self Manager tree and a Scheduled Command policy in the OV Operations Self Manager, and Server policy groups to synchronize Windows-related services at 3.00 am.

What Are the Main Components?

The three main components of OVO are:

- Management Server
- Management Console
- Managed Nodes
- Policies and Agents

These three components communicate important information via messages displayed in your message browser. Messages are generated as a result of an event being detected on a managed node. These messages can be received in an active message browser or logged into an acknowledged message browser.

Management Server

The management server is the computer that performs the central processing functions. It performs the following actions:

- Stores and consolidates messages and actions from managed nodes.
- Calculates the status of a service and of managed nodes.
- Tracks the versions of policies, policy inventory, and policy types.
- Calls the appropriate agent to start actions (local Automatic Commands are started on the managed node).
- Controls the database for historical and active messages.
- Installs OVO agent software on managed nodes.

The management server also notifies the managed nodes about configuration changes and initiates updates.

Management Console

The Microsoft Management Console (MMC) is a framework that hosts administrative tools for managing networks, servers, and other Microsoft® related operations. You install OVO for Windows within the MMC to manage services from one or more management consoles.

Managed Nodes

Nodes are computer systems or intelligent devices that can be managed from the management server. The managed nodes you specify are listed in the Nodes folder of the console tree. In the Configure Managed Nodes editor you can specify which nodes to monitor in OVO. Operators can monitor nodes and services and use the available tools to perform routine maintenance and also to resolve problems that have critical business impact. Configuring a managed node is a multi-step process that involves:

- Specifying the node or group of nodes to be managed.
- Entering details about each node's hardware and environment.
- Specifying the tools available for each managed node or node group.

Policies and Agents

A policy is a set of specifications and rules that helps automate network and system administration. Using HP OpenView Operations or OVO, administrators can deploy policies to various destinations to provide consistent, automated administration across a network.

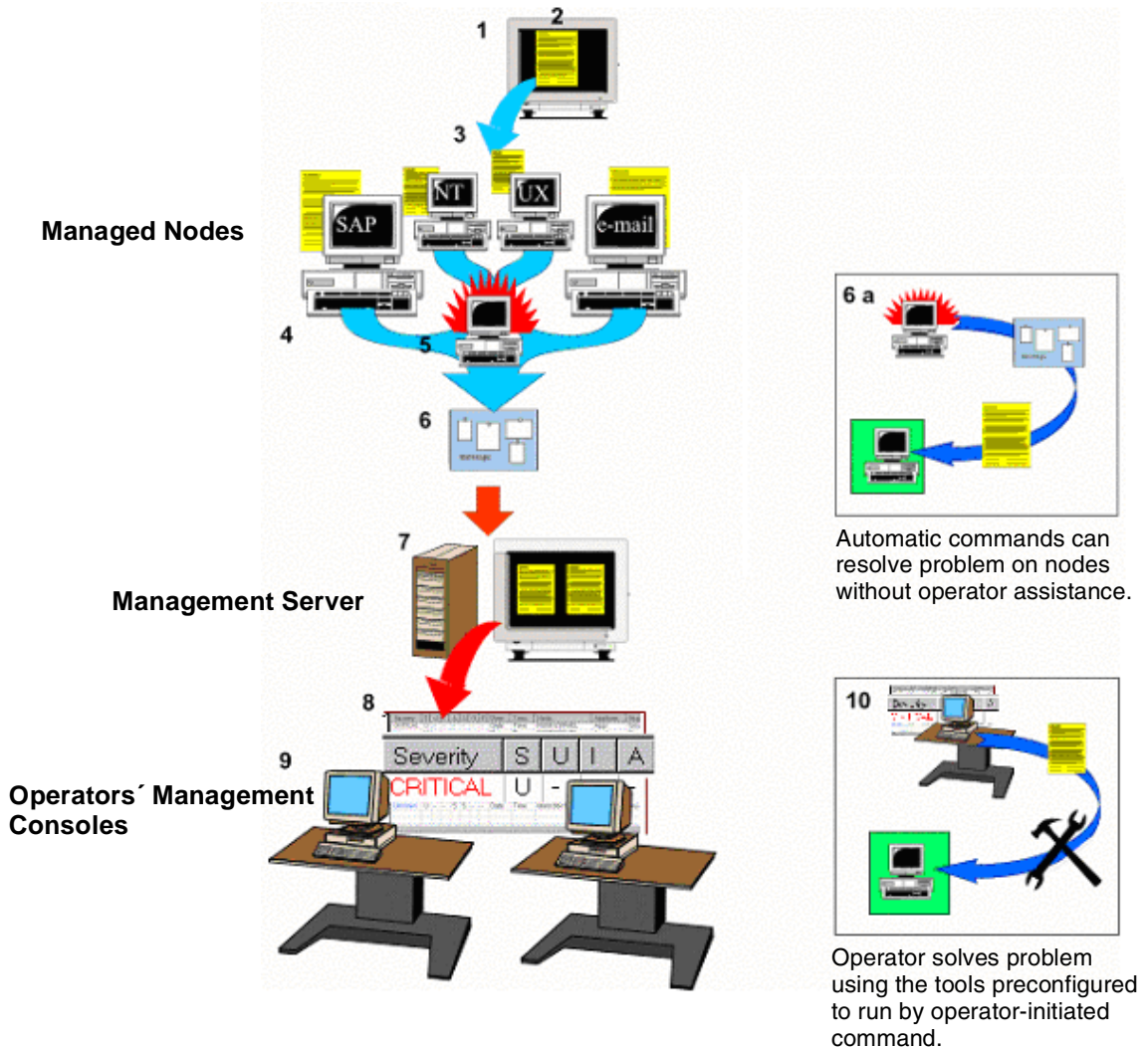
Agents are intelligent processes that are designed to run on the managed node and to perform specific tasks to assist with the management of services. For example, you can instruct agents to perform specific tasks such as monitoring managed nodes for SNMP events, notifying you of security violations, or collecting metrics.

NOTE

Agents are stored as Deployment Packages. When you deploy a policy of a specific policy type, OVO deploys the necessary agents along with the policy. Separate agent installation is not required.

Putting It All Together

Figure 1-13 OVO Overview



See the numbered items in the table for a descriptions of the key components and operations.

1. OVO is installed on the management server, management console(s), and managed nodes.
2. Policies are primarily stored and maintained on the management server.
3. Policies and other OVO software are deployed from the administrator console to managed nodes.
4. Managed nodes are the Windows NT/2000 or UNIX systems you choose to manage. Services can run on heterogeneous systems (such as SAP R/3) or homogeneous systems.
5. When an event occurs, the agents on the managed node detect the event and, according to the conditions defined in the policy, evaluate whether the agent should respond to the event.
6. Using the information in the policy, OVO creates a message that is forwarded to the management server. This type of message contains all event information.
 - 6a. Depending on the policy and the kind of event that occurred, a message is stored locally on the node where the event occurred and forwarded to the management server later. An automatic response to the event can also be configured.
7. The management server receives the message. If many messages about the same event are received, the management server can consolidate the messages.
8. The message displays in the message browser of the operator's console.
9. The active message browser has a menu of preconfigured functions and information that the operator can use to evaluate, diagnose, and respond to the problem. Active messages are removed from the message browser when an operator acknowledges them.
10. The OVO performance grapher helps to diagnose performance problems.

Details on How OVO Works

OVO management is based on messages and actions, which are passed between managed nodes, the management server, and management consoles. The management server communicates with managed nodes via agents running on the managed nodes and through policies (instructions to the agent) which reside on the managed node. You can

use the policy editor to configure the way in which the agent detects, evaluates, and responds to events. After you configure the policy for your specific requirements, you then deploy the policy to the managed node.

Role of the Agent

The role of the agent is to collect management data, send messages to the management server, and manage nodes as defined in the policy. The agent also executes automatic commands on the managed nodes. The agent can also work independently; if the agent cannot communicate with the management server (for instance, when the server or network link is down), the agent logs the message and performance data on the managed node, and continues to execute automatic commands as specified by the policy. When the connection to the management server is re-established, the locally buffered messages are forwarded to the management server.

Agents monitor managed nodes for specific events or can perform tasks like transforming a data source into a metric. For example, in order for OVO to monitor and respond to SNMP events, the Enterprise Message/Action Agent package and an SNMP Interceptor policy must be installed on the managed node. Some examples of policy types that capture events: Logfile Entry, Measurement Threshold, Open Message Interface, SNMP Interceptor, Windows Event Log, and Windows Management Interface.

Automatic Commands and Operator-Initiated Commands

An automatic command is a command, executable program, or script that is configured in the policy to launch automatically when there is a match to specific conditions in the policy. In a policy you can also configure the response to a message-generating event to be an operator-initiated command. An operator-initiated command is a command, executable program, or script that the operator executes from the Active Message menu.

What Is the Data Protector Integration?

The Data Protector Integration is a software package that enables you to monitor and manage the health and performance of your Data Protector environment with HP OpenView Operations (OVO), and the HP OpenView Performance (OVPA) Agent.

The union offers a complementary and consolidated view of Data Protector performance information and overall resource characteristics. The integration allows correlation of Data Protector performance data with the performance data of the operating system, the database, and the network - all from one common tool and in one central management system. Integration of Data Protector performance data into the OVPA helps to detect and eliminate bottlenecks in a distributed environment. In addition, the integration allows for system optimizations well as service level monitoring.

The Data Protector Integration offers the following key features:

- Instrumentation and configurations for the HP OpenView Operations agents on a Data Protector Cell Manager system to monitor the health and performance of Data Protector.
- Monitoring of multiple Data Protector Cell Managers with a single OVO Management Server.
- The Data Protector Integration depicts the functionality of Data Protector as a service tree.
- The Data Protector Integration uses the ARM and DSI interfaces of the Performance Agent to collect performance data and ARM transactions.
- The Data Protector Integration channels messages sent to OVO Management Server based on a user's role. Each OVO user sees only the messages he needs.
- The Data Protector Integration allows the Data Protector Cell Manager and the OVO Management Server to be installed on different systems.
- The Data Protector Integration enables you to run Data Protector functionality from the OVO Tools.
- The integration with Reporter Light provides reports on Backup Session, Data, and Trend by directly fetching the necessary data from the Data Protector Cell Servers.

The Data Protector Integration offers the following key benefits:

- Centralized problem management using OVO agents at the Data Protector managed nodes. The use of a central management server avoids duplicated administrative effort.
- Real-time event and configuration information for fast problem resolution.
- Powerful monitors to detect potential problem areas and to keep track of system and Data Protector events.
- Performance data collectors to ensure continuous system throughput and notify of any performance bottlenecks.
- Complements the Data Protector Administration GUI.
- Performance data collection and monitoring.
- Central data repository for storing event records and action records for all Data Protector managed nodes.
- Utilities for running Data Protector management tasks.
- The Data Protector Integration enables the OVO user to start the Data Protector GUI and use Data Protector functionality from the OVO Management Server.
- Users are able to visualize the state of health of their Data Protector Cell Managers and overall backup environment by examining the Backup Session, Data, and Trend reports available with the Reporter Light integration that is part of OVO for Windows.

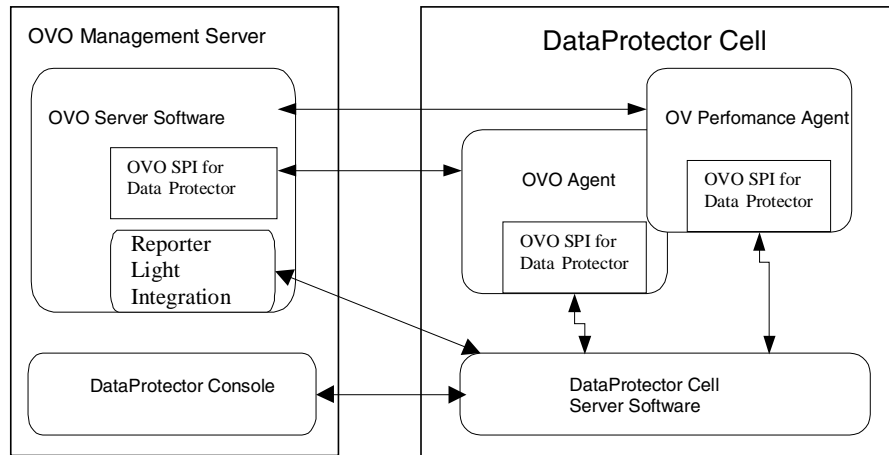
Data Protector Integration Architecture

The Data Protector Integration resides on the HP OpenView Operations (OVO) management server system and its OVO agent instrumentation on the Data Protector Cell Manager system, which is an OVO managed node. The Data Protector Cell Manager system must have the OVO agent and OVPA installed. The Data Protector Console is installed on the OVO management server.

Once installed, the OVO user can start the Data Protector graphical user interface (GUI) as an OVO application and connect to any available Data Protector Cell Manager. Both Windows and UNIX Data Protector Cell

Managers are accessible. This is facilitated by the Data Protector Console using Data Protector's communication protocol on port 5555 to exchange data.

Figure 1-14 Data Protector Integration Architecture



All the Data Protector OVO policies, which monitor:

- Data Protector vital cell manager processes
- Data Protector logfiles
- Data Protector SNMP traps

configures the OVO agent on a Data Protector Cell Manager. The OVO agent on a Data Protector Cell Manager sends messages to the OVO management server for display in the message browser only if appropriate conditions match. This minimizes network traffic between a Data Protector Cell Manager and the OVO management server.

The Data Protector Integration policies, such as policies to monitor Data Protector logfiles, SNMP traps, database and processes, define the conditions on which the OVO Agent will send messages to the OVO Management Server for display in OVO's message browser.

2 **Installing the Data Protector Integration**

In this chapter you will find information on:

- Prerequisites for installing the Data Protector Integration.
- Installing the Data Protector Integration on the system where the HP OpenView Operations management server software is installed.
- Installing the Data Protector Integration components on OVO managed node (Data Protector Cell Manager) system.
- Deinstalling the Data Protector Integration components from OVO managed node (Data Protector Cell Manager) systems.
- Deinstalling the Data Protector Integration from the system where the HP OpenView Operations management server software is installed.

Supported Platforms and Installation Prerequisites

The HP OpenView Storage Data Protector Integration is used to monitor and manage the health and performance of Data Protector environments. You can manage one or more Data Protector cells with the HP OpenView Storage Data Protector Integration. It should only be installed in an environment consisting of:

- One or more systems running OVO management server.
- The OVO Console and the Data Protector Console must be installed on the system where the Data Protector Integration Console is to be installed.
- OVO agent running on systems with the Data Protector Cell manager.

It is only guaranteed to work in these environments.

Before starting the Data Protector Integration installation process, make sure that the following requirements are met:

Data Protector Supported Versions

The Data Protector Integration is designed to work with HP OpenView Storage Data Protector, version 5.1 on the following platforms:

Table 2-1

HP OpenView Storage Data Protector Availability

Operating System	Data Protector Version
	5.1
HP-UX 11.00	✓
HP-UX 11.11	✓
HP-UX 11i	✓
Solaris 7	✓

Table 2-1 HP OpenView Storage Data Protector Availability (Continued)

Operating System	Data Protector Version
	5.1
Solaris 8	✓
Solaris 9 (OVO A.07.10 English Agent only)	✓
Microsoft Windows NT 4.0 with SP6A (Workstation, Server and Enterprise Edition)	✓
Microsoft Windows 2000 with SP3 (Professional, Server, Advanced Server, Data Center)	✓
Microsoft Windows XP Professional (32 bit), Microsoft Windows Server 2003.	✓

OVO Management Server System

HP OpenView Operations management servers are supported on the following platforms. The OVO server can run on a different host system than the system where the Data Protector Cell Manager is installed.

HP OpenView Operations and HP OpenView Service Navigator is installed and configured on a system running one of the following Operating systems:

Table 2-2 OVO Management Server Supported Versions

OVO version ^a Operating System	OVO 7.1	OVO 7.1
Microsoft Windows 2000 with SP3 (Professional, Server, Advanced Server, Data Center)	✓	✓

a. English, and Japanese.

OVO Patches

Please ensure that the following minimum patches are installed.

Table 2-3

Patches for OVO (version A.07.10)

Patch Number	Description
OVOW_00005.exe	OVO Management Server patch
OVOW_00012.exe	Message Action Windows Agent patch
OVOW_00016.exe	Windows OS SPI Management Server patch

Software Prerequisites on the OVO Management Server

Please ensure that the following software is installed on the OVO management server system:

- HP OpenView Operations for Windows. The console is installed and configured on the HP OpenView Operations management server system or other appropriate systems.
- The HP OpenView Storage Data Protector Console is installed on the HP OpenView Operations management server system.

Hardware Prerequisites on the OVO Management Server

Please ensure that the following hardware prerequisites are met on the OVO management server system:

- 5 MB disk space on the HP OpenView Operations management server system to install components necessary for the Data Protector Integration.

Managed Node Systems (Data Protector Cell Manager)

A number of agents and the Data Protector Integration are required for the complete management of Data Protector environments. The required components that must be installed on the managed node system hosting the Data Protector Cell Manager are:

- HP OpenView Operations Agent
- HP OpenView Performance Agent

Supported OVO Agent Versions

The Data Protector Cell Manager installation must be made on a platform for which the OVO Agent is available. Please refer to Table 2-4 for details of the available agent versions and ensure that the appropriate version is installed:

Table 2-4 HP OpenView Operations Agent Availability

Operating System	OVO Agent Version
HP-UX 11.00	A.07.10 or higher
HP-UX 11.11	
HP-UX 11i	
Solaris 7, 8, 9	
Microsoft Windows NT 4.0, 2000, XP	

Supported HP OpenView Performance Agent Versions

If the OVPA is to be installed, the Data Protector installation must be made on a platform for which the OVPA is available. Please refer to Table 2-5 for details of the available agent versions.

Table 2-5 HP OpenView Performance Agent Availability

Operating System	OVPA Version
HP-UX 11.00	C.03.70 or higher
HP-UX 11.11	
Solaris 7	C.03.75 or higher
Solaris 8	
Microsoft Windows NT 4.0, 2000, XP	C.03.65 or higher

Additional Software for HP-UX Managed Nodes

The following software is not installed as part of the OVO management server installation nor as part of the Data Protector Integration installation. Please refer to each product section to check whether they are required or optional.

SNMP Emanate Agent (required)

The SNMP Emanate Agent is necessary to capture SNMP traps sent by the Data Protector Cell Manager on the same system and to let the OVO Agent forward any matching SNMP trap events as OpC messages to the OVO management server. This is called *Distributed Event Interception*, since the SNMP traps are intercepted on a managed node and not on the OVO management server.

The advantages, especially for large enterprise environments with a high number of Data Protector Cell Managers, are:

- The solution scales better: Additional Data Protector Cell Managers do not put additional load on the management server as the processing of SNMP traps is done on the managed node.
- Any automatic action configured as a response to an SNMP trap can be triggered and run locally on the managed node without involvement of the management server.
- Since no SNMP trap is sent from the managed node to the management server, the network load decreases.
- The probability that SNMP traps are lost is significantly reduced as these are not transmitted over the network.
- Security over (public) networks is increased, since SNMP traps do not use a network and are sent, received and processed only on the managed node. OpC messages are sent by the OVO agent to the OVO management server using DCE/RPCs, which allows authentication and encryption.

How to Check the SNMP Emanate Agent is Installed

Please check that the SNMP Emanate Agent is installed on the Data Protector Cell Manager node using the command:

```
# swlist -l product -a description OVSNMPAgent
```

You should see the following type of entry:

Supported Platforms and Installation Prerequisites

```
# OVSNMPAgent          B.11.00 HPUX_10.0_SNMP_Agent_Product
   OVSNMPAgent.MASTER  B.11.00 MASTER
   OVSNMPAgent.SUBAGT-HPUNIX B.11.0 SUBAGT-HPUNIX
   OVSNMPAgent.SUBAGT-MIB2  B.11.0 SUBAGT-MIB2
```

Additional Software for Windows Managed Nodes

The following software is neither installed as part of the OVO management server installation nor as part of the Data Protector Integration installation. Please refer to each product section to check whether they are required or optional.

SNMP Service (required)

In order to send the Data Protector SNMP traps to the OVO management server you must install the SNMP service.

Disk-Space Requirements

Table 2-6 lists the disk space requirements for both the installation of the Data Protector Integration software and the Data Protector Integration's run-time files on the OVO management server and, in addition, on the managed node.

Table 2-6 **Disk-Space Requirements**

Machine	OVO Version	Operating System	Total
OVO Management Server	OVO 7.1	Windows 2000	5 Mb
OVO Managed Node	OVO 7.1	HP-UX 11.00, 11.11, 11i	1 Mb
		Solaris 7, 8	1 Mb
		Supported Microsoft Windows Nodes	1.5 Mb

Memory (RAM) Requirements

There are no specific requirements concerning the amount of RAM installed on either the OVO management server or managed nodes, beyond the requirements of OVO and Data Protector.

Installing the Data Protector Integration

The Data Protector Integration is delivered in the `DPSPI-B.05.03.msi` MSI package which is used to install the Data Protector Integration and console onto the OVO management server. This installs all components required for the management server and the managed nodes on the management server system. The agent software and the configuration data for these agents is then distributed by the OVO administrator to the managed nodes using OVO.

Installation

To install the software on the management server, run the `DPSPI-B.05.03.msi` executable file.

The following directories are created on the OVO management server system, where `<INSTALLDIR>` is by default:

<code>c:\Program Files\HP OpenView</code>	
<code><INSTALLDIR>\install\DPSPI\</code>	Installation directory with subdirectories for policies and OVO configuration files
<code><INSTALLDIR>\bin\</code>	Binary and script files
<code><INSTALLDIR>\install\DPSPI\vp\<Platform></code>	DSI performance agent integration
<code><INSTALLDIR>\Instrumentation\<Platform>\<Version>\SPI for DataProtector\</code>	Monitor scripts and configuration files
<code><INSTALLDIR>\Instrumentation\<Platform>\<Version>\DP-SPI Discovery\</code>	Service discovery scripts and executables
<code><INSTALLDIR>\NLS\1033\Manuals\</code>	Documentation containing: Integration Guide and Release Notes

The following directories are created on a Data Protector Cell Manager running on HP-UX or Solaris after the Data Protector Policies and Monitors have been deployed to it:

```
/var/opt/OV/bin/instrumentation/
```

- ob_spi_proc.sh
- obspi.conf
- ob_spi_backup.sh
- ob_spi_db.sh
- ob_spi_file.sh
- ob_spi_poolsize.sh
- ob_spi_poolstatus.sh
- DPCmd
- dpsvc.pl

The following directories are created on a Data Protector Cell Manager running on Windows NT 4.0 or Windows 2000 after the Data Protector Policies and Monitors have been deployed to it.

The <OpenView Installed Packages Dir> should be:

```
<System Drive>:\Program Files\HP OpenView\Installed  
Packages\{790C06B4-844E-11D2-972B-080009EfbC2A}
```

```
<OpenView Installed Packages Dir>  
\bin\instrumentation\
```

- obspi.conf
- ob_spi_backup.exe
- ob_spi_db.exe
- ob_spi_file.exe
- ob_spi_poolsize.exe
- ob_spi_poolstatus.exe
- ob_spi_proc.exe
- DPCmd.exe
- DPPath.exe
- dpsvc.pl

Installation Verification

To verify the installation:

1. Open the Add/Remove Programs as follows:
Start → Settings → Control Panel → Add/Remove Programs
2. Check that DPSPi-B.05.03 appears as an installed product.

Running the Add Data Protector Cell Application

To run the Add Data Protector Cell Application:

1. Run the **Add DP Cell** tool to create the necessary folders and nodes under the DP ALL CELLS and DP ALL MGRS node groups.

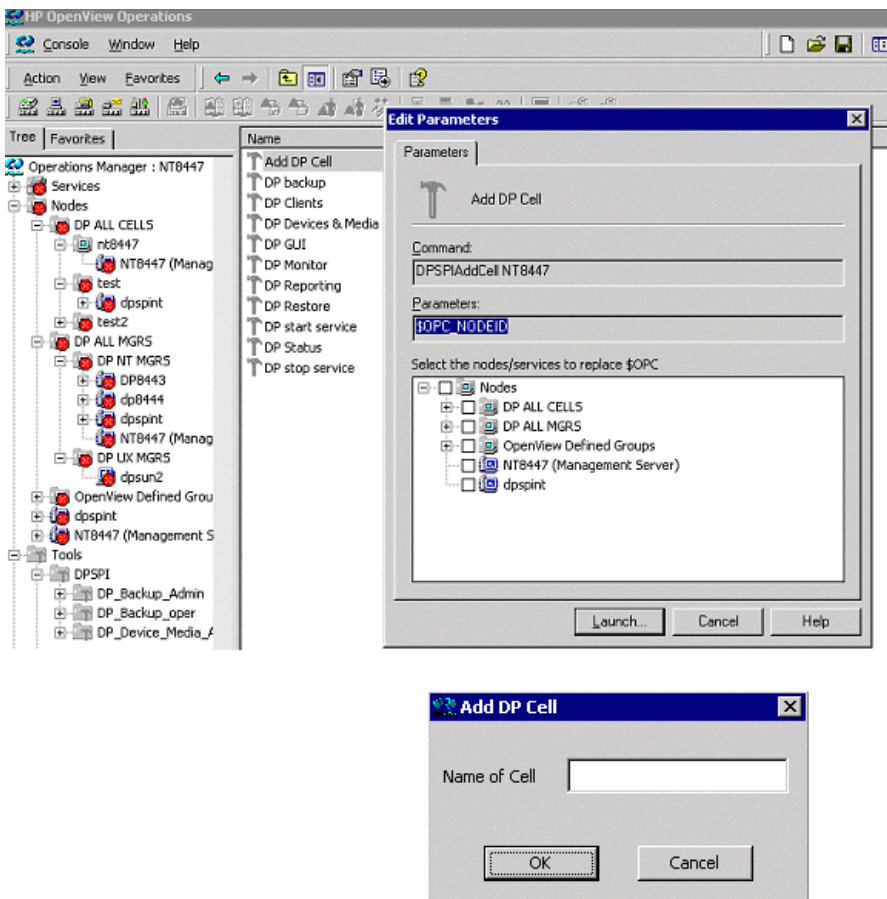
The Edit Parameters window is displayed as shown in Figure 2-1 on page 59.

2. Enter the name of the node group that you are creating under DP ALL CELLS when prompted.

In the example below, the node name of the Cell Server, nt8447, is also used for the name of the node folder created under DP ALL CELLS. This node group is provided to help you organize all systems managed by a Cell Manager, and including that Cell Manager, under the same folder in OVO. However, these name can be different. The resulting node configuration is displayed in the OVO console.

When a managed node is added to either the DP NT MGRS or the DP UX MGRS node groups, using the Add DP Cell tool, the appropriate policies group, DP-SPI NT Policies or DP-SPI UX Policies, is automatically deployed to the node.

Figure 2-1 Data Protector Integration Add Cell Session



For more information on installation of agent software and adding managed nodes to the management server, please refer to the online help for agent installation or the OVO Installation guide.

To verify that the necessary policies have been deployed, right click the node icon, then select:

View → Policy inventory

Deploy Instrumentation

To deploy instrumentation to a node that has already been added to OVO:

1. Right click the node icon to raise the pop-up menu.
2. Select **All Tasks** → **Deploy Instrumentation**

This starts the deployment of the necessary monitors and executables for automatic service discovery.

Agent Configuration

SNMP Configuration on UNIX

To enable the OVO Agent on HP-UX nodes to receive SNMP traps from Data Protector:

1. Add one of the following lines to the `/opt/OV/bin/OpC/install/opcinfo` file.
 - If an `ovtrapd` process is running add:
`SNMP_SESSION_MODE TRY_BOTH`
 - If no `ovtrapd` process is running add:
`SNMP_SESSION_MODE NO_TRAPD`
2. Configure the SNMP Emanate Agent to send SNMP traps to the local OVO agent by adding the following lines to the `snmpd.conf` file:

```
HP-UX          /etc/SnmpAgent.d/snmpd.conf
```

```
trap-dest: 127.0.0.1
```

```
Solaris       /etc/snmp/conf/snmpd.conf
```

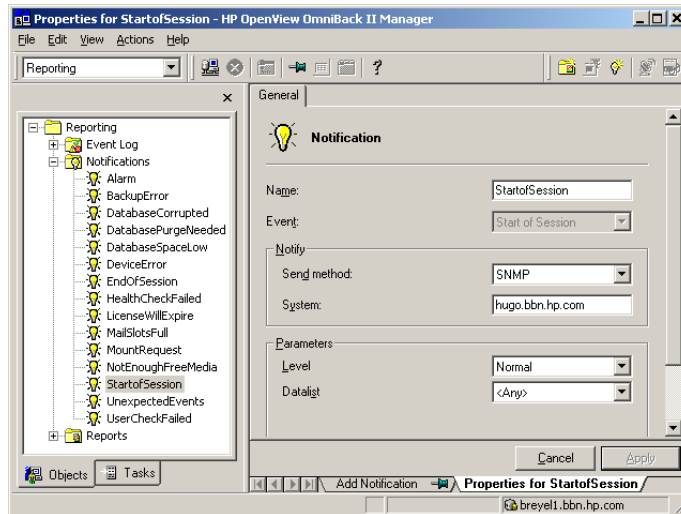
```
trap localhost
```

```
trap-community public
```

3. Configure Data Protector to send SNMP traps to the Data Protector Cell Manager host:
 - a. Use the Data Protector GUI's **Reporting** context window to setup all Notification events to use:
 - SNMP as delivery method

- Cell Manager host system as the destination

Figure 2-2 Data Protector GUI's Reporting context window



- Add the Cell Manager hostname as trap destination to the `OVdestds` file in `/etc/opt/omni/snmp`.
- Disable filtering of SNMP traps by emptying the `OVfilter` file in `/etc/opt/omni/snmp`.

SNMP Configuration on Windows

We recommend that you configure the Windows system to forward its SNMP traps to the OVO Management Server in the following way:

1. To enable Data Protector to send SNMP traps, run the command:

```
omnisnmp
```

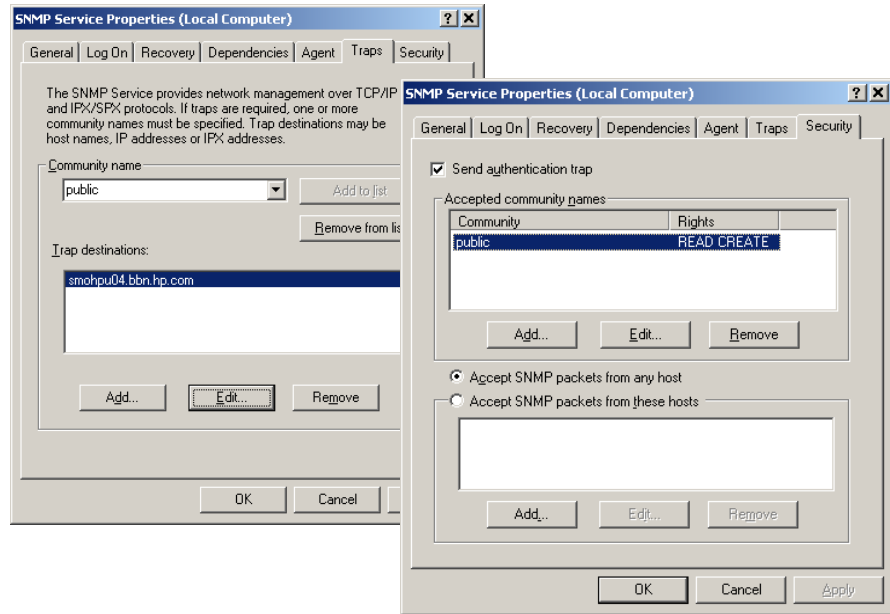
2. Add the following line to the `<Installed Package>\bin\OpC\install\opcinfo` file.

```
SNMP_SESSION_MODE    NO_TRAPD
```

3. Configure the SNMP Service on a Windows system to send traps to the OVO management server. The community name should be **public**, since this is the default community name that Data

Protector's SNMP traps use. The trap destination must be the IP address or the hostname of the OVO Management Server and the rights of the community must be **READ CREATE**.

Figure 2-3 Configuring the SNMP Service on Windows



If you want to use a custom community name other than `public`, you must set this value in the Registry. This will let Data Protector use this custom community name for sending SNMP traps:

```
HKEY_LOCAL_MACHINE\SOFTWARE\HewlettPackard\OpenView\
OmniBackII\SNMPTrap Community<REG_SZ>:
<custom community name>
```

4. Configure Data Protector to send SNMP traps to the OVO management server system:
 - a. Use the Data Protector GUI's **Reporting** context window to setup all notification events to use:
 - SNMP as delivery method
 - OVO management server system as the destination

Please see Figure 2-2 on page 61.

- b. Add the OVO management server hostname as trap destination to the OVdests file in <Data Protector Root>/Config/SNMP.
 - c. Disable filtering of SNMP traps by emptying the OVfilter file in <Data Protector Root>/Config/SNMP.
5. Configure the OVO management server to intercept SNMP traps sent by the Windows Cell Manager. To do this use the OVO GUI to select and distribute the DP_SNMP policy to the OVO management server.

The DP_SNMP policy is located in:

Policy management\Policy groups\DataProtector SPI\DP_SPI NT Policies\

Data Protector User Configuration

- UNIX** For Data Protector on HP-UX nodes, check that the local root user is in the Data Protector's admin user group.
- Windows** For Data Protector on Windows, add the local HP ITO account user and the local SYSTEM account to Data Protector's admin user group.

Miscellaneous Configuration

- Windows** For Windows nodes, the system variable:
- ```
DPHomeDir
```
- must be set with the Data Protector root path in order for the OVO Agent is able to find the Data Protector logfiles to be monitored.
- The default location is: C:\Program Files\OmniBack

---

**NOTE** After changing a Windows system variable, the system must be restarted.

---

## Program Identification

### On UNIX Managed Nodes

All Data Protector Integration programs and configuration files contain an identification string which can be displayed using the UNIX command:

**what(1):**

The output is of the form:

```
HP OpenView Storage Data Protector Integration into OVO
A.05.01 (<build_date>)
```

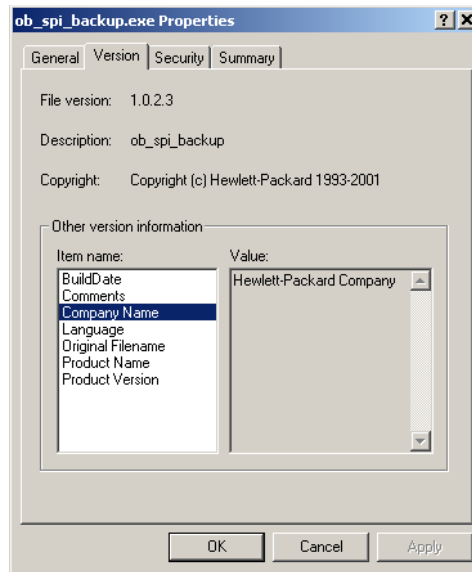
### On Windows Managed Nodes

All Data Protector Integration programs and configuration files contain an identification string which can be displayed by:



1. Right-clicking the `ob_spi_backup.exe` file.
2. Select **Properties** from the popup menu.
3. Select the **Version** tab. The following screen is displayed.

**Figure 2-4**      **Version Information**



---

## Deinstalling the Data Protector Integration

To deinstall the Data Protector Integration, you must complete the following steps:

- Manually to do some de-configuration tasks through the OVO GUI
- Remove the Data Protector Integration from the OVO Management Server.

### De-configuration tasks

#### Undeploy All Data Protector Policies from Managed Nodes

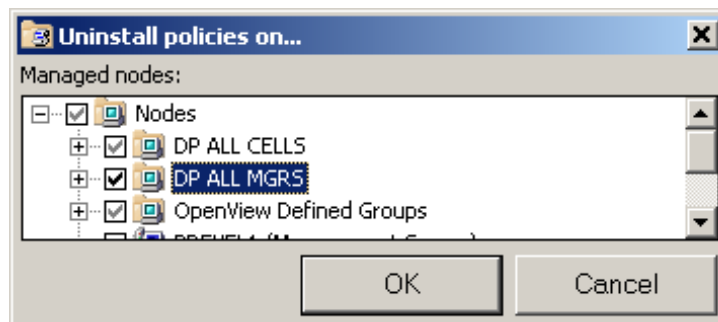
1. Select Policy management\Policy groups\DataProtector SPI, right click and from the pop-up menu select:

**All Tasks** → **Uninstall from...**

This will raise the Uninstall policies on ... window.

2. Mark the **DP ALL MGRS** node entry.

**Figure 2-5** Uninstall policies on... Window



3. Click the **OK** button.

## Remove Data Protector Policies from the OVO Management Server

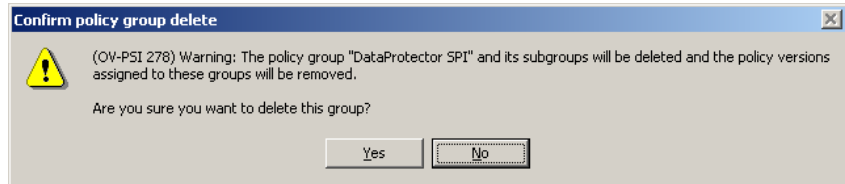
To remove the Data Protector policies from the OVO management server:

1. Select `Policy management\Policy groups\DataProtector SPI`, right click and from the pop-up menu select:

**Delete**

This will raise the `Confirm policy group delete` window.

**Figure 2-6** Confirm Delete Window



2. Click the **Yes** button to remove the policies.

### Remove Data Protector User Roles from the OVO Management Server

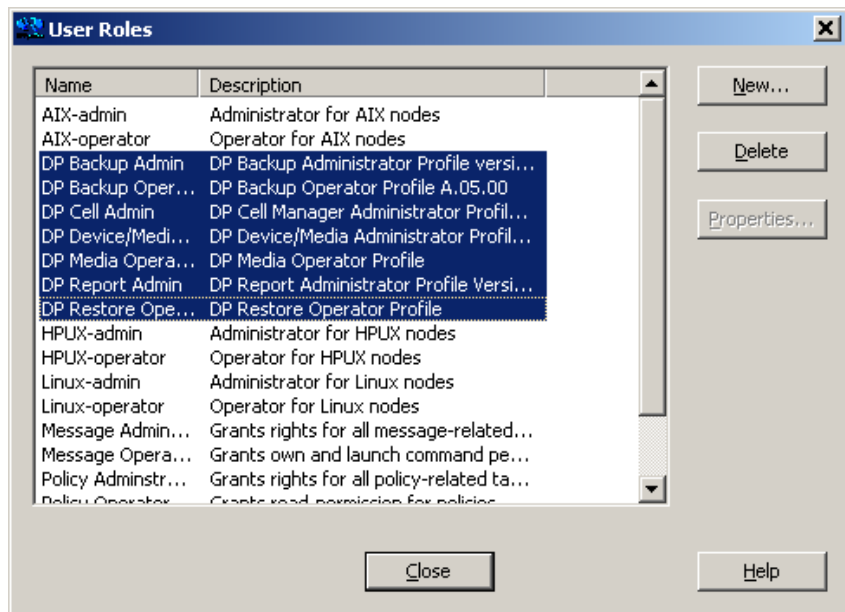
To remove the Data Protector policies from the OVO management server:

1. From the toolbar and following cascading menu, select:

**Action** → **Configure** → **User roles...**

This will raise the User Roles window.

**Figure 2-7** User Roles Window



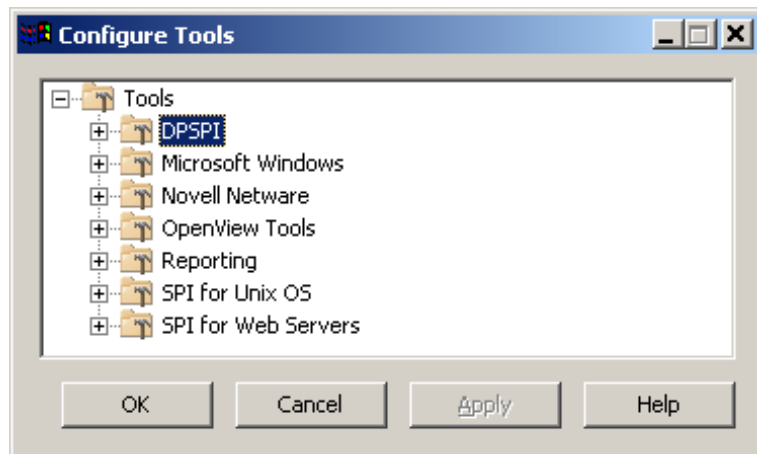
2. In the User Roles window, select all DP\* user roles and click the **Delete** button and close this window.

## Remove Data Protector Tools and Directory from the OVO Management Server

To remove the Data Protector tools and directory from the OVO management server:

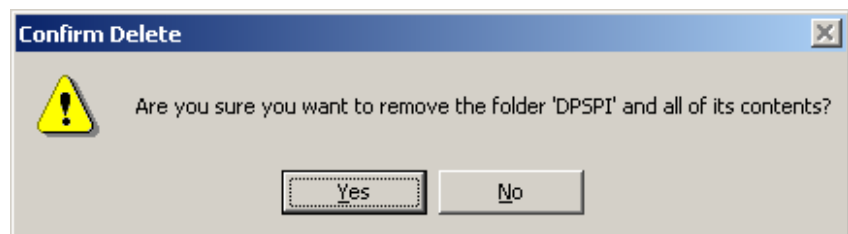
1. From the toolbar and following cascading menu, select:  
**Action** → **Configure** → **Tools...**  
This will raise the `Configure Tools` window.
2. In the `Configure Tools` window, right-click the `DPSPI` entry.

**Figure 2-8** **Configure Tools Window**



3. Select **Delete** from the popup menu. You will be shown the `Confirm Delete` window.

**Figure 2-9** **Confirm Delete Window**



4. Click the **Yes** button to continue deletion. The Confirm Delete window closes.
5. Click **Apply** and **OK** in the Configure Tools window to continue.

### Remove the Data Protector Service Tree from the OVO Management Server

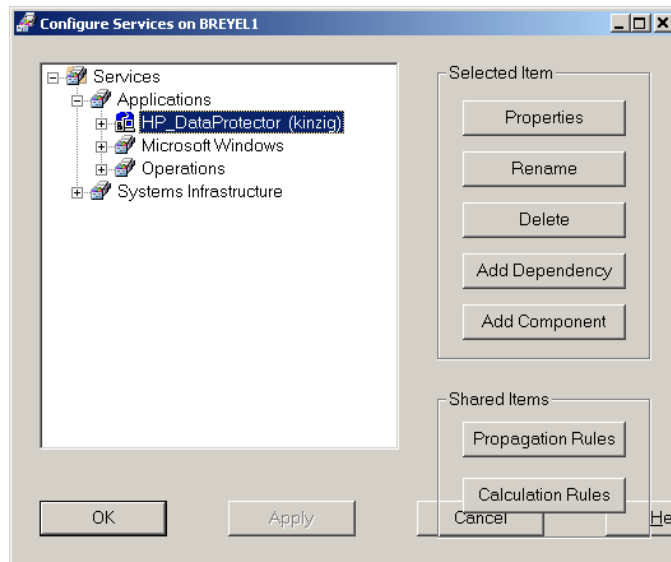
To remove the Data Protector Service Tree from the OVO management server:

1. From the toolbar and following cascading menu, select:

**Action** → **Configure** → **Services...**

This will raise the Configure Services window.

**Figure 2-10** Configure Services Window



2. In the Configure Services window, select:  
Services\Applications\HP\_DataProtector service  
and click the **Delete** button.
3. After confirmation and successful deletion, click **Apply** to activate the change and click **OK** to close this window.

## Remove Data Protector DP ALL CELLS and DP ALL MGRS Node Directories from the OVO Management Server

To remove the Data Protector DP ALL CELLS and DP ALL MGRS Node Directories from the OVO management server:

1. From the toolbar and following cascading menu, select:

**Action** → **Configure** → **Nodes...**

This will raise the Configure Managed Nodes window.

2. In the In the right part of the window, select DP ALL CELLS.
3. Right click DP ALL CELLS to raise the pop-up menu and select **Delete**.
4. Follow the same procedure for DP ALL CELLS.

## Remove the Data Protector Integration

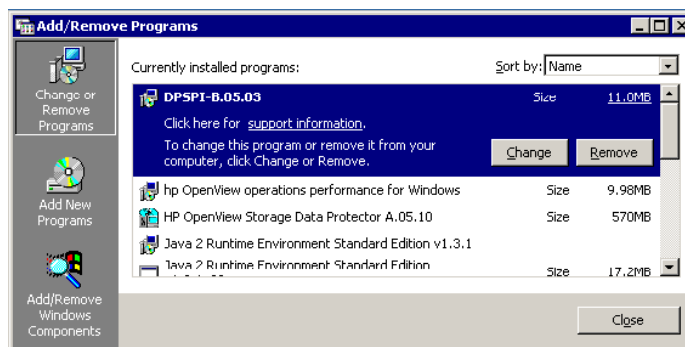
To remove the Data Protector Integration from the OVO management server:

1. From the Control Panel select:

**Add/Remove Programs**

This will raise the Add/Remove Programs window.

**Figure 2-11 Add/Remove Programs Window**



2. In the Add/Remove Programs window, scroll down until you find the DPSP1-B.05.03 entry.
3. Click the **Remove** button to start the removal. This will take a short time

Installing the Data Protector Integration  
**Deinstalling the Data Protector Integration**



---

# **3**      **Using the Data Protector Integration**

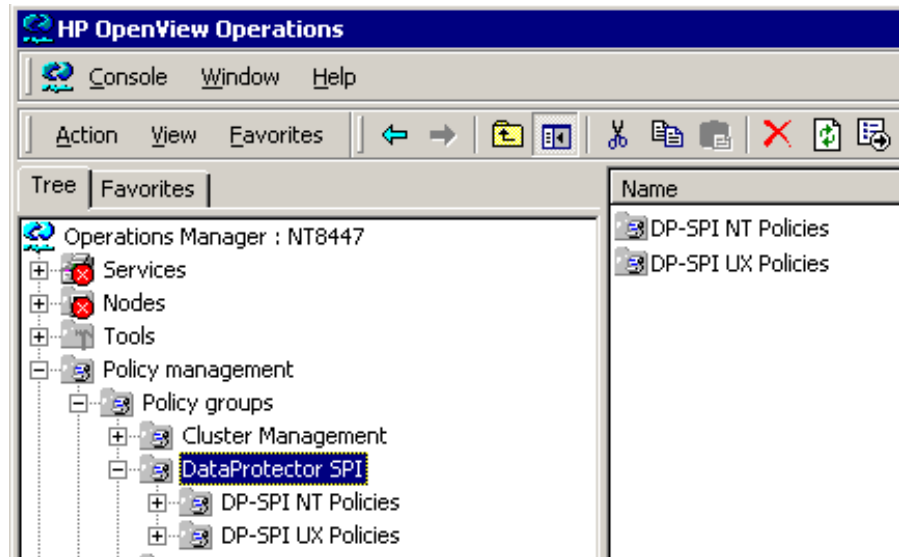
The sections in this chapter show which new components are added to OVO during the installation of the Data Protector Integration software and describe how to use them to best effect. This chapter provides detailed information about the following areas:

- “Data Protector SPI Policies”
- “Message Groups”
- “Node Groups”
- “Tools Groups”
- “Data Protector Service Tree”
- “Users and User Roles”
- “Monitored Objects”
- “Monitored Logfiles”

## Data Protector SPI Policies

The Data Protector Integration adds the DataProtectorSPI policy group to OVO. This is illustrated in Figure 3-1.

**Figure 3-1** Data Protector SPI Policy Groups



The DataProtectorSPI policy group contains two policy groups:

- DP-SPI NT Policies

Assigned by default to the DP NT MGRS node group for automatic deployment to any node added to this node group.

- DP-SPI UX Policies

Assigned by default to the DP UX MGRS node group for automatic deployment to any node added to this node group.

Run the Add DP Cell tool and the appropriate policy group is automatically deployed to the newly added Data Protector Cell Manager.

## Message Groups

A Message Group is used to categorize the messages in the OVO message browser. This allows you to filter only the messages of a certain category contained within the chosen Message Group. A Message Group and a Node Group in combination define the responsibility of an OVO Operator.

The Data Protector Integration installs six message groups that are specifically designed to handle messages generated by the policies and monitors started by the Data Protector Integration.

The Data Protector Integration generates a wide variety of messages. Where appropriate, the Data Protector Integration assigns relevant messages to existing OVO message groups. All those messages generated by the Data Protector Integration which do not obviously belong to existing OVO message groups are assigned to the following six Data Protector Integration-specific message groups:

|                |                                                                                                                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DP_Backup      | Backup session related messages                                                                                                                                                                                          |
| DP_Restore     | Restore session related messages                                                                                                                                                                                         |
| DP_Mount       | Mount request related messages                                                                                                                                                                                           |
| DP_Misc        | All other important Data Protector related messages                                                                                                                                                                      |
| DP_SPI         | Messages from the Data Protector Integration                                                                                                                                                                             |
| DP_Interactive | Detailed messages that are normally only displayed in the Data Protector GUI. This message group is disabled as default. Enable this message group if the greatest details about Data Protector's operation is required. |

## Message Format

An OVO message includes the following parameters:

|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                            |                                                                               |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>Message Group</b><br><br>The following message groups are available: | DP_Backup                                                                                                                                                                                                                                                                                                                                                                                  | Backup session messages.                                                      |
|                                                                         | DP_Restore                                                                                                                                                                                                                                                                                                                                                                                 | Restore session messages.                                                     |
|                                                                         | DP_Mount                                                                                                                                                                                                                                                                                                                                                                                   | Mount request messages.                                                       |
|                                                                         | DP_Misc                                                                                                                                                                                                                                                                                                                                                                                    | All other important Data Protector messages.                                  |
|                                                                         | DP_SPI                                                                                                                                                                                                                                                                                                                                                                                     | Data Protector Integration messages.                                          |
|                                                                         | DP_Interactive                                                                                                                                                                                                                                                                                                                                                                             | Detailed messages that are normally only displayed in the Data Protector GUI. |
| <b>Applications</b>                                                     | Set to Data Protector.                                                                                                                                                                                                                                                                                                                                                                     |                                                                               |
| <b>Node</b>                                                             | Set to the hostname of the Data Protector system the event occur.                                                                                                                                                                                                                                                                                                                          |                                                                               |
| <b>Severity</b>                                                         | Reflection of the impact that the event has on Data Protector. For SNMP trap derived messages, the severity value of the SNMP trap is used as the severity level of the message.                                                                                                                                                                                                           |                                                                               |
| <b>Service Name</b>                                                     | This depends on the impact the event has to a service. This value needs to map with a node in Data Protector's service tree.                                                                                                                                                                                                                                                               |                                                                               |
| <b>Object</b>                                                           | Allows the source of the event to be classified with fine granularity.<br><br>Data Protector SNMP traps set the object parameter to NOTIFICATION<br><br>Messages which origin from a: <ul style="list-style-type: none"> <li>• monitored logfile, set the Object parameter to the name of the logfile.</li> <li>• monitor, set the Object parameter to the name of the monitor.</li> </ul> |                                                                               |

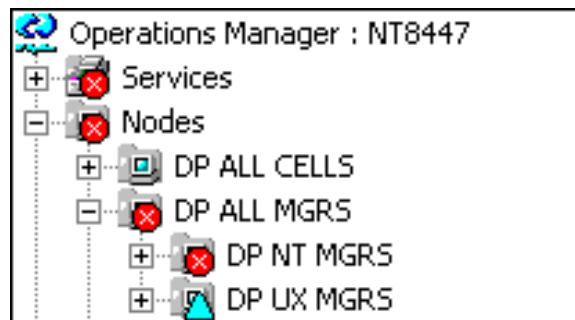
## Node Groups

Node groups are logical groups of systems or devices which are assigned in combination with message groups to an operator to manage. Each node group is represented by an icon in the Node Group Bank window. All systems within a node group can be viewed by opening the node group. A system may belong to more than one node group.

The Data Protector Integration provides the four Node Groups as illustrated in Figure 3-2:

- DP ALL CELLS
- DP ALL MGRS
- DP NT MGRS
- DP UX MGRS

**Figure 3-2** Data Protector Integration Node Groups



The Add Data Protector Cell action adds a node below the DP ALL MGRS node group. This node group is automatically created during installation.

Node groups are used to define the nodes from which a user receives messages. In combination with message groups, node groups define the:

- responsibilities of a user
- messages displayed to a user in the message browser

Node groups allow a flexible assignment to OVO Operators and convenient assignment of OVO Policies to groups of nodes. The predefined user roles of the Data Protector Integration use message groups and node groups.

The Data Protector Integration also provides the DP ALL CELLS node group by default. When the user adds a new DataProtector Cell Manager with the Add DP Cell application a Node Layout Group is included into the DP ALL CELLS node group.

There are two further node groups which are created during installation of the Data Protector Integration:

- DP NT MGRS
- DP UX MGRS

These can be used by any OVO administrator to help assign and distribute policies and monitors to all nodes of a selected operating system. If the cell administrator uses the Add Data Protector Cell application to create a new node, the node is automatically placed in the node group corresponding to its operating system.

## Tools Groups

Installation of the Data Protector Integration adds a new tools group, DPSPi to the OVO Tools folder. It contains the Data Protector-related tools as shown in Figure 3-3. Each OVO user role has a different set of Data Protector Integration applications to match the responsibilities of the OVO users who have been assigned one of these OVO user roles.

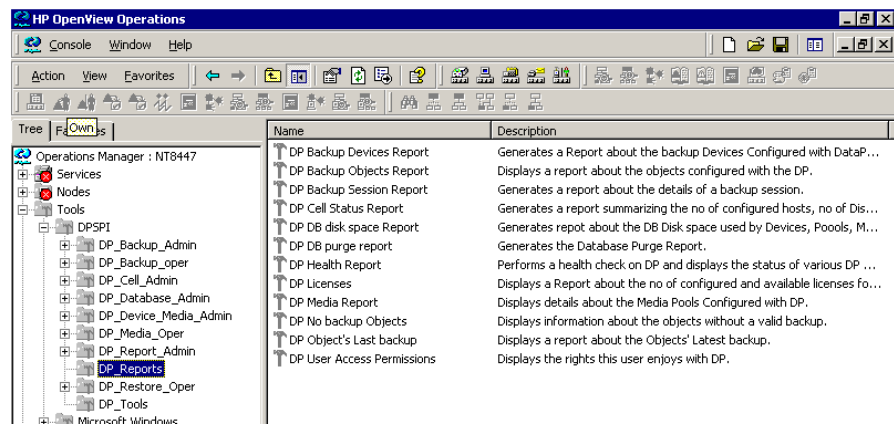
The other new Data Protector Integration tools groups is DP\_Reports. These tools groups are explained in greater detail in the sections that follow.

The tools have been conveniently grouped for assignment to user-roles loaded as part of the Data Protector Integration installation. The tools in the following two figures show all the tools available with the Data Protector Integration.

## DP\_Reports Tools Group

The Data Protector Integration tools group DP\_Reports contains tools which are intended to be used to monitor the health and performance of the Data Protector environment.

**Figure 3-3** Data Protector Integration Tools Group: DP\_Reports





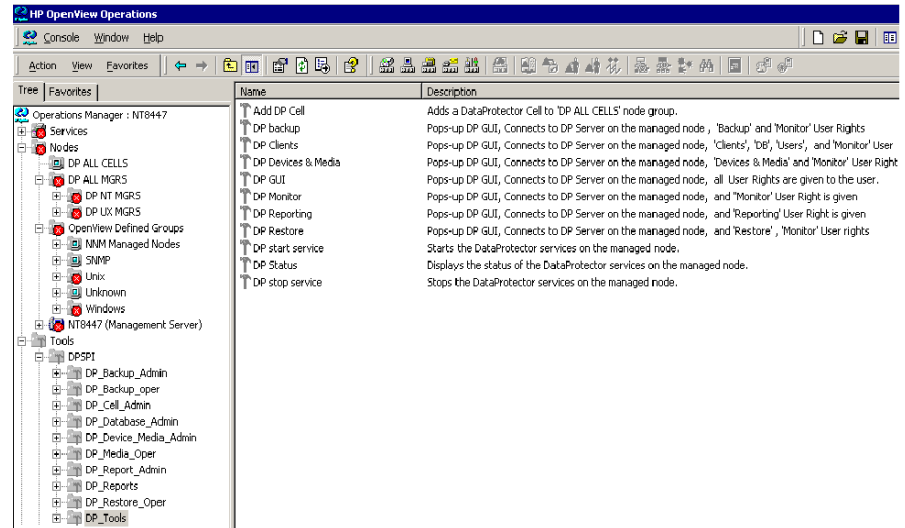
## DP\_Tools Tools Group

The Data Protector Integration application group DP\_Tools contains applications that are used to manage the Data Protector environment.

Figure 3-4 illustrates the applications contained in the DP\_Tools tools group.

Figure 3-4

## DPSPI Tools Group



## Using Tools and Reports

Usually tools execute on the management server or the managed nodes. The Add DP Cell tool runs on the system where the Console for the Management Server resides. The user name and password may be stored with the tool properties or you may have to enter them when you select to run the tool.

When you select a tool to be run and the target type for the tool is **Selected Node**, a window opens prompting you for the nodes on which to execute the application associated with the tool in the **Details** tab. If the **Allow Operator to change the login** is selected, you are also prompted to for a user name and password.

The following shows three representative examples:

**DP GUI:**

This invokes the Data Protector GUI by starting the Data Protector Console on the OVO Management Server. The Data Protector Console connects through port 5555 to the selected Data Protector Cell Manager.

**DP Cell Status Report:**

This starts the `omnicellinfo` command remotely on the OVO Managed Node/DP Cell Manager.

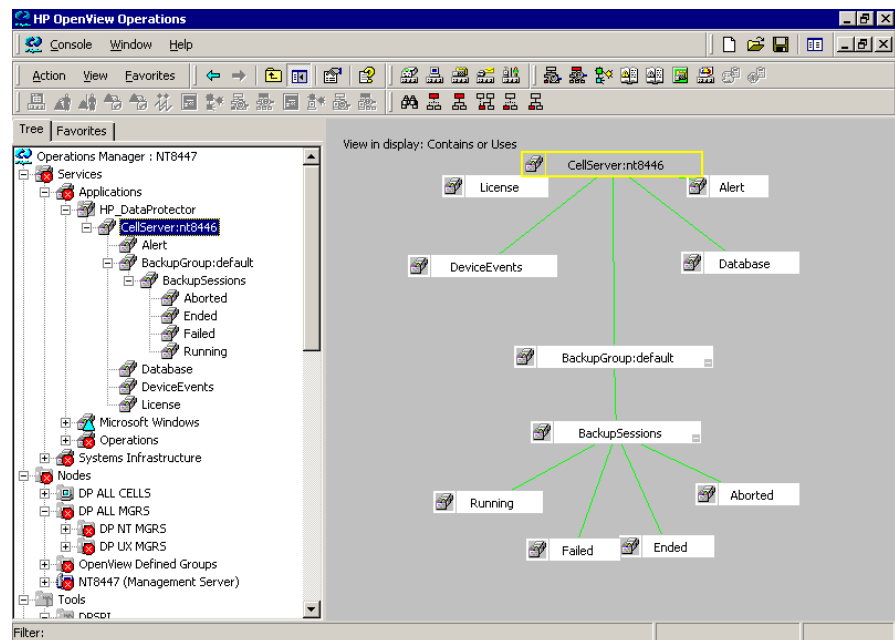
**DP Status:**

This starts the `omnisv -status` command remotely on the selected Data Protector Cell Manager.

## Data Protector Service Tree

Data Protector is represented as a service tree. Each Data Protector cell is represented by an icon within the Data Protector service. The service tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from the Data Protector Integration's monitors. Figure 3-5 illustrates the HP\_DataProtector service tree consisting of sub-tree for the Cell Manager :nt8446 Data Protector Cell Manager.

**Figure 3-5** The Data Protector Service Tree



The service tree for Data Protector Cell Managers is automatically created after the Add DP Cell tool is run and the DP\_Service\_Discovery policy is automatically deployed to the cell manager. On installing the Data Protector Integration, the following service tree type definition is loaded:

**Figure 3-6 The Data Protector Service Tree**

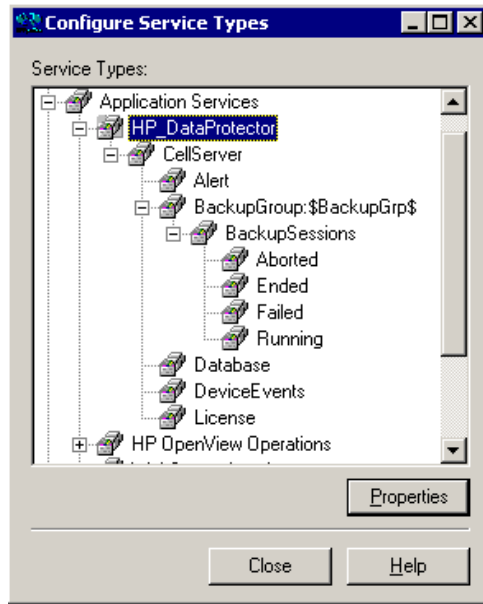


Table 3-1 lists the service tree nodes available for each cell.

**Table 3-1 Cell Service Tree Nodes**

| Node                            | Description                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Backup Group>. Backup Sessions | Contains Running, Waiting, Aborted, Failed, Completed, Completed with Failures, and Completed with Errors.<br><br>Data Protector sends SNMP traps to trigger the update of these items. |
| Running                         | Updated by Start of Session SNMP trap issued by Data Protector notification.                                                                                                            |

**Table 3-1 Cell Service Tree Nodes (Continued)**

| Node          | Description                                                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Waiting       | Updated by messages indicating that session is waiting due to: <ul style="list-style-type: none"> <li>• device being occupied</li> <li>• database is used</li> <li>• all licenses are currently allocated</li> <li>• too many backup sessions are running in parallel</li> </ul> |
| Aborted       | Updated by Session Aborted trap.                                                                                                                                                                                                                                                 |
| Failed        | Updated by Session Failed SNMP trap.                                                                                                                                                                                                                                             |
| Ended         | Updated by Session Completed, Completed with Errors, or Completed with Failures SNMP trap.                                                                                                                                                                                       |
| Database      | Updated by DB* SNMP traps issued by Data Protector notification and by messages resulting from database logfile monitoring.                                                                                                                                                      |
| Device Events | Updated by Device Error-, Mount Request-, Mail Slots-, and Full- SNMP traps issued by Data Protector notification.                                                                                                                                                               |
| Alert         | Updated by Alarm-, Health Check Failed-, User Check Failed-, Unexpected Events-, Not Enough Media- SNMP traps issued by Data Protector notification.                                                                                                                             |
| License       | Updated by License trap                                                                                                                                                                                                                                                          |

## Users and User Roles

This section explains the various user concepts in OVO, Data Protector and the Data Protector Integration. It also describes the users and roles installed by the Data Protector Integration and suggest the most appropriate uses for them.

### Data Protector and Operating System Users

The operating system user is used by Data Protector and OVO to provide access to users. In addition, Data Protector uses Data Protector user groups to define access rights for members of this group:

- **Operating System User**

Users required to login to the operating system. A valid user login is required before this user can start Data Protector or OVO. For example:

EUROPE\janesmith is a Windows user in the EUROPE domain.

uid=4110(janesmith) gid=60(marketing) is an UNIX user who's primary UNIX group is marketing.

- **Data Protector User Group**

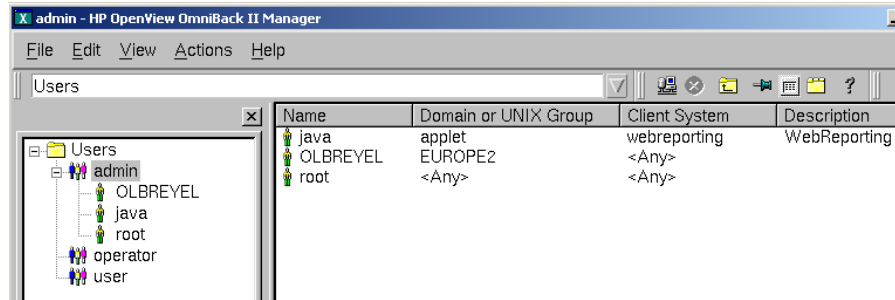
A Data Protector user group defines a set of Data Protector access rights that are available to members of this user group. A member of a user group is identified by its operating system user.

In Data Protector, the operating system user used to log in to the system belongs to a Data Protector user group which determines the access rights and the context of the Data Protector GUI for this user.

When the user starts the Data Protector GUI from **Tools**, the layout of the Data Protector GUI and the permissions this user has in Data Protector are determined by the operating system user.

Figure 3-7

## Windows Users



## Data Protector Integration Users

The operating system user is used by the Data Protector Integration. Data Protector Integration adds seven new user roles to the OVO User Roles configuration. For more information, please refer to “Data Protector OVO User Roles” on page 88. The role determines the layout of the OVO GUI:

- Applications available under **Tools**.
- Data Protector cell managers available under **Nodes**.
- Messages groups, in combination with node groups, are used for displaying Data Protector messages in the message browser.

---

### NOTE

When the OVO user starts the Data Protector GUI from **Tools**, the layout of the Data Protector GUI and the permissions this user has in Data Protector are determined by the operating system user.

---

## OVO User Roles

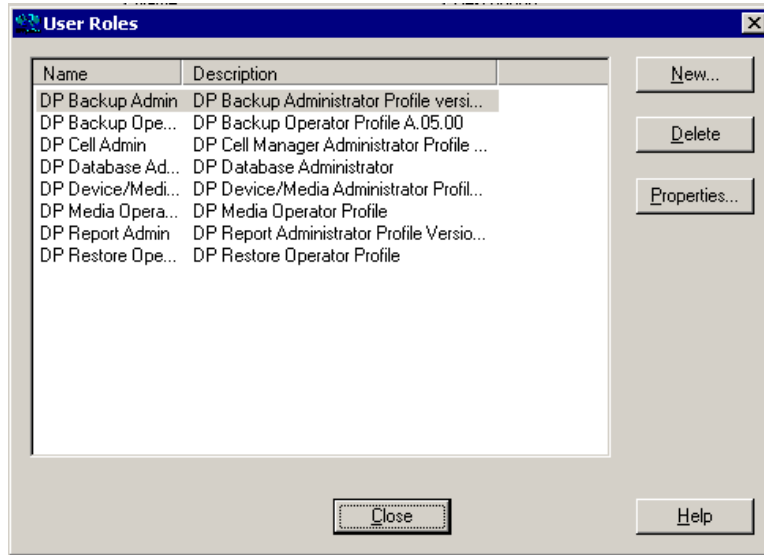
HP OpenView Operations describes the configuration of abstract users with User Roles. User roles are useful in large, dynamic environments with many OVO users and allow quick set up of OVO users with a default configuration. An OVO user may have multiple user roles assigned and therefore may simultaneously hold multiple roles.

The Data Protector Integration provides some default user roles suited for use with different OVO-Data Protector operator roles.

## Data Protector OVO User Roles

The installation of the Data Protector Integration software adds seven new user roles as illustrated in Figure 3-8. The OVO administrator uses user roles to assign responsibilities to OVO users.

**Figure 3-8** Data Protector Integration User Roles



Each of the above User Roles defines a custom subset of tools and a unique combination of the DP ALL MGRS node group with DP\_\* message groups. This defines the responsibilities of a user and the tools available to him.

The OVO user roles described in Table 3-2 are provided by the Data Protector Integration and can be used to implement the OVO user roles described in Table 3-3 on page 91:



**Table 3-2 Data Protector OVO User Roles**

| <b>Administrator / Operator Roles</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DP Backup Admin</b>                | <p>Restricted to a Data Protector Cell.</p> <p>The following Tool Groups are available:</p> <ul style="list-style-type: none"> <li>• DP_Backup_Admin</li> <li>• DP_Reports</li> </ul> <p>This administrator has access to messages in the OVO Message Browser, if the OVO message policy for detailed messages DP_Detailed is enabled.</p>                                                                                         |
| <b>DP Backup Operator</b>             | <p>Restricted to a Data Protector Cell.</p> <p>The following Tool Groups are available:</p> <ul style="list-style-type: none"> <li>• DP_Backup_Oper</li> </ul> <p>The Message Browser shows messages of the message groups:</p> <ul style="list-style-type: none"> <li>• DP_Backup</li> <li>• DP_Misc</li> <li>• DP_Mount</li> </ul> <p>These are backup session messages and mount requests of backup sessions messages.</p>      |
| <b>DP Restore Operator</b>            | <p>Restricted to a Data Protector Cell.</p> <p>The following Tool Groups are available:</p> <ul style="list-style-type: none"> <li>• DP_Restore_Oper</li> </ul> <p>The Message Browser shows messages of the message groups:</p> <ul style="list-style-type: none"> <li>• DP_Restore</li> <li>• DP_Misc</li> <li>• DP_Mount</li> </ul> <p>These are restore sessions messages and mount requests of restore sessions messages.</p> |

**Table 3-2 Data Protector OVO User Roles (Continued)**

| <b>Administrator / Operator Roles</b>         | <b>Description</b>                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DP Device/<br/>Media<br/>Administrator</b> | Restricted to a Data Protector Cell.<br>The following Tool Groups are available: <ul style="list-style-type: none"> <li>• DP_Device_Media_Admin</li> </ul> This administrator has access to messages in the OVO Message Browser, if the OVO message policy for detailed messages <code>DP_Detailed</code> is enabled.  |
| <b>DP Media<br/>Operator</b>                  | Restricted to a Data Protector Cell.<br>The following Tool Groups are available: <ul style="list-style-type: none"> <li>• DP_Media_Oper</li> </ul> The Message Browser shows mount requests of backup and restore sessions ( <code>DP_Mount</code> ) messages.                                                         |
| <b>DP Cell Admin</b>                          | Restricted to clients of Data Protector Cells.<br>The following Tool Groups are available: <ul style="list-style-type: none"> <li>• DP_Reports</li> <li>• DP_Tools</li> </ul> The Message Browser shows messages of the messages groups: <ul style="list-style-type: none"> <li>• DP_Misc</li> <li>• DP_SPI</li> </ul> |
| <b>DP Report<br/>Admin</b>                    | Restricted to Data Protector Cells.<br>The following Tool Groups are available: <ul style="list-style-type: none"> <li>• DP_Report_Admin</li> </ul> This Administrator is not shown any messages in the Message Browser.                                                                                               |

## Data Protector OVO Operators

The Data Protector OVO Operators use OVO to maintain, manage, monitor, and control multiple Data Protector cells from a single console. Table 3-3 defines the roles a Data Protector OVO Operator might have and describes the appropriate access rights of an equivalent Data Protector user.

---

**NOTE**

OVO users and Data Protector users are different and have to be set up in OVO and Data Protector separately.

OVO users are not created by the Data Protector Integration. The roles described in Table 3-3 are examples of possible roles you may create and use to manage Data Protector.

---

**Table 3-3** Data Protector OVO Operators and their Roles

| Role                        | Description & Data Protector Privileges                                                                      |                                                                                                                                                                                                                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Backup Administrator</b> | Creates backup specifications (what to backup, from which system, to which device) and schedules the backup. |                                                                                                                                                                                                                                                                                  |
|                             | Save backup specification                                                                                    | Allows a user to create, schedule, modify and save their own backup specification.                                                                                                                                                                                               |
|                             | Switch session ownership                                                                                     | Allows a user to specify the owner of the backup specification under which the backup is started. By default, the owner is the user who started the backup. Scheduled backups are started as root on a UNIX Cell Manager and under the Cell Manager account on a Windows system. |

**Table 3-3 Data Protector OVO Operators and their Roles (Continued)**

| Role                   | Description & Data Protector Privileges                                                                                                      |                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Backup Operator</b> | Starts a backup, if not scheduled, and monitors the status of backup sessions, and responds to mount requests by providing media to devices. |                                                                                                                                                                                                                                                                                  |
|                        | Start backup specification                                                                                                                   | Allows a user to perform a backup using a backup specification, so the user can back up objects listed in any backup specification and can also modify existing backup specifications.                                                                                           |
|                        | Backup as root                                                                                                                               | Allows a user to back up any object with the rights of the root login. This is a UNIX specific user right. It is required to run any backup on NetWare clients.                                                                                                                  |
|                        | Switch session ownership                                                                                                                     | Allows a user to specify the owner of the backup specification under which the backup is started. By default, the owner is the user who started the backup. Scheduled backups are started as root on a UNIX Cell Manager and under the Cell Manager account on a Windows system. |
|                        | Start backup                                                                                                                                 | Allows users to back up their own data, to monitor and abort their own sessions.                                                                                                                                                                                                 |
|                        | Mount request                                                                                                                                | Allows a user to respond to mount requests for any active session in the cell.                                                                                                                                                                                                   |
|                        | Monitor                                                                                                                                      | Allows a user to view information about any active session in the cell, and to access the Data Protector database to view past sessions. A user with monitor rights can use the Data Protector database context.                                                                 |

**Table 3-3 Data Protector OVO Operators and their Roles (Continued)**

| Role                    | Description & Data Protector Privileges                                                                                                                                                       |                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Restore Operator</b> | Starts restore on demand (from which device, what to restore, to which system), and monitors the status of the restore session, and responds to mount requests by providing media to devices. |                                                                                                                                                                                                                                     |
|                         | Restore to other clients                                                                                                                                                                      | Allows a user to restore an object to a system other than the one where the object was backed up.                                                                                                                                   |
|                         | Restore from other users                                                                                                                                                                      | Allows a user to restore objects belonging to another user. This is a UNIX specific user right.                                                                                                                                     |
|                         | Restore as root                                                                                                                                                                               | Allows a user to restore objects with the rights of the root UNIX user. Note that this is a powerful right that can affect the security of your system. This user right is required to run any restore on NetWare clients.          |
|                         | Start restore                                                                                                                                                                                 | Allows a user to restore own data, to monitor and abort own restore sessions. A user that has this user right is able to view their own and public objects on the Cell Manager.                                                     |
|                         | Mount request                                                                                                                                                                                 | Allows a user to respond to mount requests for any active session in the cell.                                                                                                                                                      |
|                         | Monitor                                                                                                                                                                                       | Allows a user to view information about any active session in the cell, and also allows a user to access the Data Protector database to view past sessions. A user with monitor rights can use the Data Protector database context. |

**Table 3-3 Data Protector OVO Operators and their Roles (Continued)**

| Role                                    | Description & Data Protector Privileges                                                                                                       |                                                                                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Device &amp; Media Administrator</b> | Creates and configures logical devices and assigns media pools to devices, creates and modifies media pools and assigns media to media pools. |                                                                                                                                                     |
|                                         | Device configuration                                                                                                                          | Allows a user to create, configure, delete, modify and rename devices. This includes the ability to add a mount request script to a logical device. |
|                                         | Media configuration                                                                                                                           | Allows a user to manage media pools and the media in the pools and to work with media in libraries, including ejecting and entering media.          |
| <b>Media Operator</b>                   | Responds to mount requests by providing media to the devices.                                                                                 |                                                                                                                                                     |
|                                         | Mount request                                                                                                                                 | Allows a user to respond to mount requests for any active session in the cell.                                                                      |

**Table 3-3 Data Protector OVO Operators and their Roles (Continued)**

| Role                        | Description & Data Protector Privileges                                                                                                                      |                                                                                                                                                                                                                                     |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cell Administrator</b>   | Installation and update of Data Protector client systems, add, delete, or modify Data Protector users and groups and administer the Data Protector database. |                                                                                                                                                                                                                                     |
|                             | Client configuration                                                                                                                                         | Allows a user to perform installation, and an update of client systems.                                                                                                                                                             |
|                             | User configuration                                                                                                                                           | Allows a user to add, delete and modify users or user groups. Note that this is a powerful right.                                                                                                                                   |
|                             | Monitor                                                                                                                                                      | Allows a user to view information about any active session in the cell, and also allows a user to access the Data Protector database to view past sessions. A user with monitor rights can use the Data Protector database context. |
|                             | See private object                                                                                                                                           | Allows a user to see private objects. This Data Protector user right has to be granted to database administrators.                                                                                                                  |
| <b>Report Administrator</b> | Create and modify Data Protector reports.                                                                                                                    |                                                                                                                                                                                                                                     |
|                             | Reporting and notifications                                                                                                                                  | Allows a user to create Data Protector reports. To use Web Reporting, you also need a java user under applet domain in the admin user group.                                                                                        |

---

## Monitored Objects

OVO monitors thresholds of an object to help early detection of problems. If an object exceeds a threshold for a specified period of time, a message can be sent to the OVO operator. This message enables the operator to resolve the problem before it affects the functionality of the system and the work of end users.

### Permanently Running Processes on the Cell Manager

The processes that run permanently on the Data Protector Cell Manager are:

- Cell Request Server (crs)
- Media Management Daemon (mmd)
- Raima Velocis Database Server (rds)

Only one instance of each process must be running.

Threshold:                      Number of processes <3

Polling interval:              10 min

Message structure:

|                                                     |                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <b>Message Group</b>                                | DP_Misc                                                         |
| <b>Applications</b>                                 | Data Protector                                                  |
| <b>Note</b>                                         | <name_cell_manager>.                                            |
| <b>Severity</b>                                     | Critical                                                        |
| <b>Service Name</b>                                 | Services.Data Protector.<cell name>                             |
| <b>Object</b>                                       | DP_CheckProc_NT on Windows<br>DP_CheckProc_UX on UNIX           |
| <b>Operator Action</b><br>in case of problem        | Start services                                                  |
| <b>Message Text</b><br>when problem has been solved | Auto acknowledge this message and the preceding problem message |



## Databases

Checks amount and percent of used available space.

Threshold:                >= 95% for error  
                               >= 80% for warning

Command:                 omnidbutil -extend info

Polling interval:        60 min

Message structure:

|                                                     |                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <b>Message Group</b>                                | DP_Misc                                                         |
| <b>Applications</b>                                 | Data Protector                                                  |
| <b>Note</b>                                         | <name_database_server>.                                         |
| <b>Severity</b>                                     | Critical                                                        |
| <b>Service Name</b>                                 | Services.Data Protector.<cell name>.Database                    |
| <b>Object</b>                                       | DP_CheckDB_NT on Windows<br>DP_CheckDB_UX on UNIX               |
| <b>Automatic Action</b><br>in case of problem       | Status of database                                              |
| <b>Operator Action</b><br>in case of problem        | Purge or extend the database                                    |
| <b>Message Text</b><br>when problem has been solved | Auto acknowledge this message and the preceding problem message |

## Media Pool Status

Checks if there are media pools with media status:

Poor                                      Critical  
 Fair                                        Warning  
 Polling interval:                      60 min

Message structure:

|                                                     |                                                                   |
|-----------------------------------------------------|-------------------------------------------------------------------|
| <b>Message Group</b>                                | DP_Misc                                                           |
| <b>Applications</b>                                 | Data Protector                                                    |
| <b>Note</b>                                         | <name_cell_manager>.                                              |
| <b>Severity</b>                                     | Critical or Warning                                               |
| <b>Service Name</b>                                 | Services.Data Protector.<cell name>                               |
| <b>Object</b>                                       | DP_CheckPoolStatus_NT on Windows<br>DP_CheckPoolStatus_UX on UNIX |
| <b>Operator Action</b><br>in case of problem        | Status of the Media Pool                                          |
| <b>Message Text</b><br>when problem has been solved | Auto acknowledge this message and the preceding problem message   |

## Media Pool Size

Checks the amount of used space:

Threshold:                >= 95% of total available space is Critical  
                               >= 85% of total available space is Warning

Command:                 omnim -list\_pool -detail

Polling interval:        60 min

Message structure:

|                                                     |                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <b>Message Group</b>                                | DP_Misc                                                         |
| <b>Applications</b>                                 | Data Protector                                                  |
| <b>Note</b>                                         | <name_cell_manager>.                                            |
| <b>Severity</b>                                     | Critical or Warning                                             |
| <b>Service Name</b>                                 | Services.Data Protector.<cell name>                             |
| <b>Object</b>                                       | DP_CheckPoolSize_NT on Windows<br>DP_CheckPoolSize_UX on UNIX   |
| <b>Operator Action</b><br>in case of problem        | Status of the Media Pool                                        |
| <b>Message Text</b><br>when problem has been solved | Auto acknowledge this message and the preceding problem message |

## Monitor Status of Long Running Backup Sessions

Checks if there are backup up sessions that have been running for longer than:

12 hrs (Critical)

8 hrs (Warning).

Polling interval: 60 min

Message structure:

|                                                     |                                                                                     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Message Group</b>                                | DP_Backup                                                                           |
| <b>Applications</b>                                 | Data Protector                                                                      |
| <b>Note</b>                                         | <name_database_server>.                                                             |
| <b>Severity</b>                                     | Critical or Warning                                                                 |
| <b>Service Name</b>                                 | Services.Data Protector.<cell name>.<backup group>.Backup Sessions.<session status> |
| <b>Object</b>                                       | DP_CheckLongBackup_NT on Windows<br>DP_CheckLongBackup_UX on UNIX                   |
| <b>Automatic Action</b><br>in case of problem.      | Session status                                                                      |
| <b>Operator Action</b><br>in case of problem        | Session report                                                                      |
| <b>Message Text</b><br>when problem has been solved | Auto acknowledge this message and the preceding problem message                     |

## Check Important Configuration Files

OB\_CheckFile\_NT starts `ob_spi_file.exe` on Windows nodes.

OB\_CheckFile\_UX starts `ob_spi_file.sh` on UNIX nodes.

### Windows Systems

Checks if the following files exist.

They are located in subdirectories of the Data Protector configuration directory, the default location being:

`C:\Program Files\OmniBack\Config\`

The usage of these files is described in:

- `cell\cell_info`
- `cell\cell_server`
- `cell\installation_servers`
- `users\userlist`
- `users\classspec`
- `users\webaccess`
- `snmp\OVdests`
- `snmp\OVfilter`
- `options\global`
- `options\trace`

Polling interval: 15 min

The value for `<OBHOME>` is read by `ob_spi_file.exe` from the registry key:

`HKLM\SOFTWARE\Hewlett-Packard\OpenView\DataProtector\`

`Common HomeDir <REG_SZ>: "C:\Program Files\DataProtector\"`

### HP-UX Systems

Checks if the following files exist. The usage of these files is described in:

- `/etc/opt/omni/cell/cell_info`
- `/etc/opt/omni/cell/installation_servers`
- `/etc/opt/omni/users/UserList`
- `/etc/opt/omni/users/ClassSpec`

## Monitored Objects

- /etc/opt/omni/users/WebAccess
- /etc/opt/omni/snmp/OVdests
- /etc/opt/omni/snmp/OVfilter
- /etc/opt/omni/options/global
- /etc/opt/omni/options/trace
- /etc/opt/omni/cell/cell\_server

Polling interval: 15 min

## Changing Monitor Parameters

Some of the monitors above have default parameters set in the `obspi.conf` file. This file resides on the Data Protector Cell Manager along with the monitor executables. These parameters may be altered by entering new values in the `obspi.conf` file.

The location of the file is:

**UNIX** /var/opt/OV/bin/instrumentation

**Windows** <OPENVIEW Installed Packages Dir>\bin\instrumentation

Examples of the default `obspi.conf` files are given below:

```
Windows: [OB_CheckFile_NT]
 \Config\cell\cell_info
 \Config\cell\installation_servers
 \Config\users\userlist
 \Config\users\classspec
 \Config\users\webaccess
 \Config\SNMP\OVdests
 \Config\SNMP\OVfilter
 \Config\Options\global
 \Config\Options\trace
 \Config\cell\cell_server

 [OB_CheckProc_NT]
 rds.exe
 crs.exe
 mmd.exe

 [OB_CheckLongBackup_NT]
 critical=12:00
 warning=08:00
```

```
UNIX: [DP_CheckFile_UX]
 /etc/opt/omni/cell/cell_info
 /etc/opt/omni/cell/installation_servers
 /etc/opt/omni/users/UserList
 /etc/opt/omni/users/ClassSpec
 /etc/opt/omni/users/WebAccess
 /etc/opt/omni/snmp/OVdests
 /etc/opt/omni/snmp/OVfilter
 /etc/opt/omni/options/global
 /etc/opt/omni/options/trace
 /etc/opt/omni/cell/cell_server

 [DP_CheckProc_UX]
 rds
 crs
 mmd

 [DP_CheckLongBackup_UX]
 critical=12:00
 warning=8:00
```

Use the OVO Policy Editor on the OVO Management Server to adjust the how often each monitor is started. If you change any OVO policy, it must be redistributed to the assigned systems before it becomes active.

## Monitored Logfiles

You can use OVO to monitor applications by observing their logfiles. You can suppress logfile entries or forward them to OVO as messages. You can also restructure these messages or configure them with OVO-specific attributes. For details, please refer to the OVO documentation and online help.

Four Data Protector logfiles are monitored for warning and error patterns. Basic information is provided in *HP OpenView Storage Data Protector Administrators' Guide*.

### Data Protector Default Logfiles

There are two default logfiles on every system where the Data Protector core is installed:

- `omnisv.log`
- `inet.log`

#### **omnisv.log**

This log is generated when `omnisv -start` or `omnisv -stop` is executed. The date/time format is fix and not language dependant. The format is:

YYYY-[M]M-[D]D [H]H:MM:SS - {START|STOP}

The parameters for messages for the default logfiles are:

|                         |                                                     |
|-------------------------|-----------------------------------------------------|
| <b>Message Group</b>    | DP_Misc                                             |
| <b>Applications</b>     | Data Protector                                      |
| <b>Note</b>             | <name_system> on which logfile resides              |
| <b>Severity</b>         | omnisv.log      NORMAL<br>inet.log          WARNING |
| <b>Service Name</b>     | Services.Data Protector.<cell name>                 |
| <b>Object</b>           | <logfile name>                                      |
| <b>Automatic Action</b> | Get status of cell manager processes                |



The following messages will be captured and forwarded to OVO's message browser:

```
2001-6-13 7:46:40 -STOP
HP OpenView Data Protector services successfully stopped.
2001-6-13 7:46:47 -START
HP OpenView Data Protector services successfully started.
```

### **inet.log**

This logfile provides security information. The messages document requests to the `inet` process from non-authorized systems. The data/time format depends on the value of the language environment variable. The following messages are captured and forwarded to OVO's message browser:

```
06/14/01 09:42:30 INET.12236.0 ["inet/allow_deny.c /main/7":524] A.04.00 b364
A request 0 came from host Jowet.mycom.com which is not a cell manager of this client
Thu Jun 14 09:42:30 2001 [root.root@jowet.mycom.com] : .util
06/14/01 09:43:24 INET.12552.0 ["inet/allow_deny.c /main/7":524] A.04.00 b364
A request 1 came from host jowet.mycom.com which is not a cell manager of this client
Thu Jun 14 09:22:46 2001 [root.sys@jowet.mycom.com] : .util
6/14/01 10:17:53 AM CRS.411.413 ["cs/mcrs/daemon.c /main/145":1380] A.04.00 b364
User LARS.R&D@cruise2000.mycom.com that tried to connect to CRS not found in user list
```

### **UNIX inet.log**

```
6/14/01 10:20:53 INET.12236. 0["inet/allow_deny.c /main/7":524] A.04.00 b364
Illegal command xxx
```

### **Windows inet.log**

```
6/14/01 10:20:53 INET.12236. 0["inet/allow_deny.c /main/7":524] A.04.00 b364
Unrecoverable error occurred (=core dump), exception code was: 0x*08x
6/14/01 10:20:53 INET.12236. 0["inet/allow_deny.c /main/7":524] A.04.00 b364
OmniInet service was teminated.
```

## Data Protector Database Logfile

There is a `purge.log` logfile on Cell Manager systems only. These systems contain a catalog and media management database.

### **purge.log**

This logfile contains purge session messages. Purge sessions are used to clean up the database. The data/time format depends on the value of the language environment variable. The following messages will be captured and forwarded to OVO's message browser:

```
06/17/01 15:42:15 ASM.1999 5.0 ["sm/asm/asm_purge.c /main/16":435] A.04.00 b364
Purge session started.
06/17/01 15:42:15 ASM.1999 5.0 ["sm/asm/asm_purge.c /main/16":445] A.04.00 b364
Filename purge session started.
06/17/01 15:42:16 ASM.1999 6.0 ["sm/asm/asm_purge.c /main/16":205] A.04.00 b364
Purge session finished.
06/17/01 15:42:16 ASM.1999 5.0 ["sm/asm/asm_msg.c /main/12":91] A.04.00 b364
Filename purge session ended.
```

The parameters for messages for the default logfiles are:

|                         |                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------|
| <b>Message Group</b>    | DP_Misc                                                                                |
| <b>Applications</b>     | Data Protector                                                                         |
| <b>Note</b>             | <name_system> on which logfile resides                                                 |
| <b>Severity</b>         | Purge start/finish messages      NORMAL<br>All other messages                  WARNING |
| <b>Service Name</b>     | Services.Data Protector.<cell name>.Database                                           |
| <b>Object</b>           | <logfile name>                                                                         |
| <b>Automatic Action</b> | omnidbutil -info                                                                       |

## Data Protector Media Logfile

There is a `media.log` logfile on the Data Protector Cell Manager.

### **media.log**

This logfile contains information about media:

- time
- medium id
- medium label
- type of operation or session id in which medium is used

The following messages will be captured and forwarded to OVO's message browser:

```
06/13/01 13:58:19 0a1104aa:3b27555a:4057:0001 "Default File_1" [INITIALIZATION]
06/13/01 14:30:33 0a1104aa:3b275ce9:6bb6:0001 "Default File_4" [INITIALIZATION]
06/14/01 14:38:43 0a1104aa:3b275ce9:6bb6:0001 "Default File_4" [2001/06/14-1]
06/18/01 14:05:14 0a1104aa:3b28a5f4:5e64:0001 "Default File_1" [2001/06/18-1]
06/19/01 10:44:23 AM b902110a:3b2727e1:00b9:0001 "Default File_3" [AUTOINITIALIZATION]
06/19/01 10:44:23 AM b90 2110a:3b2727e1:00b9:0001 "Default File_3" [2001/06/19-12]
06/21/01 1:38:13 PM 3578880f:3ce24f81:05c4:0001 "Default File_1" [IMPORT]
06/21/01 1:42:54 PM 3578880f:3ce39b3c:08fc:0001 "Default File_2" [COPY]
```

The parameters for messages for the default logfiles are:

|                      |                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------|
| <b>Message Group</b> | DP_Misc                                                                                                  |
| <b>Applications</b>  | Data Protector                                                                                           |
| <b>Note</b>          | <name_system> on which logfile resides                                                                   |
| <b>Severity</b>      | Operation type or session id exists   NORMAL<br>All other messages                               WARNING |
| <b>Service Name</b>  | Services.Data Protector.<cell name>                                                                      |
| <b>Object</b>        | <logfile name>                                                                                           |

## Logfiles Not Monitored by Data Protector Integration

The following logfiles either do not provide information relevant to the correct operation of Data Protector or the information is extracted from other sources, for example, SNMP traps.

|                             |                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>debug.log</code>      | Exception messages that have not handled.                                                                                                                                                                               |
| <code>RDS.log</code>        | Raima Database service messages.                                                                                                                                                                                        |
| <code>readascii.log</code>  | Messages generated during when the database is read from a file using <code>readascii</code> .                                                                                                                          |
| <code>writeascii.log</code> | messages generated when the database is written to a file with <code>writeascii</code> .                                                                                                                                |
| <code>lic.log</code>        | Unexpected licensing events.                                                                                                                                                                                            |
| <code>sm.log</code>         | Contains detailed errors during backup or restore sessions, i.e. error while parsing the backup specification. No message catalog is used. The time/date format differs depending on the language environment variable. |



In this chapter you will find introductory information on integrating the HP OpenView Storage Data Protector Integration into HP OpenView Performance:

- Storing of Performance data
- Configuration
- Installation
- De-installation

---

## Integration Overview

With the integration into HP OpenView Performance, the HP OpenView Storage Data Protector Integration gathers performance data from Data Protector and transfers it into the Performance Agent (OVPA) for processing. This processed data can then be displayed graphically by the HP OpenView Performance console.

---

### NOTE

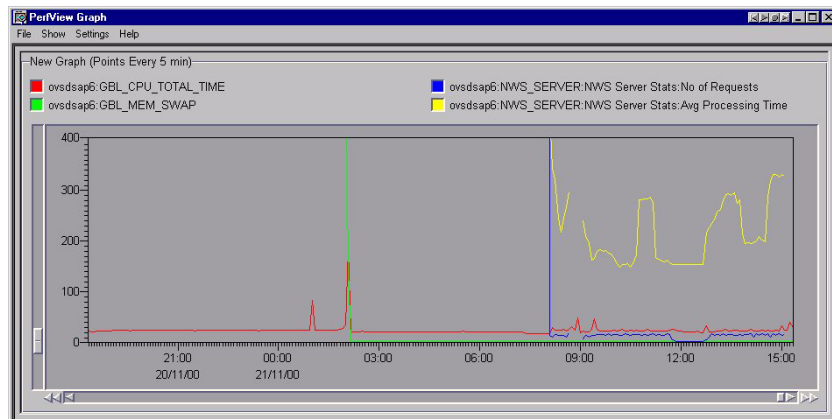
To be able to use the Performance Integration of the Data Protector Integration, the OVPA has to be running on all agent nodes running Data Protector Cell Managers.

---

The OVPA also collects many metrics from the operating environment, for example, I/O, network, and processes, and stores them in logfiles. Data Protector uses the ARM interface to measure the duration of transactions. These transaction durations are also collected by the HP OpenView Performance Agent. It is possible to direct additional sources of performance data into the OVPA via DSI (Data Source Integration) which is used to put performance data for the Data Protector environment into the OVPA. The collected data can be viewed centrally by the OVP Console to show trends and can also be combined with the internal data or data from other applications to get correlations, for example, to the CPU utilization or network data.

Figure 4-1

### HP OpenView Performance Console



**Integration Overview**

The performance measurement forms the basis for evaluating what corrective actions need to be made in order to optimize performance and resource utilization of the Data Protector environment. Typically, this is an off-line operation where a window of time is selected for detailed analysis of system performance, behavior and resource utilization.



## Installing Performance Integration Components

### Installation Steps for Window Nodes

After installation of the Data Protector Integration on the OVO management server the configuration files for the OVPA integration reside in the directory:

```
<HP OpenView Installation Directory>\install\DPSPi\vpp\4.0WINNT
```

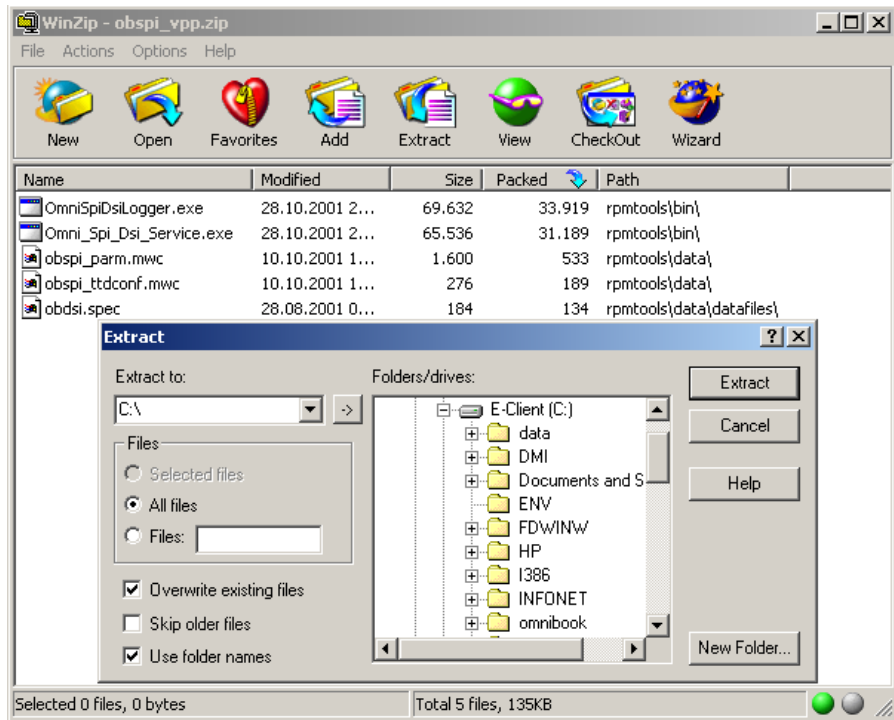
This directory contains the zip file named `obspi_vpp.zip` which contains all configuration files for Windows. There is no distribution functionality for the OVPA configuration files. The following manual steps are required.

1. Transfer the zip file to the managed node by using ftp.
2. Install the files in the OVPA directory. While unzipping the zip file, ensure that the files are copied to the appropriate OVPA directories. To do this:
  - a. Open the `obspi_vpp.zip` file with the WinZip application.
  - b. Select the parent directory of the OVPA Installation as the extraction directory, which is usually:  
`C:\`
  - c. Click the extract button to unzip the files to the chosen directories.

After unzipping, the following files are installed:

- `rpmtools\bin\OmniSpiDsiLogger.exe`
- `rpmtools\bin\Omni_Spi_Dsi_Service.exe`
- `rpmtools\data\obspi_parm.mwc`
- `rpmtools\data\obspi_ttdconf.mwc`
- `rpmtools\data\datafiles\obdsi.spec`

**Figure 4-2** Installing the Performance Integration



## Installation Steps for UNIX Nodes

After installation of the Data Protector Integration on the OVO management server, the configuration files for the OVPA integration reside in the one of the following directory depending upon the operating system of the managed node:

```
<HP OpenView Installation Dir>\install\DPSPI\vpp\11.0HPUX_PA32
<HP OpenView Installation Dir>\install\DPSPI\vpp\2.3 Solaris
```

These directories contains the tar file named `obspi_vpp.tar` which contains all associated configuration files for HP-UX or Solaris. There is no distribution functionality for the OVPA configuration files. The following manual steps are required.

1. Transfer the tar file to the managed node by using ftp.
2. Copy the file to the root directory
3. Use the tar command to decompress the archive:

```
tar -xf obspi_vpp.tar
```

After decompressing, the following files reside in the directory:

```
/opt/OV/OpC/integration/obspi/vpp/
```

- `obdsi.ksh`
- `obdsi.spec`
- `obspi_parm`
- `obspi_ttd.conf`

## Collecting ARM Transactions

Data Protector uses the ARM interface to measure the duration of Data Protector transactions. These can be collected by the HP OpenView Performance Agent. The following transaction time metrics are forwarded to the OVPA via the ARM interface:

- Overall session duration
- Restore session duration
- Object backup duration
- Database purge duration
- Database check duration

To enable ARM Transaction Tracking, the following files must be modified:

|                |                                        |
|----------------|----------------------------------------|
| <b>Windows</b> | <code>rpmtools\data\parm.mwc</code>    |
|                | <code>rpmtools\data\ttdconf.mwc</code> |
| <b>UNIX</b>    | <code>/var/opt/perf/parm</code>        |
|                | <code>/var/opt/perf/ttd.conf</code>    |

## Modifying the parm File

To modify the `parm` file to enable ARM transaction tracking:

1. Open the `parm` file in an editor.
2. Find the line which specifies the types of data that the OVPA is to log.

The entry has the form:

```
log global process application transaction dev=disk
```

3. Set transaction parameter to:

```
transaction=correlator
```

## Modifying the ttd.conf File

The default `ttd.conf` configuration file specifies that all ARM transactions instrumented within applications are to be monitored. To prevent this and to only collect the Data Protector ARM transactions modify the `ttd.conf` file as follows:

1. Before you make any changes to the `ttd.conf` file, shut down:

- HP OpenView Performance Agent service
- All ARM instrumented applications

See the HP OpenView Performance Agent handbook “Tracking your Transactions” for further information.

2. Open the `ttd.conf` file in an editor.

3. Delete the default line:

```
tran=* range=0.5,1,2,3,5,10,30,120,300 slo=5.0
```

4. Add the following lines to collect all Data Protector ARM transactions:

```
[HP OpenView Storage Data Protector]
```

```
tran=BS*
```

```
tran=RS*
```

```
tran=BO*
```

```
tran=DP
```

```
tran=DC
```

You can find the complete syntax for monitoring the Data Protector ARM transactions in the following files, after installation of the Data Protector OVPA integration:

**Windows** <Performance Agent Root>\Data\obsapi\_ttdconf.mmc

**UNIX** /opt/OV/OpC/integration/obsapi/vpp/obsapi\_ttd.conf

See Table 4-1 for an overview of the syntax.

**Table 4-1 ARM Transactions Syntax Overview**

| Transaction Name           | Additional Information                           | Transaction Description                       |
|----------------------------|--------------------------------------------------|-----------------------------------------------|
| BS-<Backup_specification > | Time                                             | Duration of a backup session                  |
| RS-<Session_ID>            | Time                                             | Duration of a restore session                 |
| BO-<Object_name>           | Time                                             | Duration of a backup of a specified object    |
| DP                         | Number of purged records and database size in MB | Duration of the Data Protector database purge |
| DC                         | Database size in MB                              | Duration of the Data Protector database check |

5. On HP-UX 11.x:

Replace the `/opt/omni/lib/arm/libarm.sl` with a softlink of the same name to `/opt/perf/lib/libarm.0`

6. After modifying the `ttd.conf` file, restart all ARM instrumented applications and the OVPA services.

Once these modifications are made to the `ttd.conf` file, you can collect transaction information about the task executed by Data Protector listed in Table 4-1.

## Collecting Data Protector Process Data

Data Protector runs processes dedicated to the specific tasks handled by the Cell Manager, the Media Agent, the Disk Agent, and the Installation Server. You can use the OVPA to collect process data from the various tasks. To do this, you must modify the `parm` file.

You can find the complete syntax for monitoring the Data Protector processes in the `parm` files which are located in:

**Windows**            <Performance Agent Root>\Data\obs\_pi\_parm.mmc

**UNIX**                /opt/OV/OpC/integration/obs\_pi/vpp/obs\_pi\_parm

directory after the installation of the Data Protector OVPA integration.

---

### NOTE

It is possible to collect process information about any nodes that are Data Protector clients, because a Data Protector Disk Agent or a Data Protector Media Agent runs on all Data Protector nodes.

---

## Modifying the `parm` File on a Data Protector Cell Manager

To enable OVPA to collect Data Protector Cell Manager process data, add the following application groups to the `parm` file on the Data Protector Cell Manager node:

```
application CellManager_Daemon
file crs mmd rds OmniInet
application CellManager_Session
file bsm rsm msm psm dbm
```

## Modifying the `parm` File on a Data Protector Media Agent

To enable OVPA to collect Data Protector Media Agent process data, add the following application groups to the `parm` file on the Data Protector Media Agent node:

```
application Media_Agent
file bma rma mma
```

## **Modifying the parm File on a Data Protector Disk Agent**

To enable OVPA to collect Data Protector Disk Agent process data, add the following application groups to the parm file on the Data Protector Disk Agent node:

```
application Disk_Agent
file vbda vrda rbda rda fsbrda dbbda OmniInet
```

## **Modifying the parm File on a Data Protector Installation Server**

To enable OVPA to collect Data Protector Installation Server process data, add the following application groups to the parm file on the Data Protector Installation Server node:

```
application Installation_Server
file OmniInet bmsetup
```



## Performance Agent Data Source Integration

The Data Protector OVPA Integration can collect further information about Data Protector and feed them via the `dsilog` interface into the OVPA.

DSI technology allows you, via its `dsilog` process, to use OVPA to log data and access metrics from new sources of data beyond the metrics logged by the OVPA collector. The `dsilog` process stores the data in a format that allows offline viewing and analysis by OpenView products such as HP OpenView Performance Console.

The metrics collected are:

- Number of clients controlled by the Data Protector Cell Manager
- Size of the database used by the Data Protector Cell Manager

To collect these metrics, you must complete the following steps:

- Compile the `obdsi.spec` class specification file with the OVPA command `sdlcomp` to acquire the logfile set for logging the data.
- Collect the data and use the `dsilog` interface to store them in the OVPA database.

### Compiling the `obdsi.spec` File

To be able to store the collected data in the OVPA database, you must create a logfile set. To create the logfile set, you must compile the class specification file `obdsi.spec` with the OVPA command `stdlcomp`. The `obdsi.spec` files are located in the following directories after the installation of the Data Protector OVPA integration:

**Windows**            <Performance Agent Root>\Data\Datafiles

**UNIX**                /opt/OV/OpC/integration/obspi/vpp/

The `sdlcomp` command has the following syntax:

```
sdlcomp specification_file logfile_set
```

`specification_file` Name of the class specification file. If it is not in the current directory, it must be fully qualified.

`Logfile_set` Name of the logfile set. For the Data Protector Data Source Integration, the name *must* be **omniback**.

If you do not specify a path, the logfile set is created in the current directory. There is no restriction to where you choose to store your logfiles during compilation, but you *must not* move them once they have been compiled.

An example of the usage of the `sdlcomp` command for compiling the Data Protector specification file:

#### **Windows**

```
sdlcomp obdsi.spec C:\rpmtools\data\datafiles\omniback
```

#### **UNIX**

```
sdlcomp obdsi.spec /var/opt/perf/datafiles/omniback
```

For further information see the HP OpenView Performance Agent Data Source Integration Guide.

## **Collecting Data on Windows Nodes**

### **Installing the Data Protector DSI Log Service**

In order to collect the Data Protector data and store it in the compiled logfile set on Windows systems, you must install the Data Protector DSI Log service.

After the installation of the Data Protector OVPA integration, the service installation file `omni_spi_dsi_service.exe` resides in the directory:

```
<Performance Agent Root>\Bin
```

To install the Data Protector DSI Log service, type the following command:

```
Omni_spi_dsi_service.exe -i
```

This registers the service in the Service Control Manager.

To check if the installation was successful, look for the service:

**Start → Settings → Control Panel → Administrative Tools → Services**

If you find the Data Protector DSI Log service listed, the installation was successful.

### Starting the Data Protector DSI Log Service

To start collecting data, you must start the Data Protector DSI Log service in one of the following ways:

- Enter the command:

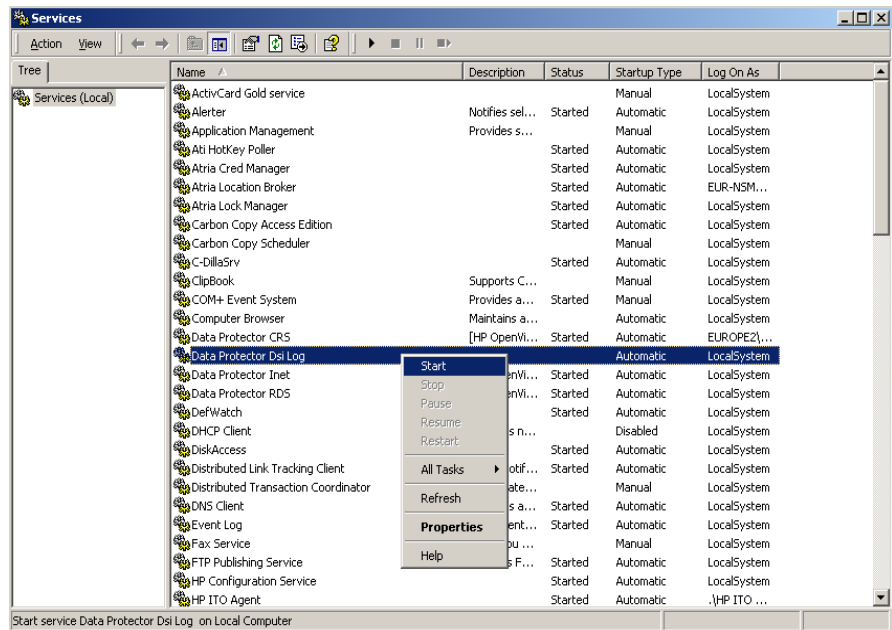
```
Omni_Spi_Dsi_Service.exe -s
```

- From the Service Control Manager GUI, go to:

**Start → Settings → Control Panel → Administrative Tools → Services**

and right-click the Data Protector Dsi Log service and select the start option in the context menu (see Figure 4-3 on page 123).

**Figure 4-3 Starting the Data Protector Dsi Log Service**



### Specifying the Data Collection Frequency

The default data collection frequency is 12 minutes. This is the same time configured in the `obdsi.spec` file which is used to create the OVPA logfile set. If you want to change the collection frequency, you need to change the appropriate entry in the `obdsi.spec` file (see *HP OpenView Performance Agent Data Source Integration Guide*), create a new logfile set using `sdlcomp`, and configure the Data Protector `Dsi Log` service accordingly.

To specify a new data collection frequency, you must do one of the following:

- Enter the command:

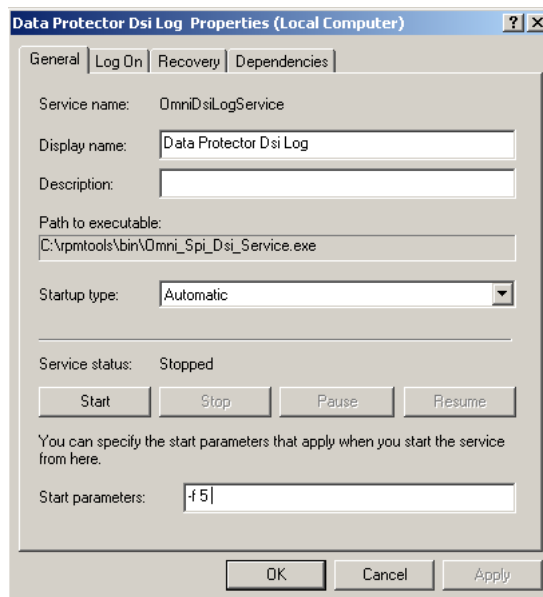
```
Omni_Spi_Dsi_Service.exe -s -f <minutes>
```

- From the Service Control Manager GUI, go to:

**Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**

and double click the Data Protector Dsi Log service, select the **General** tab and input the start parameter `-f minutes` in the textbox (see Figure 4-4).

**Figure 4-4** Specifying the Data Collection Frequency



## Configuring the Data Protector DSI Log Service

To enable tracing options for the Data Protector Dsi Log service, you must configure the service to provide the path of the trace file and the level of tracing information. You can do this with the command:

```
Omni_Spi_Dsi_Service.exe -t [TracePath]
```

Where `TracePath` is the fully qualified path of the trace files destination directory. This parameter is optional. If you do not specify a path, the default `temp` directory from the system environment (usually `C:\Temp`) is used.

If the `-t` option is not used to enable tracing, no trace files will be written.

To specify the type of information that is written to the trace files, you can configure the trace level for the Data Protector Dsi Log service. There are 4 tracing levels which contain the following information:

- Trace Level 1: Error Information.
- Trace Level 2: Function calls (shows call of internal functions).
- Trace Level 3: Shows information about the current service activities.
- Trace Level 4: Provides important internal data to check for correct resources and configuration.

If you used the `-t` option to enable tracing, the default tracing level is 1. To change the tracing level use the following command:

```
Omni_Spi_Dsi_Service.exe -v tracelevel
```

where the `tracelevel` value must be between 1 and 4.

The Data Protector Dsi Log service uses another executable, the `OmniSpiDsiLogger.exe` to collect the data. These executable reside after the installation in the:

```
<Performance Agent Root>\Bin
```

directory. By default, the service uses this directory to find the executable. So if you have relocated this file, you must specify the new path to the file. To do this use the command:

```
Omni_Spi_Dsi_Service.exe -x path/name
```

where `path` contains the fully qualified path and name of the file.

The configuration data is stored in the registry. It is possible to modify this data manually from the registry itself. The information is stored under the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OmniDsi
LogService
```

To disable tracing, you must remove the registry value:

```
TraceFilePath
```

from the registry key above.

### **Deinstalling the Data Protector DSI Log Service**

Before you can remove the files `Omni_Spi_Dsi_Service.exe` and `OmniSpiDsiLogger.exe`, you must uninstall the registered service. To do this use the command:

```
Omni_Spi_Dsi_Service.exe -u
```

### **Collecting Data on UNIX Nodes**

In order to collect the Data Protector data and store it in the compiled logfile set on UNIX nodes, you must make the `obdsi.ksh` script run as a shell-independent daemon.

To do this, use the UNIX `at` command as follows:

```
at now
```

```
'/opt/OV/OpC/integration/obspi/vpp/obdsi.ksh | dsilog
/var/opt/perf/datafiles/Omniback OMNIBACKII'
```

```
Ctrl-D
```

### **Performance Alarms for the Performance Agent**

No alarms based on these new metrics are defined, but the `alarmdef` file can be extended to define alarms using these new metrics for the MeasureWare agent.

---

# **5** **Reporter Light Integration**

In this chapter you will information on how to integrate into Reporter Light and create Data Protector reports. The chapter is divided into the following main sections:

- “Reporter Light Overview”
- “Reporter Light Integration with Data Protector Architecture”
- “Installing The Reporter Light Integration”
- “Using the Reporter Light Integration with Data Protector”
- “Preconfigured Reports”



## Reporter Light Overview

The Reporter Light is a simplified version of OpenView Reporter (OVR). It has the capability of generating Crystal format reports and is available as a part of OVO for Windows. The graphical user interface that is part of OVR is not included in Reporter Light.

The Reporter Light Integration With Data Protector contains utilities to obtain high-level Backup Session reports from Data Protector. The reports provided with this package give graphical representations of the backup session details of all the registered Data Protector management systems.

### Key Features

- It can directly Communicate with Data Protector to obtain data.
- Ability to view session trend reports and get an insight to the overall health of Data Protector cell servers over a selected period of time.
- Ability to view trend reports on the data backup, backup duration and number of files backed up.
- Reports the Error Status and Session Health details over a selected period of time
- Easy for administrators to predict the volume of data to be backed up in the future, as the trend reports shows the amount of data growth.
- Using the trends for the number of files backed up and amount of data backed up, administrators can calculate the optimum media block size.

### Standard Reports

The Reporter Light Integration With Data Protector provides the following 7 Reports:

- Backup Session Trend Report
- Backup Duration Trend Report
- Data Backup Trend Report
- Number of Files Trend Report

Reporter Light Integration  
**Reporter Light Overview**

- Skipped Files Report
- Backup Session Health Overview
- Operational Error Status Report

## Reporter Light Integration with Data Protector Architecture

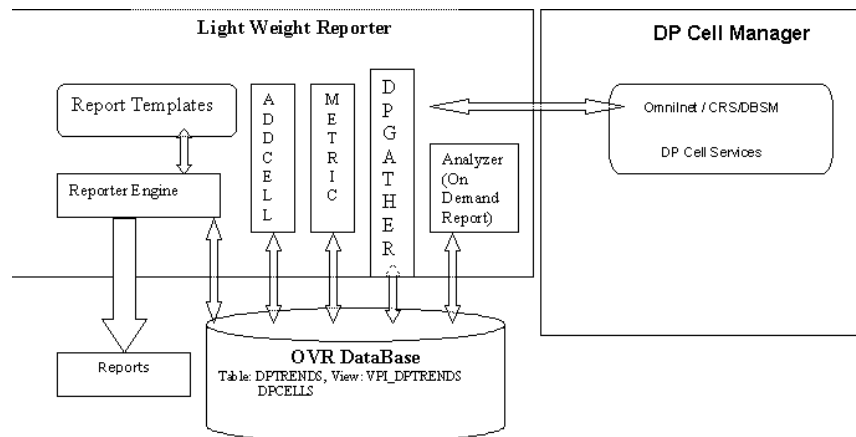
This Integration is completely installed on OVO for Windows. This Module can directly communicate with the Data Protector management System and obtain the necessary backup Session Details in order to generate the required Reports.

Both Windows and UNIX Data Protector Cell Manager can be accessed by this module and this module communicates with the following Data Protector processes to collect the backup session details and then stores this information in the OVO for Windows database:

- omniInet
- CRS
- DBSM

A high level representation of the integration is shown in Figure 5-1:

**Figure 5-1** Reporter Light Integration With Data Protector Architecture



## Data Flow

1. The Add Cell utility is used to register a Data Protector management server with this module.
2. Once the required Data Protector management server is registered with this module, the Gatherer (DPGather) supplied as a part of this package, is used to collect the required data from Data Protector and this data is added to the database.
3. The Reporter Engine of Reporter Light then generates the reports using the database and the templates.
4. These reports can then be viewed using a browser.

## Installing The Reporter Light Integration

Reporter Light Integration With Data Protector is available as a part of DPSPi.msi executable. It is installed as part of the HP OpenView Storage Data Protector Integration installation. It cannot be installed separately. The installation of the HP OpenView Storage Data Protector Integration installs all the templates and executables necessary for this integration.

During installation, the following directories are created on the OVO for Windows system, where, by default:

<INSTALL\_DIR> is C:\Program Files\HP Openview.

<INSTALL\_DIR>\bin                      Contains the Binaries  
required for this Integration

<INSTALL\_DIR>\newconfig\Packages      Contains XML and SRP files  
used for creating Database  
tables/views and to add the  
report Definitions

<INSTALL\_DIR>\data\reports\DP        Contains the Report  
Templates (used to Generate  
the Reports) and a  
ReadMe.txt file

### Installation Verification

To verify the installation:

1. Open the Add/Remove Programs window as follows:  
**Start → Settings → Control Panel → Add/Remove Programs**
2. Check that DPSPi-B.05.03 appears as an installed product.

### De-installation

Since this module is not installed independently, but installed as part of DPSPi-B.05.03 it cannot be de-installed separately. This module is de-installed when you de-install the DPSPi-B.05.03 product.

---

## Using the Reporter Light Integration with Data Protector

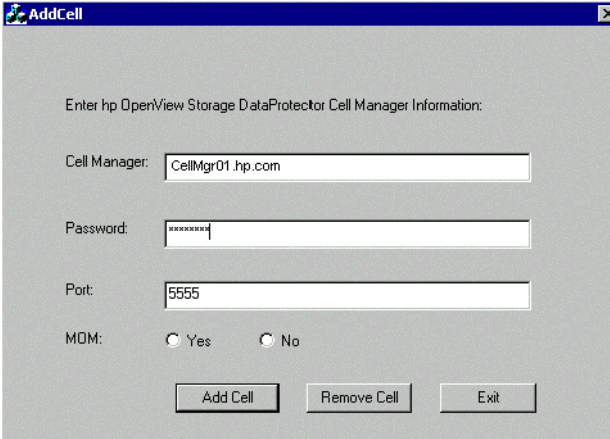
### Registering a Data Protector Cell Manager with this Module

In order to use this module, you must register the Data Protector Cell Manager with this module. An executable utility `AddCell.exe` available under `<INSTALL_DIR>\bin` is used to register the Data Protector Management System. You must first establish the following information:

- The hostname of the Data Protector Cell Manager.
- The port number of the omniInet process (default: 5555).
- Whether the Data Protector Cell Manager is a manager of managers system.
- Java user password (default: no password).

**Figure 5-2**

**Add Cell Window**



Enter hp OperView Storage DataProtector Cell Manager Information:

Cell Manager:

Password:

Port:

MDM:  Yes  No

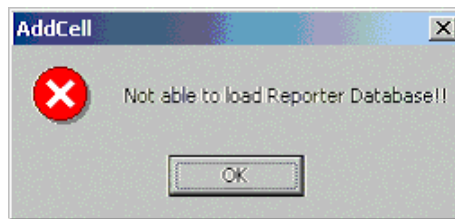
Use this utility to register (add) as many Data Protector Cell Manager as required.

### Troubleshooting Registering Cell Managers for Reporting

The following screenshots illustrate the possible error conditions that can be encountered while using this application and gives some possible solutions.

- If the application is not able to access the Reporter database, the following error message is displayed.

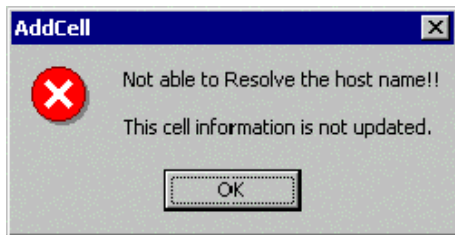
**Figure 5-3** Reporter Database Error



Make sure that the reporter database is accessible.

- If the application cannot resolve the host name the following error message is displayed:

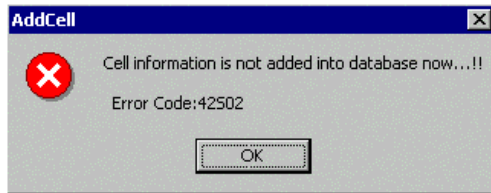
**Figure 5-4** Host Name Error



Make sure that the host system exists and is accessible.

- If the application cannot find the required database table, the following error message is displayed:

**Figure 5-5 Database Table Error**



Make sure that the database table DPCELLS is present.

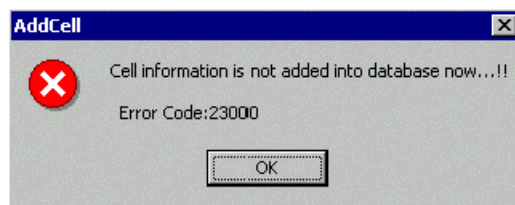
If the tables do not exist, create/recreate them using the following commands:

```
newdb -xml <INSTALL_DIR>\newconfig\Packages\DPCELLS.xml
and
```

```
newdb -xml <INSTALL_DIR>\newconfig\Packages\DPTREND.xml
```

- If a Data Protector Cell Manager is already registered (added) with this module, you cannot use this application to update the information.

**Figure 5-6 Cell Manager Update Error**

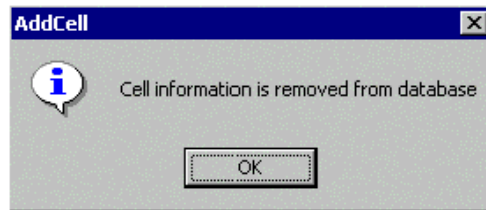


To add the same Data Protector Cell Manager, with different information, remove the existing information from the database and then add the new information.



- To remove (de-register) a Data Protector Cell Manager from this module, use the `AddCell.exe` application, enter the relevant details and then click the **Remove Cell** button.

**Figure 5-7** Add Cell Window



Once the Data Protector Cell Manager is removed (de-registered) from this module, data for reports can no longer be collected from this Cell Manager.

## Gathering Data from Data Protector

Once the Data Protector Cell Managers are registered to this module, the Backup Session Details must be obtained from the registered Data Protector Cell Managers. An executable utility `DPGather.exe` is used to collect data from registered Data Protector Cell Managers. There is no need to manually invoke this application, as it is automatically launched when required.

## Generating Reports

The Reporter Light contains an executable utility `Repccrys.exe`, used to generate reports. There is no need to manually invoke this application, as it is automatically launched when required.

## Viewing Reports

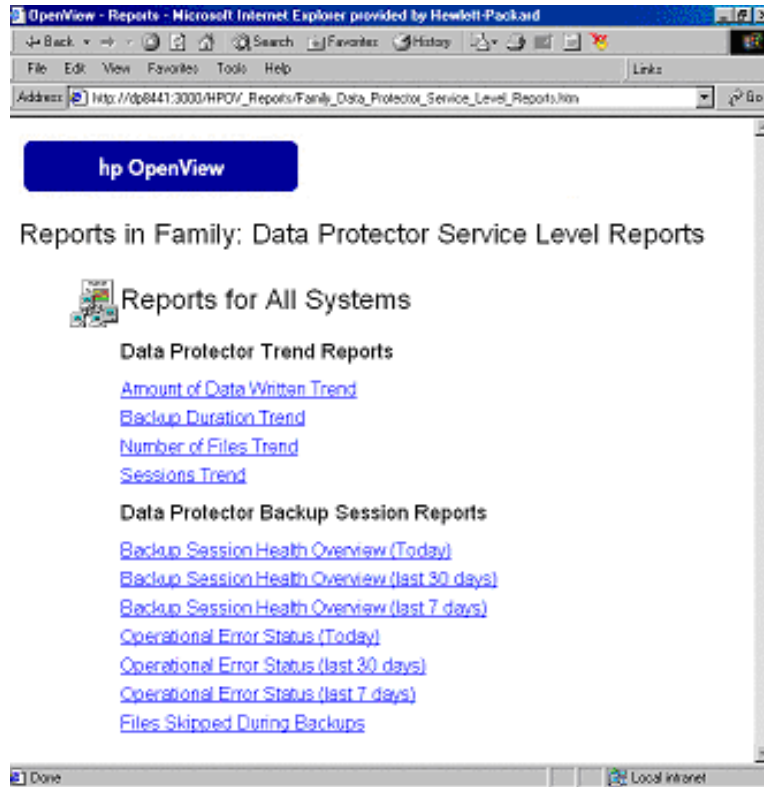
Use the following link to view the generated reports:

```
http://<OVO_SERVER>:PortNumber/HPOV_Reports/
Family_Data_Protector_Service_Level_Reports.htm
```

Where PortNumber is the port on which the web server is running.

**Figure 5-8**

### Reports Web Page



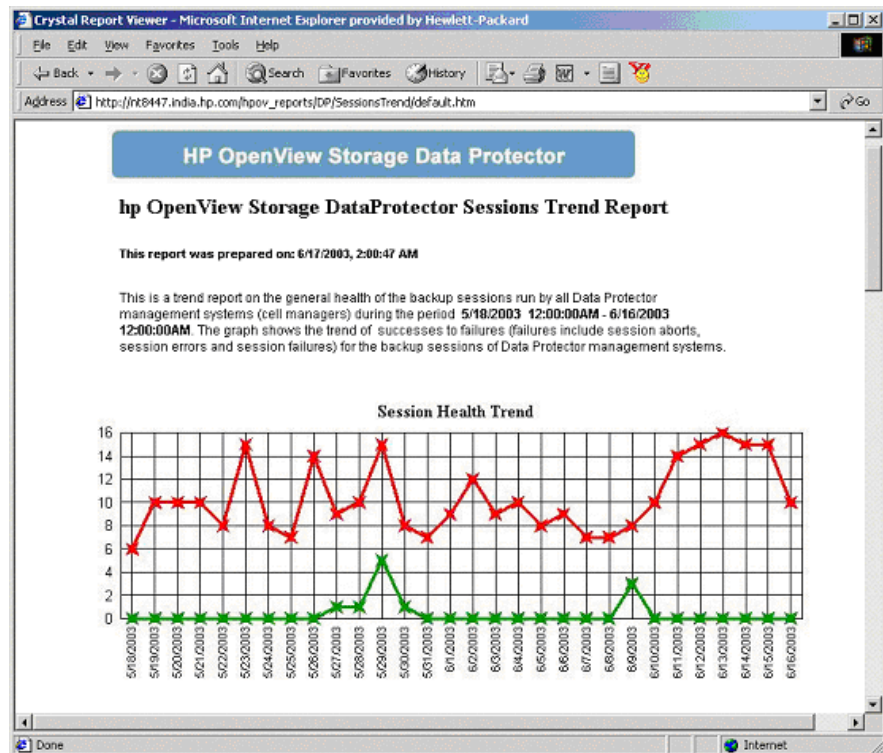
Click on the appropriate link to view the desired report.

## Preconfigured Reports

### Session Trend Report

Session Trend graph shows the trend of backup session success and failure over a period of time. The default period is 30 days. The date range is configurable by administrators. The trend graph contains overall sessions trend and individual cell manager trends.

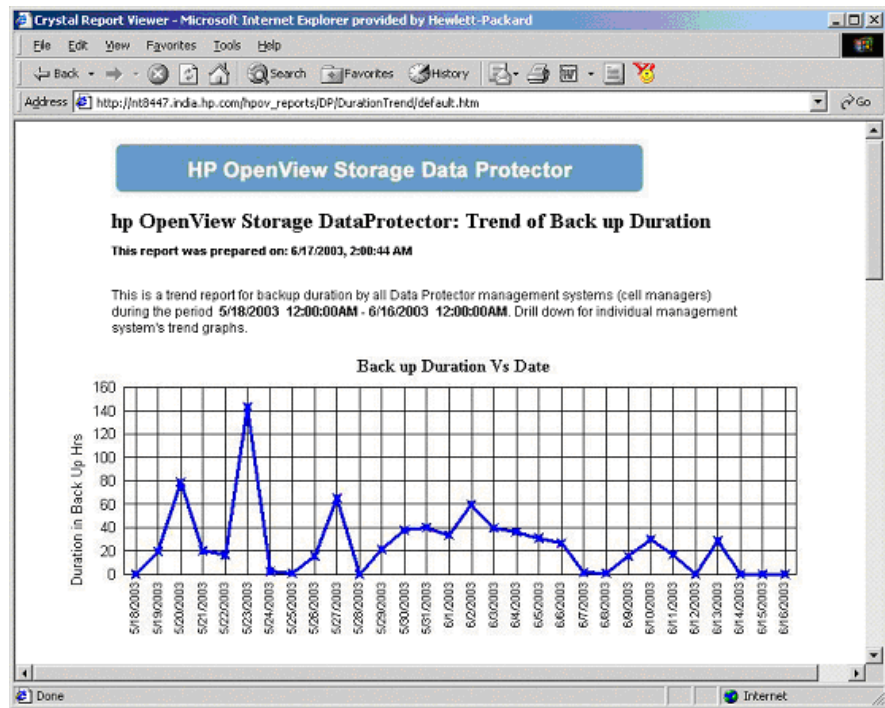
**Figure 5-9** Session Trend Report



## Backup Duration Trend

Backup Duration Trend report shows the trend of backup session duration in backup hours over a selected period of time. The default is 30 days. The date range is configurable by administrators.

**Figure 5-10** Backup Duration Trend Report

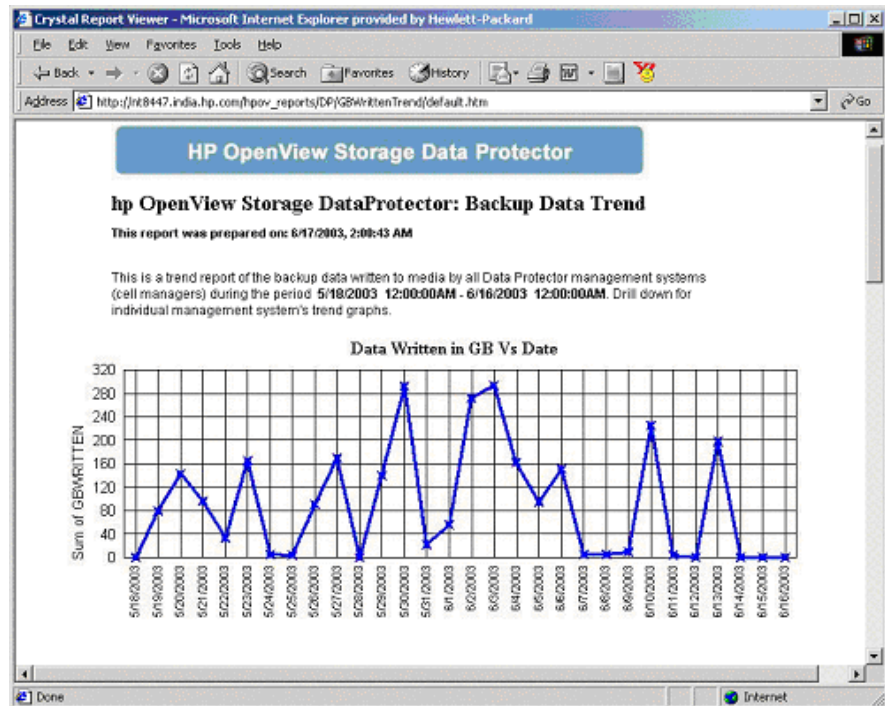


## Data Backup Trend Report

Data Backup Trend graph shows the trend of amount of data written to back up media over a selected period of time. The default is 30 days. The date range is configurable by administrators. The trend graph contains overall session trend and individual cell manager trends.

The amount of data written is displayed in Gigabytes (GB). To get the number of files backed up with the amount of data written in one graph, the On Demand report template is used. See “On Demand Report - Number of Files, Data Written and Date” on page 145.

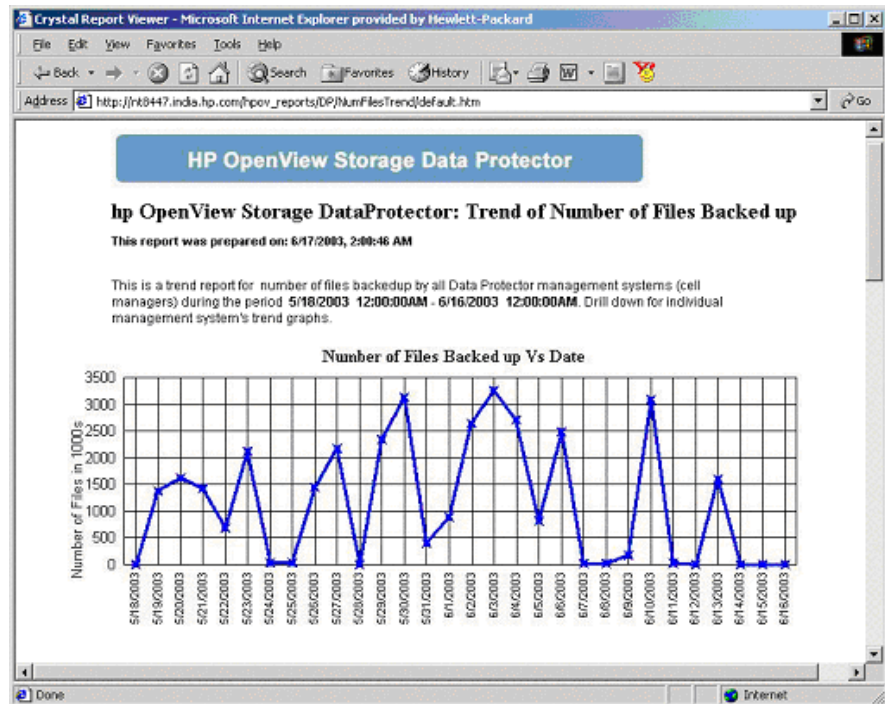
**Figure 5-11 Data Backup Trend Report**



## Number of Files Trend

Number of Files Trend graph shows the trend of the number of files (in 1000s) backed up over a selected period of time. The default is 30 days. The date range is configurable by administrators only. The trend graph contains overall session trend and individual cell manager trends.

**Figure 5-12** Number of Files Trend Report

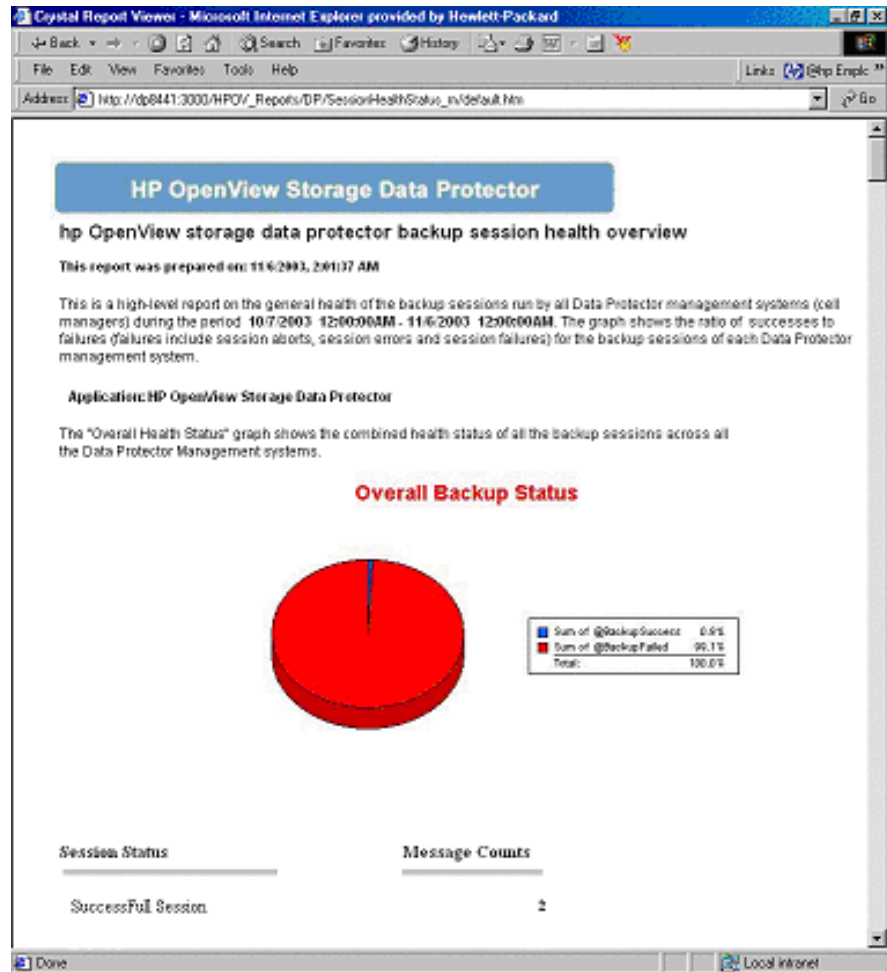


## Backup Session Health Overview

The Backup Session Health Overview graph shows the ratio of successes to failures (failures include session aborts, session errors and session failures) for the backup sessions of each Data Protector Management system.

One Graph is produced for each of the session run for the past month, week and day.

**Figure 5-13 Backup Session Health Overview Report**

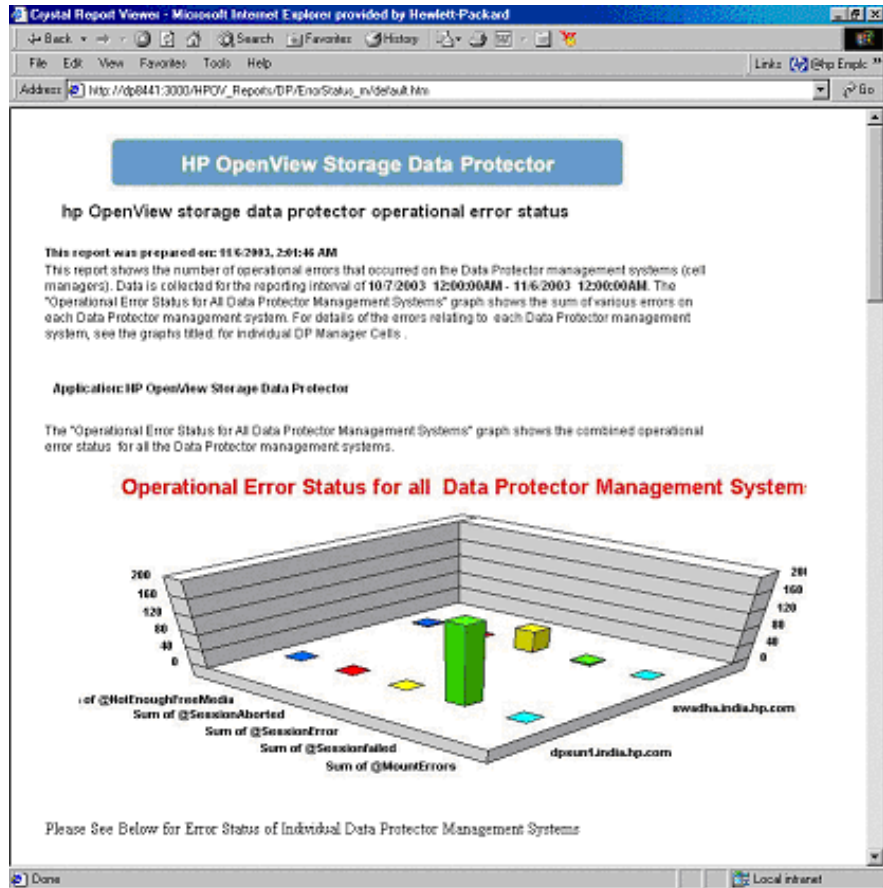


## Operational Error Status

The Operational Error Status report shows the number of operational errors that occurred on the Data Protector Cell Managers. The error status includes Session Aborted, Session Error, Session Failed, Mount Errors, Mount Request (Not Enough free Media).

Figure 5-14

### Operational Error Status Report





## Skipped Files Report

This report gives the list of the files which were not backed up during the backup Session.

Figure 5-15

### Skipped Files Report

**hp OpenView data protector Skipped Files Report**  
 This report was prepared on: Tue Nov 11 01:00:09 EST 2003  
 Note: If the Data Protector Management System name is not in the report, then there are no skipped files in that system. Also, if the session name is not present, then there are no skipped files for that session.

Application: hp OpenView data protector

| Cell Manager        | Session ID   | Client              | Skipped File Name                                                                                |
|---------------------|--------------|---------------------|--------------------------------------------------------------------------------------------------|
| rwedha.india.hp.com | 2003/11.07-2 | nt1670.india.hp.com | O:\win\Default User\15ulm15.at\parent.lock                                                       |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\DFC734.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm159.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm160.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm161.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm16F.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm16E.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\DF6027.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Temp\Acm1DE.tmp                                    |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Application Data\Microsoft\Windows\Users\Chazz.dat |
| rwedha.india.hp.com | 2003/11.07-2 | nt12150             | C:\Documents and Settings\MANU\Local Settings\Application                                        |

## On Demand Report - Number of Files, Data Written and Date

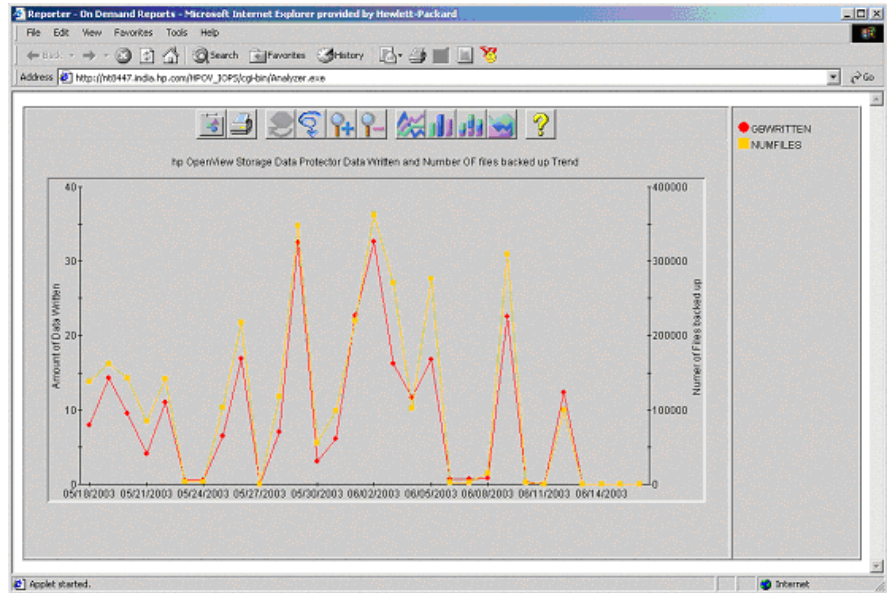
You can generate custom reports and standard reports. For standard reports the DataProtector template file is used with the following graph names:

- Sessions Trend

- GBWritten Over Number of Files backed-up

The sample graph GBWritten Over Number of Files backed-up is shown in Figure 5-16.

**Figure 5-16**      **On Demand Report**



---

# Index

---

## A

agent  
  configuration, 60  
  operations versions supported  
    by OVO, 52  
  performance versions  
    supported by OVO, 52  
alarms  
  OVPA, 126  
  performance agent, 126  
application  
  agents, 22  
  groups  
    DPSPI\_Applications, 81  
    DPSPI\_Reports, 80  
    using, 80  
architecture  
  Data Protector Integration, 45  
ARM transactions, 116

## B

backup  
  agent, 22  
  operation, 23  
  sessions, 24

## C

cell manager, 22  
  in Data Protector, 21  
  permanently running  
    processes, 96  
  prerequisites, 51  
cells  
  backup, 23  
  in Data Protector, 21  
  restore, 23  
clients in Data Protector, 21  
configuration  
  agent, 60  
  configuration files  
    monitoring, 101  
configuring

  DSI log service, 125  
conventions  
  typographical, 13

## D

Data Protector  
  application agents, 22  
  architecture, 21  
  backup agent, 22  
  cell, 21  
  cell manager, 21, 22  
    prerequisites, 51  
  client systems, 21  
  collecting process data, 119  
  command-line interfaces, 27  
  configuring the DSI log service,  
    125  
  deinstalling the DSI log  
    service, 126  
  devices, 21  
  disk agent, 22  
  drive server, 22  
  enterprise environment, 26  
  features, 17  
  functionality, 17  
  graphical user interface, 27, 28  
  installation servers, 22  
  installing the DSI log service,  
    122  
  manager-of-managers, 26  
  media agents, 22  
  miscellaneous configuration on  
    OVO managed nodes, 64  
  OVO operators, 91  
  OVO user profiles, 88  
  performance agent data  
    collection frequency, 124  
  performance agent data source  
    integration, 121  
  platforms, 49  
  service tree, 83

  starting the DSI log service,  
    123  
  user configuration on OVO  
    managed nodes, 64  
  user group, 86  
  versions, 49  
Data Protector Integration, 44  
  application groups, 80  
  DPSPI\_Applications, 81  
  DPSPI\_Reports, 80  
  architecture, 45  
  database logfiles, 106  
  default logfiles, 104  
  directories on OVO  
    management server, 56,  
    57  
  inet.log logfile, 105  
  installing on OVO  
    management server, 56  
  media logfiles, 107  
  media.log logfile, 107  
  message formats, 77  
  message groups, 76  
  monitored logfiles, 104  
  monitored object, 96  
  node  
    groups, 78  
  non-monitored logfiles, 108  
  omnisv.log logfile, 104  
  program identification, 64  
  purge.log logfile, 106  
  user profiles, 86  
  users, 87  
Data Protector user interfaces,  
  22  
data source integration, 121  
  collection frequency, 124  
database  
  monitor thresholds, 97  
deinstalling  
  DSI log service, 126  
depot

---

# Index

---

- installing on management server, 56
- devices in Data Protector, 21
- disk agent, 22
- disk space
  - installing on OVO server, 54
- DP\_Backup message group, 76
- DP\_Interactive message group, 76
- DP\_Misc message group, 76
- DP\_Mount message group, 76
- DP\_Restore message group, 76
- DP\_SPI message group, 76
- DPSPI\_Applications
  - application group, 81
- DPSPI\_Reports
  - application group, 80
- drive server, 22
- DSI log service
  - configuring, 125
  - deinstalling, 126
  - installing, 122
  - starting, 123
- F**
- formats
  - message, 77
- G**
- groups
  - application, 80
  - message, 76
  - node, 78
- H**
- hardware prerequisites
  - OVO management server, 51
- I**
- installation servers, 22
- installing
  - Data Protector Cell Manager prerequisites, 51
  - Data Protector Integration on OVO management server, 56
  - Data Protector versions, 49
  - depot, 56
  - disk space, 54
  - DSI log service, 122
  - management server patches, 51
  - OVO managed node prerequisites, 51
  - OVO management server
    - hardware prerequisites, 51
    - patches, 51
    - prerequisites, 50
    - software prerequisites, 51
  - OVPA integration components, 113
  - Performance integration
    - components, 113
    - prerequisites, 49
  - RAM, 55
  - verification, 58
- L**
- logfiles
  - Data Protector database, 106
  - Data Protector default, 104
  - Data Protector media, 107
  - inet.log, 105
  - media.log, 107
  - monitored, 104
  - not monitored, 108
  - omnisv.log, 104
  - purge.log, 106
- long running backup sessions, 100
- M**
- managed nodes
  - Data Protector user configuration, 64
  - miscellaneous configuration, 64
  - SNMP configuration on UNIX, 60
  - SNMP configuration on Windows, 61
  - management server
    - depot installation, 56
    - installation verification, 58
    - installing Data Protector Integration, 56
    - OVO, 39
    - patches, 51
  - media agents, 22
  - media pool size
    - monitor thresholds, 99
  - media pool status
    - monitor thresholds, 98
  - message formats
    - using, 77
  - message groups
    - DP\_Backup, 76
    - DP\_Interactive, 76
    - DP\_Misc, 76
    - DP\_Mount, 76
    - DP\_Restore, 76
    - DP\_SPI, 76
    - using, 76
  - monitored logfiles, 104
    - database logfiles, 106
    - default logfiles, 104
    - inet.log logfile, 105
    - media logfiles, 107
    - media.log logfile, 107
    - omnisv.log logfile, 104
    - purge.log logfile, 106
  - monitored object, 96
    - configuration files, 101
    - databases, 97
    - long running backup sessions, 100

---

# Index

---

- media pool size, 99
  - media pool status, 98
  - permanently running
    - processes on cell manager, 96
  - monitoring
    - configuration files, 101
  - N**
  - node
    - groups, using, 78
  - non-monitored logfiles, 108
  - O**
  - obspi.spec file, 121
  - operating system
    - users, 86
  - operators
    - Data Protector OVO, 91
  - OVO, 29
    - additional software for
      - Windows nodes, 53, 54
    - Data Protector
      - operators, 91
      - user profiles, 88
    - Data Protector Cell Manager
      - installation prerequisites, 51
    - Data Protector Integration
      - directories, 56, 57
    - managed nodes
      - Data Protector user configuration, 64
    - installation prerequisites, 51
    - miscellaneous configuration, 64
    - SNMP configuration on
      - UNIX, 60
    - SNMP configuration on Windows, 61
    - management server, 39
      - depot installation, 56
      - hardware prerequisites, 51
    - installing
      - prerequisites, 50
      - verification, 58
    - installing Data Protector Integration, 56
    - patches, 51
    - software prerequisites, 51
    - versions, 50
  - SNMP Emanate Agent for Windows nodes, 53
  - SNMP service for Windows nodes, 54
  - supported operations agent
    - versions, 52
  - supported performance agent
    - versions, 52
  - user profiles, 87
- OVPA
  - alarms, 126
  - data collection frequency for Data Protector, 124
  - Data Protector process data, 119
  - data source integration for Data Protector, 121
  - installing integration
    - components, 113
  - integration overview, 111
  - transaction times metrics, 116
- P**
- parm file, 116, 119
- patches
  - management server, 51
  - OVO management server, 51
- Performance
  - agent alarms, 126
  - agent versions supported by OVO, 52
  - installing integration
    - components, 113
  - integration overview, 111
  - transaction times metrics, 116
- prerequisites, 49
  - Data Protector cell manager, 51
  - OVO managed node, 51
  - OVO management server, 50
- process data, 119
- profiles
  - user, 86
- program identification
  - Data Protector Integration, 64
- R**
- RAM requirements
  - OVO server, 55
- restore
  - operation, 23
  - sessions, 25
- S**
- service
  - tree
    - Data Protector, 83
- Service Navigator
  - Data Protector service tree, 83
- sessions
  - backup, 24
  - restore, 25
- SNMP
  - configuration on UNIX OVO managed nodes, 60
  - configuration on Windows OVO managed nodes, 61
  - Emanate Agent Windows nodes, 53
- software
  - prerequisites
    - OVO management server, 51
- starting
  - DSI log service, 123
-

---

## T

- thresholds
  - monitored object, 96
- transaction times metrics, 116
- ttdconf file, 117

## U

- user
  - Data Protector Integration, 87
  - groups
    - Data Protector, 86
  - operating system, 86
  - profiles
    - Data Protector OVO, 88
    - OVO, 87
    - using, 86
- user interfaces, 22
  - Data Protector, 27
- using
  - application groups, 80
  - applications
    - DPSPI\_Applications, 81
    - DPSPI\_Reports, 80
  - Data Protector
    - database logfiles, 106
    - default logfiles, 104
    - inet.log logfile, 105
    - media logfiles, 107
    - media.log logfile, 107
    - omnisv.log logfile, 104
    - purge.log logfile, 106
  - message formats, 77
  - message groups, 76
  - monitored
    - logfiles, 104
    - object, 96
  - node
    - groups, 78
  - non-monitored logfiles, 108
  - user profiles, 86

## V

- verifying
  - management server
    - installation, 58

## W

- Windows nodes
  - additional software, 53, 54
  - SNMP Emanate Agent, 53
  - SNMP service, 54
- Windows User Interface
  - Data Protector, 28