

**HP OpenView Storage Data Protector
Integration Guide
for
HP OpenView Operations 7.5
for Windows**

Version: B.06.00



Manufacturing Part Number: B6960-96017

July 2006

Legal Notices

©Copyright 2006 Hewlett-Packard Development Company, L.P.

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

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

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

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California. UNIX® is a registered trademark of The Open Group. Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

UNIX® is a registered trademark of The Open Group.

Contents

1. Introduction

The Data Protector Integration	11
Data Protector Integration Architecture.....	12
Self-Healing Services	13

2. Installing the Data Protector Integration

Supported Platforms and Installation Prerequisites.....	17
Data Protector Supported Versions.....	17
OVO Management Server System.....	18
OVO Patches	18
Software Prerequisites on the OVO Management Server	18
Hardware Prerequisites on the OVO Management Server	19
Managed Node Systems (Data Protector Cell Manager)	19
Supported OVO Agent Versions	20
Supported HP OpenView Performance Agent Versions	20
Additional Software for HP-UX Managed Nodes	20
SNMP Emanate Agent (required)	21
Additional Software for Windows Managed Nodes	21
SNMP Service (required)	22
Disk-Space Requirements	22
Memory (RAM) Requirements	22
Installing the Data Protector Integration	23
Installation	23
Installation Verification.....	26
Running the Add Data Protector Cell Application.....	26
Agent Configuration.....	28
SNMP Configuration on UNIX.....	28
SNMP Configuration on Windows	30
Data Protector User Configuration	32
Program Identification.....	32
Uninstalling the Data Protector Integration.....	34
De-configuration Tasks	34

Contents

Undeploy All Data Protector Policies from Managed Nodes	34
Remove Data Protector Policies from the OVO Management Server	34
Remove Data Protector User Roles from the OVO Management Server	35
Remove the Data Protector Service Tree from the OVO Management Server	36
Remove the Data Protector Integration.	36

3. Using the Data Protector Integration

Data Protector SPI Policies	41
Message Groups	42
Message Format	43
Node Groups	44
Tools Groups	46
Using Tools and Reports.	47
Using Self-Healing Services	49
Tools.	49
Using DPSPi SHS Data Collector Self-Healing Services Client	49
Data Protector Service Tree.	55
Users and User Roles.	58
Data Protector and Operating System Users	58
Data Protector Integration Users	59
OVO User Roles.	59
Data Protector OVO User Roles.	60
Data Protector OVO Operators	63
Monitored Objects	67
Permanently Running Processes on the Cell Manager	67
Databases	68
Media Pool Status	70
Media Pool Size	71
Monitor Status of Long Running Backup Sessions.	72

Contents

Check Important Configuration Files	73
Windows Systems	73
UNIX Systems	74
Changing Monitor Parameters	74
Monitored Logfiles	77
Data Protector Default Logfiles	77
omnisv.log	77
inet.log	78
Data Protector Database Logfile	79
purge.log	79
Logfiles Not Monitored by Data Protector Integration	80
4. Performance Measurement with the HP OpenView Performance Agent	
Integration Overview	83
Installing Performance Integration Components	85
Installing on Windows Nodes	85
Installing on UNIX Nodes	86
Collecting ARM Transactions	87
Modifying the parm File	87
Modifying the ttd.conf File	88
Collecting Data Protector Process Data	90
Modifying the parm File on a Data Protector Cell Manager	90
Modifying the parm File on a Data Protector Media Agent	91
Modifying the parm File on a Data Protector Disk Agent	91
Modifying the parm File on a Data Protector Installation Server	91
Performance Agent Data Source Integration	92
Compiling the obdsi.spec File	92
Collecting Data on Windows Nodes	93
Installing the Data Protector DSI Log Service	93
Starting the Data Protector DSI Log Service	94
Configuring the Data Protector DSI Log Service	95

Contents

Uninstalling the Data Protector DSI Log Service	96
Collecting Data on UNIX Nodes.	97
Performance Alarms for the Performance Agent	97

5. ReporterLite Integration

ReporterLite Overview.	101
Standard Reports	101
ReporterLite Integration with Data Protector Architecture	103
Installing the ReporterLite Integration	105
Verifying Installation	105
Uninstalling.	105
Using the ReporterLite Integration with Data Protector	106
Registering a Data Protector Cell Manager with the Module	106
Troubleshooting	107
Gathering Data from Data Protector	108
Generating Reports	108
Viewing Reports	109
Preconfigured Reports	110
Session Trend Report	110
Backup Duration Trend Report	111
Amount of Data Written Trend Report	112
Number of Files Backed Up Trend by All Backup Groups Report.	113
Backup Session Health Overview Report	114
Operational Error Status Report	115
Skipped Files Report.	116
On Demand Report—Number of Files, Data Written and Date	117
Media Pool Usage Trend.	118
Successful Backup Trend	119
Backup Volume Usage Trend	120
Number of Files Backed Up Trend.	121

Printing History

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

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

Table 1

Edition History

Part Number	Manual Edition	Product
B6960-90089	April 2003	HP OpenView Storage Data Protector A.05.10
B6960-90119	October 2004	HP OpenView Storage Data Protector B.05.04
B6960-90018	July 2006	HP OpenView Storage Data Protector B.06.00

1 Introduction

This chapter provides an overview of the HP OpenView Storage Data Protector Integration, its key features and its architecture.

For descriptions of HP OpenView Storage Data Protector and HP OpenView Operations, see the *HP OpenView Storage Data Protector Concepts Guide* and the *HP OpenView Operations Concepts Guide*.

The Data Protector Integration

The Data Protector Integration enables you to monitor and manage the health and performance of your Data Protector environment using HP OpenView Operations (OVO) and the HP OpenView Performance Agent (OVPA).

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. It also assists system optimization well as service level monitoring.

The Data Protector Integration offers the following key features:

- HP OpenView Operations agents on a Data Protector Cell Manager system monitor the health and performance of Data Protector.
- A single OVO Management Server can monitor multiple Data Protector Cell Managers.
- The integration also depicts the functionality of Data Protector as a service tree.
- The ARM and DSI interfaces of the Performance Agent collect performance data and ARM transactions.
- Messages sent to OVO Management Server are channeled according to users' profiles. OVO users see only messages they need.
- The Data Protector Cell Manager and the OVO Management Server to be installed on different systems.
- You can run Data Protector functionality from the OVO Application Bank window.
- Data Protector Integration messages sent to the OVO management server includes instructions that help you correct the problem.
- Support for HP OpenView Self-Healing Services. See http://support.openview.hp.com/self_healing.jsp for information.

The main benefits of the integration are:

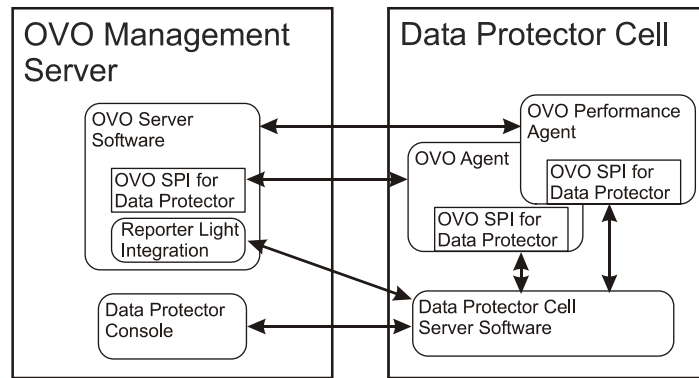
- Centralized problem management using OVO agents at Data Protector managed nodes. Using a central management server avoids duplicated administrative effort.
- Real-time event and configuration information (including online instructions) for fast problem resolution.
- Powerful monitors to detect potential problem areas and to keep track of system and Data Protector events.
- Performance data collectors to ensure continuous system throughput and notify any performance bottlenecks.
- Complements the Data Protector Administration GUI.
- Collection and monitoring of performance data.
- A central data repository for storing event records and action records for all Data Protector managed nodes.
- Utilities for running Data Protector management tasks.
- Allowing OVO users to start the Data Protector GUI and use Data Protector functionality from the OVO Management Server.
- Enabling users 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 ReporterLite integration that is part of OVO for Windows.

Data Protector Integration Architecture

The Data Protector Integration resides on the 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 1-1 Data Protector Integration Architecture



The Data Protector OVO policies monitor:

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

They are configured on the OVO agent on a Data Protector Cell Manager. The agent 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 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.

Self-Healing Services

HP OpenView Self-Healing Services provide a framework for the self-healing process:

1. The software detects a problem.
2. It collects relevant information relating to the problem.
3. The information is sent to HP, where it is analyzed for possible solutions.

4. A web page is published on eCare with the analysis results and any relevant documents relating to the problem.
5. You are sent an email notifying you a problem has been detected and a web page prepared.

You can then use the information on the web page to solve the problem. If this is unsuccessful, you can have a traditional support case opened automatically. The support engineer will have access to all the information collected by the Self-Healing Service, thus speeding the response.

See “Using Self-Healing Services” on page 49 for details of how the Self-Healing Services are used with DPSPI.

For more information on SHS see

<http://www.managementsoftware.hp.com/service/selfheal/index.html>.

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 Data Protector Integration components on OVO managed node (Data Protector Cell Manager) system.
- Uninstalling Data Protector Integration components from OVO managed node (Data Protector Cell Manager) systems.
- Uninstalling 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 installed on the same system on which the Data Protector Integration Console is to be installed.
- OVO agent running on systems with the Data Protector Cell manager.

Before installing the Data Protector Integration, ensure the following requirements are met:

Data Protector Supported Versions

The Data Protector Integration is designed to work with HP OpenView Storage Data Protector, versions 5.1, 5.5 and 6.0 on the following platforms:

Table 2-1 HP OpenView Storage Data Protector Availability

Operating System	Data Protector Version			
	5.0	5.1	5.5	6.0
HP-UX 11.00	✓	✓	✓	✓
HP-UX 11.11	✓	✓	✓	✓
HP-UX 11.23			✓	✓
Solaris 7	✓	✓	✓	✓
Solaris 8	✓	✓	✓	✓
Solaris 9		✓	✓	✓

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

Operating System	Data Protector Version			
	5.0	5.1	5.5	6.0
Solaris 10				✓
Microsoft Windows 2000	✓	✓	✓	✓
Microsoft Windows XP Professional (32-bit)	✓	✓	✓	✓
Microsoft Windows Server 2003		✓	✓	✓
SUSE Linux Enterprise Server 9 (x64)				✓

OVO Management Server System

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

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

Table 2-2 OVO Management Server Supported Versions

OVO Version and Operating System	OVO 7.5
<i>English and Japanese:</i> Microsoft Windows 2000, Windows 2003	✓

OVO Patches

Ensure up-to-date patches are installed.

Software Prerequisites on the OVO Management Server

Ensure 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

Ensure the following hardware prerequisites are met on the OVO management server system:

- 15 MB disk space on the HP OpenView Operations management server system

NOTE

The Data Protector Integration supports OVO installed in an MS Cluster environment. However the integration does not support Data Protector Cell Managers (managed nodes) in a Cluster environment.

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. 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

Ensure the Data Protector Cell Manager is installed on a platform for which the OVO Agent is available:

Table 2-3 HP OpenView Operations Agent Availability

OVO Agent Version	Operating System
7.5	HP-UX 11.00, 11.11, 11.23
	Solaris 7, 8, 9, 10
	Microsoft Windows 2000, Windows XP Pro (32-bit), Windows 2003
	SUSE Linux Enterprise Server 9.x (x64)

Supported HP OpenView Performance Agent Versions

Ensure Data Protector is installed on a platform for which the OVPA is available:

Table 2-4 HP OpenView Performance Agent Availability

Operating System	OVPA Version
HP-UX 11.00	C.03.70
HP-UX 11.11	C.03.70, C.03.86
HP-UX 11.23	C.03.86
Solaris 7, 8, 9	C.03.75, C.03.82
Microsoft Windows 2000, XP, 2003	C.03.65
SUSE Linux Enterprise Server 9.x (x64)	C.03.86

Additional Software for HP-UX Managed Nodes

The following software is required, but is not installed as part of the OVO management server installation nor as part of the Data Protector Integration installation.

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 because SNMP traps are processed 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 involving the management server
- Since SNMP traps are not sent from the managed node to the management server, the network load decreases, and the probability that traps are lost is significantly reduced. Security over public networks is also improved. OpC messages are sent by the OVO agent to the OVO management server using either HTTPS and DCE/RPCs, which allow authentication and encryption.

Check the SNMP Emanate Agent is installed on the Data Protector Cell Manager node:

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

You should see the following type of entry:

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

Additional Software for Windows Managed Nodes

The following software is required but is not installed as part of the OVO management server installation nor as part of the Data Protector Integration installation:

SNMP Service (required)

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

Disk-Space Requirements

The following table lists 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 on the managed node.

Machine	OVO Version	Operating System	Total
OVO Management Server	OVO 7.5	Windows 2000, 2003	15 MB
OVO Managed Node	OVO 7.5	HP-UX 11.00, 11.11, 11.23	2 MB
		Solaris 7, 8, 9, 10	2 MB
		Supported Microsoft Windows Nodes	2 MB
		SUSE Linux Enterprise Server 9	2 MB

Memory (RAM) Requirements

There are no specific requirements for RAM on 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 DPSPPI_OVOW75-B.06.00.msi MSI package used to install the 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. Agent software and 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 DPSPPI_OVOW75-B.06.00.msi executable file.

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

c:\Program Files\HP OpenView	
<INSTALLDIR>\install\DPSPPI\	Installation directory with subdirectories for policies and OVO configuration files
<INSTALLDIR>\install\DPSPPI\vpp\ <Platform>	DSI performance agent integration
<INSTALLDIR>\bin\	Binary and script files
<INSTALLDIR>\Instrumentation\ <Platform>\<Version>\SPI for DataProtector\	Monitor scripts and configuration files
<INSTALLDIR>\Instrumentation\ <Platform>\<Version>\DP-SPI Discovery\	Service discovery scripts and configuration files
<INSTALLDIR>\NLS\1033\Manuals\	Documentation containing this <i>Integration Guide</i> and the <i>Product Announcements, Software Notes, and References</i>

Installing the Data Protector Integration

Installing the Data Protector Integration

The following directories are created on a Data Protector Cell Manager running on UNIX after the Data Protector Policies and Monitors have been deployed to it:

In `/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`
- `ob_spi_medialog.sh`
- `ob_spi_omnisvlog.sh`
- `ob_spi_purgelog.sh`
- `obspi1.conf`
- `obspi2.conf`
- `spi_datapro.sh`
- `spi_datapro.xml`
- `spi_datapro_input.xml`
- `spi_datapro_install.xml`
- `spi_datapro_reg.xml`
- `spi_datapro_runSHSCollector.xml`
- `spi_datapro_task.xml`

The following directories are created on a Data Protector Cell Manager running on Windows 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-080009Ef8C2A}
```

In `<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
- ob_spi_medialog.vbs
- ob_spi_medialog.bat
- ob_spi_omnisvlog.vbs
- ob_spi_omnisvlog.bat
- ob_spi_purgelog.vbs
- ob_spi_purgelog.bat
- obspi1.conf
- obspi2.conf
- spi_datapro.cmd
- spi_datapro.xml
- spi_datapro_input.xml
- spi_datapro_install.xml
- spi_datapro_reg.xml
- spi_datapro_runSHSCollector.cmd
- spi_datapro_task.xml

Installation Verification

To verify the installation:

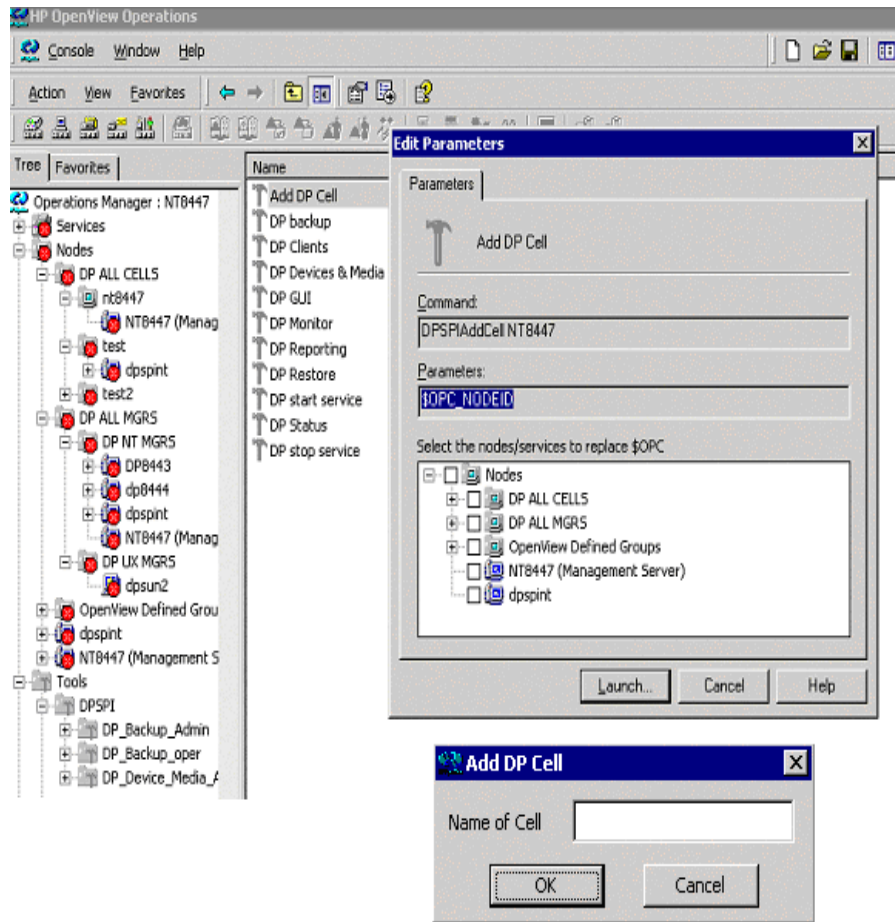
1. Open the Add/Remove Programs:
Start → Settings → Control Panel → Add/Remove Programs
2. Check `DP SPI-OVOW75-B.06.00` appears as an installed product.

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:



2. When prompted, enter the name of the node group that you are creating under DP ALL CELLS.

In the example in window above, 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. You can use a different name if you wish. The resulting node configuration is displayed in the OVO console.

Installing the Data Protector Integration

Installing the Data Protector Integration

When you use the `Add DP Cell` tool to add a managed node to the `DP NT MGRS` or `DP UX MGRS` node group, the appropriate policies group, `DP-SPI NT Policies` or `DP-SPI UX Policies`, and the required instrumentation is automatically deployed to the node.

For more information on installing agent software and adding managed nodes to the management server, see the online help for agent installation or the *OVO Installation Guide*.

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

View → **Policy inventory**

Agent Configuration

NOTE

In order to receive the File Library SNMP events from Data Protector 5.5, the following Data Protector patches need to be installed on the Data Protector Cell server:

- *Windows*: DPWIN_00167
- *HP-UX*: PHSS_33637
- *Solaris*: DPSOL_00173

The patches can be downloaded from:

<http://support.openview.hp.com/cpe/patches/dp/dp.jsp>

SNMP Configuration on UNIX

NOTE

SNMP events are not supported for Data Protector Cell Manager SUSE Linux Enterprise Server 9.

To enable the OVO Agent on UNIX nodes to receive SNMP traps from Data Protector:

1. Add one of the following lines to the `/opt/OV/bin/OpC/install/opcinfol` 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:

HP-UX:

`/etc/SnmpAgent.d/snmpd.conf`

`trap-dest: 127.0.0.1`

Solaris:

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

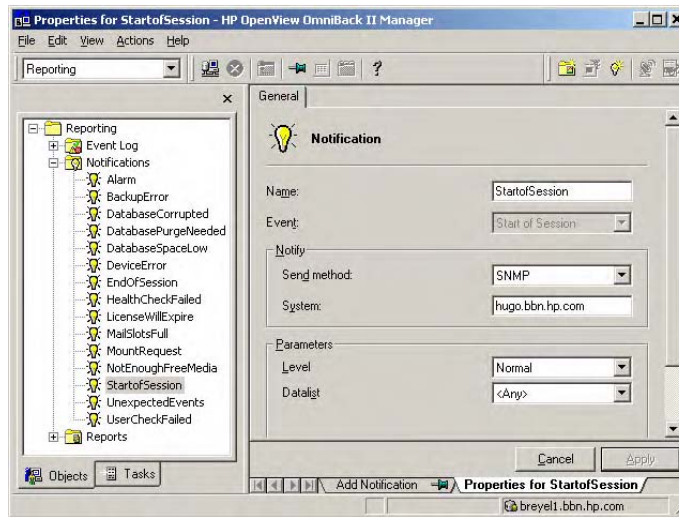
`trap localhost`

`trap-community public`

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

- Cell Manager host system as the destination

Figure 2-1 Data Protector GUI's Reporting context window



- b. Add the Cell Manager hostname as trap destination to the `OVdests` file in
`/etc/opt/omni/snmp` (Data Protector 5.1 and below)
`/etc/opt/omni/server/snmp` (Data Protector 5.5 and above).
- c. Disable filtering of SNMP traps by emptying the `OVfilter` file in
`/etc/opt/omni/snmp` (Data Protector 5.1 and below)
`/etc/opt/omni/server/snmp` (Data Protector 5.5 and above).

SNMP Configuration on Windows

Configure the Windows system to forward its SNMP traps to the OVO Management Server as follows:

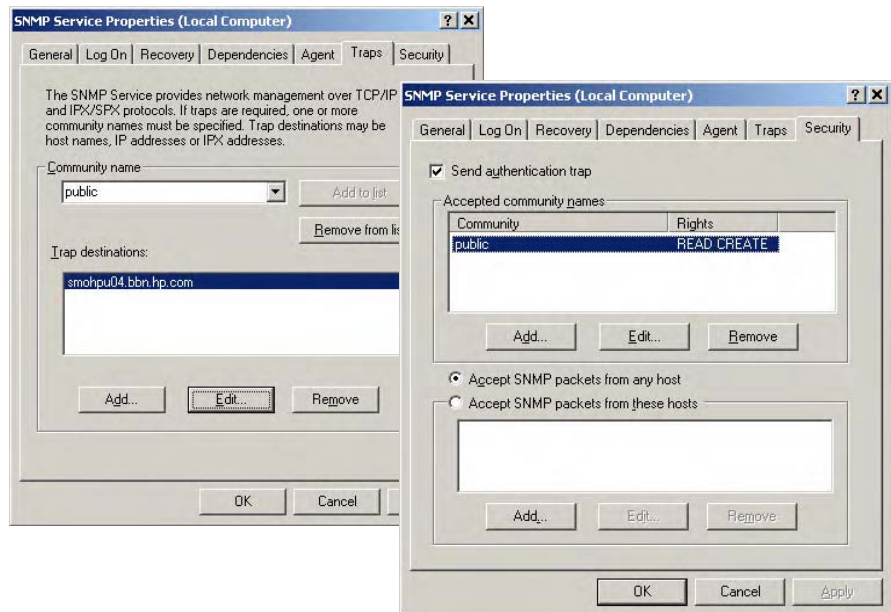
1. To enable Data Protector to send SNMP traps, run the command:
omnisnmp
2. Add the following line to the file
`<Installed Package>\{790C06B4-844E-11D2-972B-080009EF8C2A}\bin\OpC\install\opcinfo:`
SNMP_SESSION_MODE NO_TRAPD

3. Configure the SNMP Service on a Windows system to send traps to the OVO management server. The community name should be **public** (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**.

To use a custom community name other than `public`, set the value in the Registry. Data Protector can then use the name for sending SNMP traps:

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

Figure 2-2 Configuring the SNMP Service on Windows



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

- OVO management server system as the destination

Please see Figure 2-1 on page 30.

- b. Add the OVO management server hostname as trap destination to the `OVdests` file in `<DataProtector Root>/Config/SNMP`.
 - c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `<DataProtector 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 nodes: Check the local root user is in Data Protector's admin user group.

Windows: Add the local `HP_ITO_account` user and the local `SYSTEM` account to Data Protector's admin user group.

Program Identification

UNIX managed nodes: All Data Protector Integration programs and configuration files contain an identification string that can be displayed using the UNIX command `what(1):`.

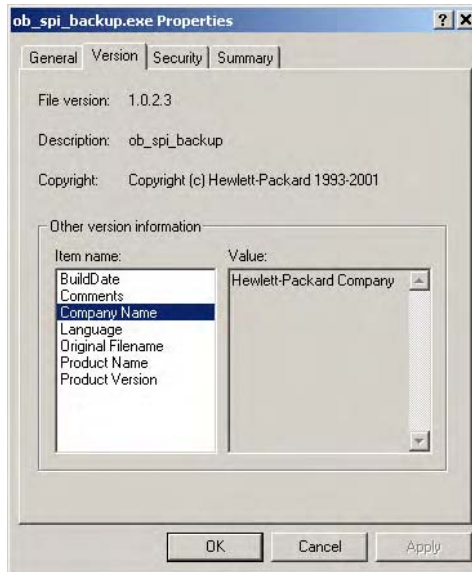
The output is of the form:

```
HP OpenView Storage Data Protector Integration into  
OVO A.06.00 (<build_date>)
```

Windows managed nodes: All Data Protector Integration programs and configuration files contain an identification string:

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:



Uninstalling the Data Protector Integration

To uninstall the Data Protector Integration:

- Perform some de-configuration tasks manually 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 \ SPI for DataProtector`, 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 2-3 Uninstall policies on... Window



3. Click **OK**.

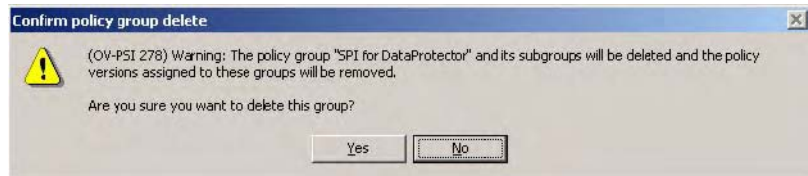
Remove Data Protector Policies from the OVO Management Server

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

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

Delete

This will raise the Confirm policy group delete window:



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

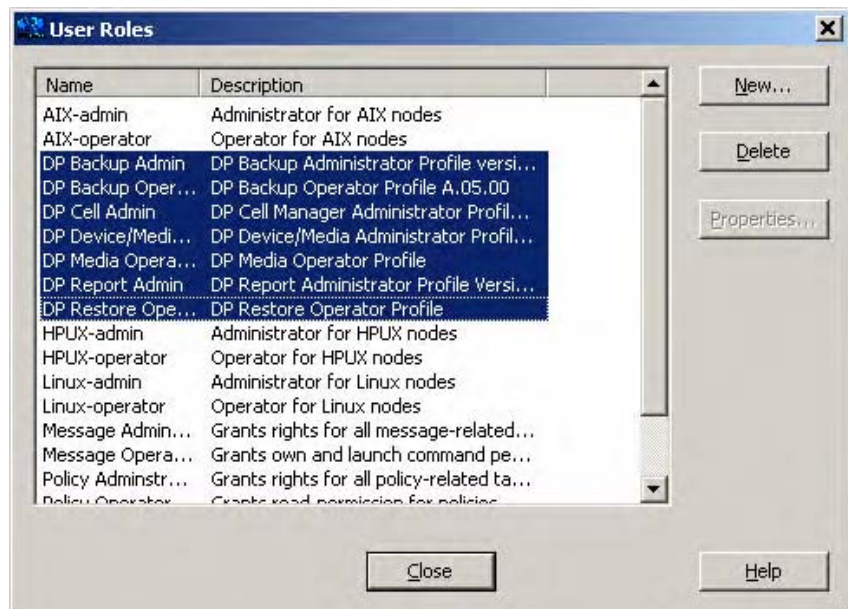
Remove Data Protector User Roles from the OVO Management Server

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.



Installing the Data Protector Integration

Uninstalling the Data Protector Integration

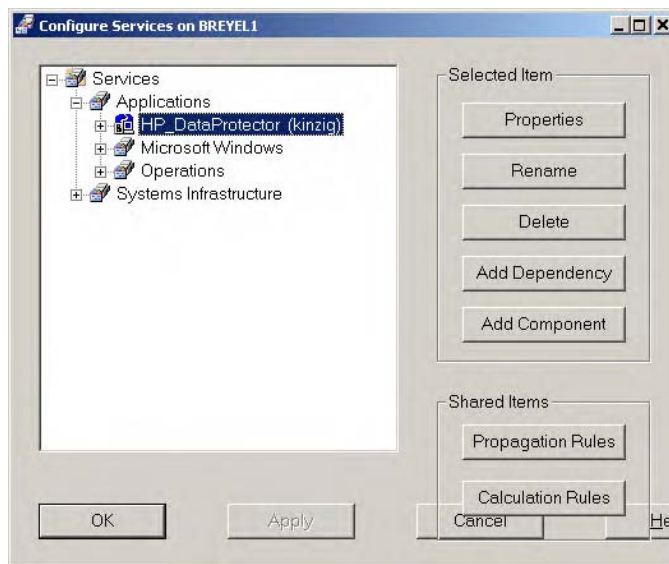
2. In the `User Roles` window, select all `DP*` user roles and click the **Delete** button and close this window.

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...**

The `Configure Services` window is displayed:



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

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

The Add/Remove Programs window is displayed:



2. In the Add/Remove Programs window, scroll down until you find the `DPSPI-OVOW75-B.06.00` entry.
3. Click **Remove** to start the removal. This will take a short time

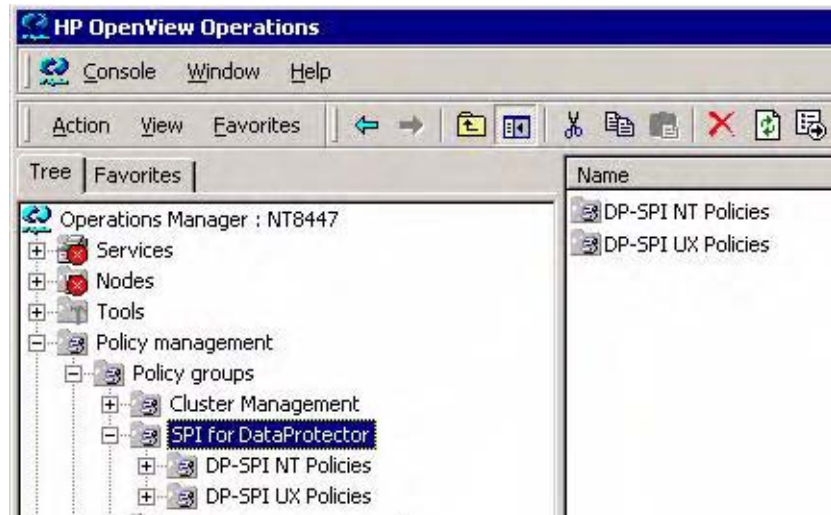
Installing the Data Protector Integration
Uninstalling the Data Protector Integration

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:

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

Data Protector SPI Policies

The Data Protector Integration adds the SPI for DataProtector policy group to OVO:



The SPI for DataProtector policy group contains:

- DP-SPI NT Policies
- DP-SPI UX Policies

Both are 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

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

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

Where appropriate, the integration assigns relevant messages to existing OVO message groups. Other messages are assigned to the following six Data Protector Integration-specific message groups:

<code>DP_Backup</code>	Backup session messages
<code>DP_Restore</code>	Restore session messages
<code>DP_Mount</code>	Mount request messages
<code>DP_Misc</code>	All other important Data Protector related messages
<code>DP_SPI</code>	Messages from the Data Protector Integration
<code>DP_Interactive</code>	Detailed messages normally only displayed in the Data Protector GUI. This message group is disabled as default. Enable the group for the greatest level of detail about Data Protector's operation.

Message Format

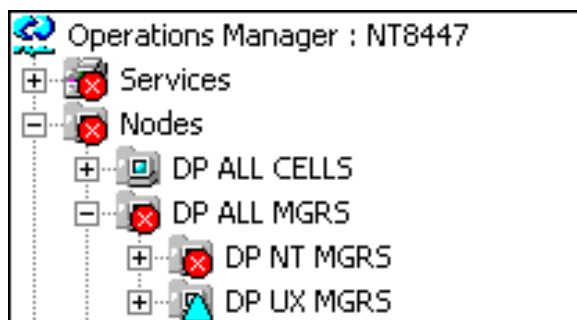
An OVO message includes the following parameters:

<i>Message Group</i>	The following groups are available, as described above: DP_Backup, DP_Restore, DP_Mount, DP_Misc, DP_SPI, DP_Interactive
<i>Applications</i>	Set to Data Protector.
<i>Node</i>	Set to the hostname of the Data Protector system on which the event occurred.
<i>Severity</i>	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.
<i>Service Name</i>	Depends on the impact the event has on a service. The value must map with a node in Data Protector's service tree.
<i>Object</i>	Allows the source of the event to be classified with fine granularity. Data Protector SNMP traps set the parameter to NOTIFICATION. Messages originating from a monitored logfile set this parameter to the name of the logfile. <ul style="list-style-type: none">• Messages originating from a monitor set it to the name of the monitor.

Node Groups

Node groups are logical groups of systems or devices assigned together with message groups to an operator to manage. Each node group is represented by an icon in the Node Group Bank window. Open a node group to view all systems within it. A system may belong to more than one node group.

The Data Protector Integration provides the four Node Groups, DP ALL CELLS, DP ALL MGRS, DP NT MGRS and DP UX MGRS:



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 determine which nodes a user receives messages from. Together with message groups, they define:

- the user's responsibilities
- which messages the user sees 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 you add a new Data Protector Cell Manager with the Add DP Cell application, a Node Layout Group is included into the DP ALL CELLS node group.

Two further node groups are created during installation of the Data Protector Integration:

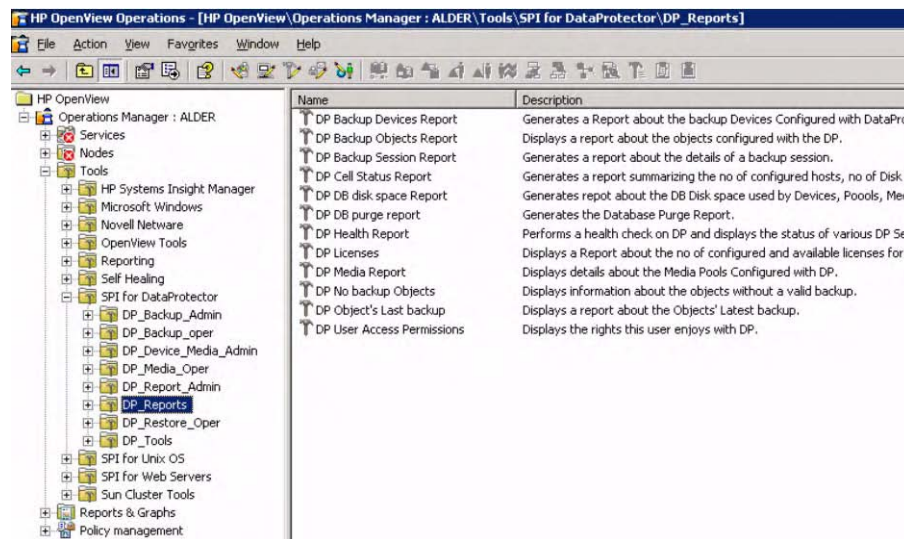
- DP NT MGRS
- DP UX MGRS

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.

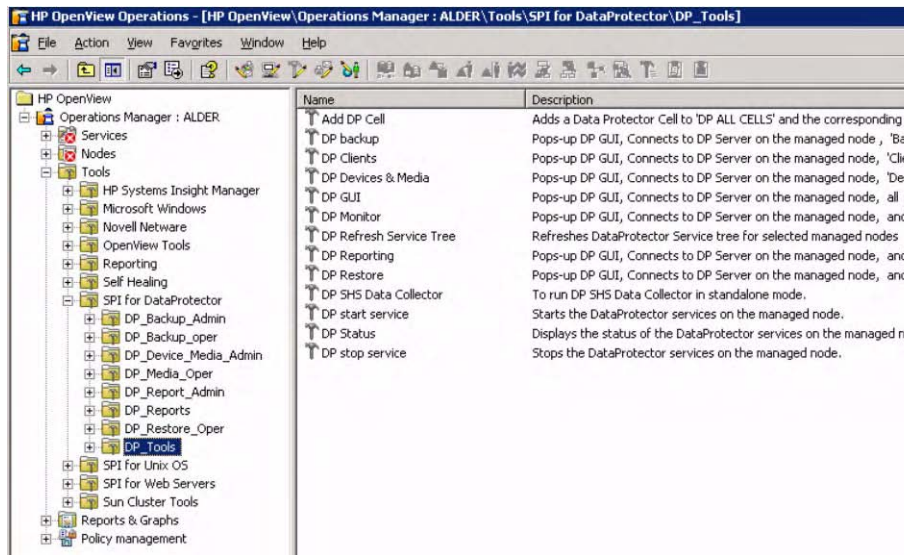
Tools Groups

Installation of the Data Protector Integration adds two new tools groups to the OVO `Tools` folder. Each different OVO user role has an appropriate set of Data Protector Integration applications.

- `DP_Reports`, containing tools for monitoring the health and performance of the Data Protector environment:



- DP SPI, containing applications used to manage the Data Protector environment:



Using Tools and Reports

Tools usually execute on the management server or 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 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 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 for a user name and password.

Examples:

DP GUI:

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:

Starts `omnicellinfo` remotely on the OVO Managed Node/DP Cell Manager.

Using the Data Protector Integration Tools Groups

DP Status:

Starts `omnisv -status` remotely on the selected Data Protector Cell Manager.

Using Self-Healing Services

Self-Healing Services can be used in two ways:

- Tools
- Self-Healing Services Client

Tools

Use the DP SHS Data Collector tool in the tool group `DP_Tools`. Run the tool by selecting the node on which SHS for DPSPI information needs to be collected.

Using DPSPI SHS Data Collector Self-Healing Services Client

To use DPSPI SHS Data Collector through the Self-Healing Services client, ensure the client is running. After deploying the policies on the managed node, register the Self-Healing Client for the node with the help of the tool present under **Tools** → **Self Healing** → **Self-Healing Register**

After completing the Self-Healing Client registration, you need to run the following scripts on their appropriate managed nodes:

On Windows Managed Node:

```
<DRIVE>\Program Files\Hewlett-Packard\  
SH Services\bin\recon.bat
```

On UNIX Managed Node:

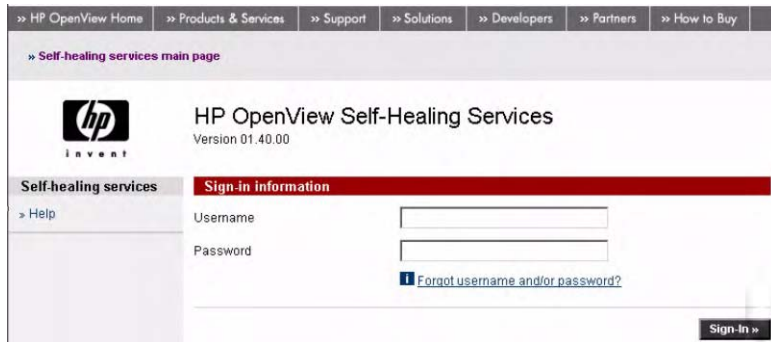
```
/opt/hpsupport/bin/recon.sh
```

To use DPSPI SHS Collector, follow these steps:

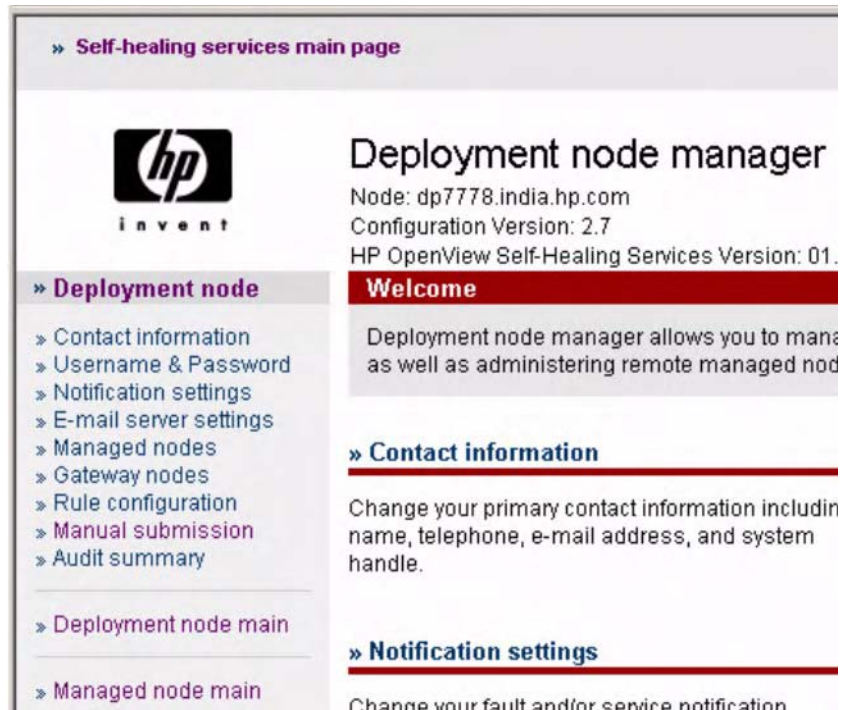
1. On a web browser, open the link:

```
https://<Managed Node name>:5814/
```

The following page opens:



2. Log in. The default username is `admin` with password `admin`.
The Deployment Node Manager is displayed:



Use the **Managed nodes** and **Gateway nodes** links in the left column to add managed and gateway nodes.

3. Click **Manual submission** in the left column to display the following page:

Manual submission

Click the link for the managed node for which you want to submit an incident to be routed to that node's manual submission page.

Host name	Port
dp7778.india.hp.com	5814
hpomt5.india.hp.com	5814

4. Select the managed node on which you want to collect DPSPi information. The information page is displayed:

Manual submission

Manual submission information

Node : dp7778.india.hp.com

* = required field

Product/Application

Problem title (maximum of 80 characters)*

Problem description (maximum of 4000 bytes)*

In the Product/Application field, select Smart Plug-In for Data Protector.

Type appropriate details in the other two fields and click **Submit**.

Using the Data Protector Integration
Using Self-Healing Services

5. After submitting, select the **Managed node main** in the left column. Select **Incident Viewer** in the page that opens to display the **Incident search criteria**:

Incident search criteria

Status	Source
<input type="text" value="Received"/> <input type="text" value="Failed"/> <input type="text" value="Hold"/> <input type="text" value="Ignored"/> <input type="text" value="Submitted"/> <input type="text" value="Suppressed"/>	<input type="text" value="SPI_datapro operations for Windows"/>

Incident search results

Check the incidents and then click 'Delete Checked Incidents' button to delete incidents. Click the Incident name link to edit/view the gateway node properties.

Delete	Incident name	Status	Date/Time	Source
<input type="checkbox"/>	Hello	Hold	Nov 25, 2005 / 6:00:24 AM (GMT)	SPI_datapro
<input type="checkbox"/>	Test	Submitted	Sep 13, 2005 / 8:15:27 AM (GMT)	SPI_datapro
<input type="checkbox"/>	TestTest	Submitted	Sep 21, 2005 / 5:37:36 AM (GMT)	SPI_datapro

6. In the Source field, select SPI_datapro and click **Search**. The search results on the page will list the status of all incidents submitted for DPSPI.

7. Select an incident. In the page that opens, select **View collected data submission** settings to display the following:

The screenshot displays a web interface with several sections of information:

- Instructions:** A grey box containing the text: "The information on these pages is read-only because the incident has already been submitted; making further changes would have no effect. Click the link for each item to see details."
- System configuration information:** A red header followed by links for:
 - [Basic system information](#)
 - [Memory and swap information](#)
 - [File system information](#)
 - [Environment variables](#)
- System resource information:** A red header followed by a link for:
 - [DNS information](#)
- Application information:** A red header followed by a list of links:
 - [Self-Healing Services](#)
 - [service desk](#)
 - [performance agent](#)
 - [omniback II](#)
 - [network node manager](#)
 - [operations for Windows](#)
 - [event correlation services](#)
 - [reporter](#)
 - [service information portal](#)
 - [instant support enterprise edition](#)
 - [emanate SNMP agent](#)
 - [data protector](#)
 - [Smart Plug-In for Data Protector](#)

8. Select **Smart Plug-In for Data Protector**. A page displays details of the collected information:

The screenshot displays a web interface with the following sections:

- Collected data filter:** A section with the subtext "Application information: Table of contents".
- Application report summary:** A red header followed by a table:

Source name	SPI_datapro
Application name	Smart Plug-In for Data Protector
- Application features:** A red header followed by links for:
 - [Components](#)
 - [Data files](#)
 - [System commands](#)

There are three application features:

Using Self-Healing Services

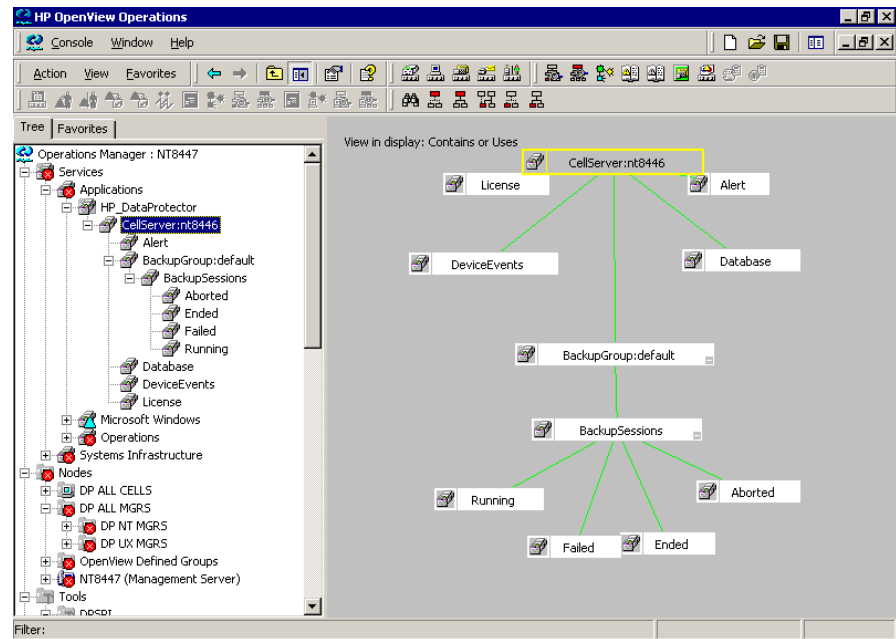
- `Components`: giving details of components being collected.
- `Data files`: giving details of files being collected.
- `System Commands`: giving details of commands executed as part of DPSPi SHS Data Collector.

Data Protector Service Tree

Data Protector is represented as a service tree with each cell an icon. The tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from Data Protector Integration's monitors. Figure 3-1 illustrates the HP_Data Protector service tree consisting of a sub-tree for the Cell Manager:nt8446 Data Protector Cell Manager.

Figure 3-1

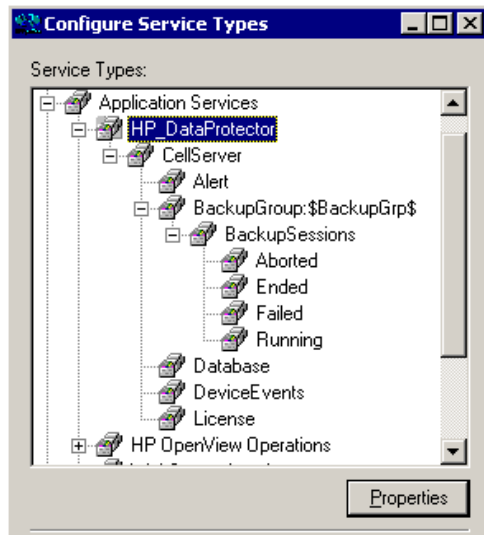
The Data Protector Service Tree



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.

Data Protector Service Tree

On installing the Data Protector Integration, the following service tree type definition is loaded:



The following service tree nodes are 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. 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 because: <ul style="list-style-type: none"> • the device is occupied • the database is in use • all licenses are currently allocated • too many backup sessions are running in parallel
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 describes the types of user in OVO, Data Protector and the Data Protector Integration. It also describes the users and roles installed by the Data Protector Integration and suggests 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**, required to log in to the operating system. A user requires a valid user login to start Data Protector or OVO.

Examples:

Windows user in the EUROPE domain: EUROPE\janesmith

UNIX user who's primary Unix group is marketing:

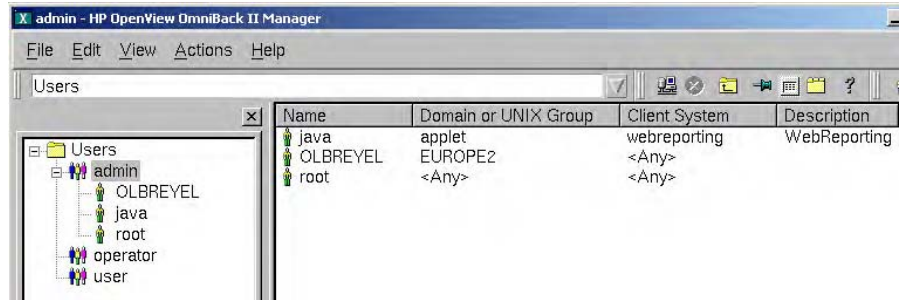
```
uid=4110(janesmith) gid=60(marketing)
```

- **Data Protector User Group**

A Data Protector user group defines access rights for its members. A member of a user group is identified by the group's operating system user. This user, used to log in to the system, has access rights and Data Protector GUI context determined by the user group.

When a user from the group starts the Data Protector GUI from **Tools**, the layout of the Data Protector GUI and permissions for the user are determined by the operating system user.

Figure 3-2 Windows Users



Data Protector Integration Users

The operating system user is required by the Data Protector Integration. The integration adds seven new user roles to the OVO User Roles configuration. For details, see “Data Protector OVO User Roles” on page 60. 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.

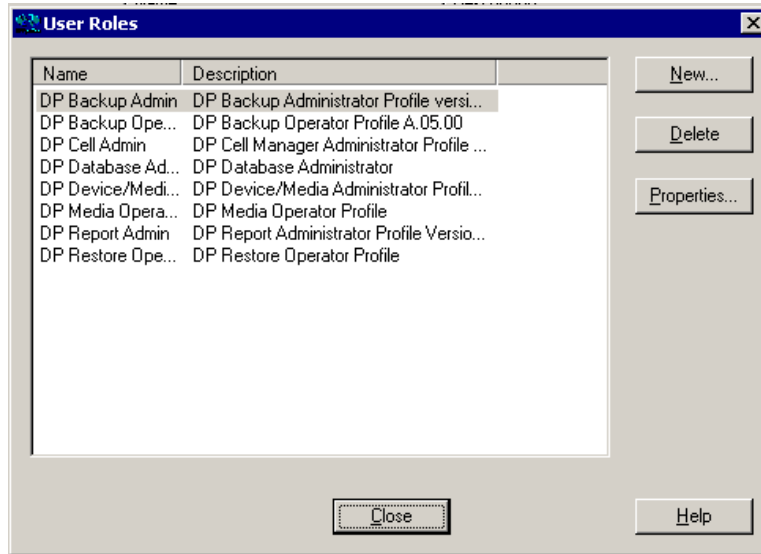
OVO User Roles

OVO uses **User Roles** to describe the configuration of abstract users. They are useful in large, dynamic environments with many OVO users and allow the rapid setting up of OVO users with default configuration. An OVO user may have multiple user profiles assigned and so can hold multiple roles.

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

Data Protector OVO User Roles

The OVO administrator uses user roles to assign responsibilities to OVO users. During installation, the Data Protector Integration software adds seven new user roles:



Each of these 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 roles can be used to implement the OVO user roles described in “Data Protector OVO Operators” on page 63.

<p>DP Backup Admin</p>	<p>Restricted to a Data Protector Cell.</p> <p><i>Tool Groups:</i></p> <ul style="list-style-type: none"> • DP_Backup_Admin • DP_Reports <p>Can access messages in the OVO Message Browser, if the OVO message policy for detailed messages DP_Detailed is enabled.</p>
------------------------	---

<p>DP Backup Operator</p>	<p>Restricted to a Data Protector Cell.</p> <p><i>Tool Groups:</i> DP_Backup_Oper</p> <p><i>Message Groups:</i></p> <ul style="list-style-type: none"> • DP_Backup • DP_Misc • DP_Mount <p>These are backup session messages and mount requests of backup sessions messages.</p>
<p>DP Restore Operator</p>	<p>Restricted to a Data Protector Cell.</p> <p><i>Tool Groups:</i> DP_Restore_Oper</p> <p><i>Message Groups:</i></p> <ul style="list-style-type: none"> • DP_Restore • DP_Misc • DP_Mount <p>These are restore session messages and mount requests of restore sessions messages.</p>
<p>DP Device & Media Administrator</p>	<p>Restricted to a Data Protector Cell.</p> <p><i>Tool Groups:</i> DP_Device_Media_Admin</p> <p>Can access messages in the OVO Message Browser, if the OVO message policy for detailed messages DP_Detailed is enabled.</p>
<p>DP Media Operator</p>	<p>Restricted to a Data Protector Cell.</p> <p><i>Tool Groups:</i> DP_Media_Oper</p> <p><i>Messages:</i> Mount requests of backup and restore sessions (DP_Mount) messages.</p>

Users and User Roles

DP Cell Administrator	Restricted to clients of Data Protector Cells. <i>Tool Groups:</i> <ul style="list-style-type: none">• DP_Reports• DP_Tools <i>Message Groups:</i> <ul style="list-style-type: none">• DP_Misc• DP_SPI
DP Report Administrator	Restricted to a Data Protector Cell. <i>Tool Groups:</i> DP_Reporting <i>Messages:</i> None.

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 3-2 defines roles for Data Protector OVO operators and describes their access rights .

NOTE

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

OVO users are not created by the Data Protector Integration. The roles described in Table 3-2 are examples of possible roles you may create and use to manage Data Protector.

Table 3-2 Data Protector OVO Operators and their Roles

Role	DP Privileges	Description
Backup Administrator		Create backup specifications (what to back up, from which system, to which device) and schedule the backup.
	Save backup specification	You can create, schedule, modify and save personal backup specifications.
	Switch session ownership	You can specify the owner of the backup specification under which backup is started. By default, this 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 3-2 Data Protector OVO Operators and their Roles (Continued)

Role	DP Privileges	Description
Backup Operator		Start a backup (if not scheduled), monitor the status of backup sessions, and respond to mount requests by providing media to devices.
	Start backup specification	You can back up using a backup specification, so you can back up objects listed in any backup specification and also modify existing specifications.
	Backup as root	You can back up any object with the rights of the root login. UNIX specific user right, required to run any backup on NetWare clients.
	Switch session ownership	You can specify the owner of the backup specification under which the backup is started. By default, this 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	You can back up your own data, monitor and abort your own session.
	Mount request	You can respond to mount requests for any active session in the cell.
	Monitor	You can view information about any active session in the cell, and access the Data Protector database to view past sessions. You can use the Data Protector database context.

Table 3-2 Data Protector OVO Operators and their Roles (Continued)

Role	DP Privileges	Description
Restore Operator		Start restore on demand (from which device, what to restore, to which system), monitor the status of the restore session, and respond to mount requests by providing media to devices.
	Restore to other clients	You can restore an object to a system other than that from which the object was backed up.
	Restore from other users	You can restore objects belonging to another user. UNIX specific user right.
	Restore as root	You can restore objects with the rights of the root UNIX user. <i>Note:</i> This is a powerful right that can affect the security of your system. Required to restore on NetWare clients.
	Start restore	You can restore your own data, monitor and abort your own restore sessions. You can view your own and public objects on the Cell Manager.
	Mount request	You can respond to mount requests for any active session in the cell.
	Monitor	You can view information about any active session in the cell, and access the Data Protector database to view past sessions. You can use the Data Protector database context.
Device & Media Administrator		Create and configure logical devices and assign media pools to devices, create and modify media pools and assign media to media pools.
	Device configuration	You can create, configure, delete, modify and rename devices. This includes the ability to add a mount request script to a logical device.
	Media configuration	You can manage media pools and media in the pools, and work with media in libraries, including ejecting and entering media.
Media Operator		Respond to mount requests by providing media to the devices.
	Mount request	You can respond to mount requests for any active session in the cell.

Table 3-2 Data Protector OVO Operators and their Roles (Continued)

Role	DP Privileges	Description
Cell Administrator		Installs and update Data Protector client systems, add, delete, or modify Data Protector users and groups, and administer the Data Protector database.
	Client configuration	You can install and update client systems.
	User configuration	You can add, delete and modify users or user groups. <i>Note:</i> This is a powerful right.
	Monitor	You can view information about any active session in the cell, and access the Data Protector database to view past sessions. You can use the Data Protector database context.
	See private object	You can see private objects. Database administrators require this right.
Report Administrator	Create and modify Data Protector reports.	
	Reporting and notifications	You can 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 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

Processes running 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 minutes

Message structure:

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

Databases

Checks amount and percentage of used available space.

Threshold: $\geq 95\%$ for error, $\geq 80\%$ for warning

Command:

```
omnidbutil -extend info
omnidbcheck -core -summary
omnidbcheck -filenames -summary
omnidbcheck -bf -summary
omnidbcheck -sibf -summary
omnidbcheck -smbf -summary
omnidbcheck -dc -summary
```

Polling interval: 60 minutes

Message structure:

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

NOTE

The usage of this monitor program is as follows:

Windows: `ob_spi_db.exe DP_CheckDB_NT <days>`

UNIX: `ob_spi_db.sh DP_CheckDB_UX obspi.conf <days>`

Use the parameter `<days>` to define how often the monitor performs an IDB status check (default value 1 = once a day, 0 means no check will be performed).

Media Pool Status

Checks if there are media pools with media status:

- Poor (Critical)
- Fair (Warning)

Polling interval: 60 minutes

Message structure:

Message Group	DP_Misc
Applications	Data Protector
Note	<name_cell_manager>.
Severity	Critical or Warning
Service Name	Services.Data Protector.<cell name>
Object	<i>Windows:</i> DP_CheckPoolStatus_NT <i>UNIX:</i> DP_CheckPoolStatus_UX
Operator Action in case of problem	Status of the Media Pool
Message Text when problem 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: omnimm -list_pool -detail

Polling interval: 60 minutes

Message structure:

Message Group	DP_Misc
Applications	Data Protector
Note	<name_cell_manager>.
Severity	Critical or Warning
Service Name	Services.Data Protector.<cell name>
Object	<i>Windows:</i> DP_CheckPoolSize_NT <i>UNIX:</i> DP_CheckPoolSize_UX
Operator Action in case of problem	Status of the Media Pool
Message Text when problem 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 hours (Critical)
- 8 hours (Warning)

Polling interval: 60 minutes

Message structure:

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

Check Important Configuration Files

Windows nodes: OB_CheckFile_NT starts `ob_spi_file.exe`

UNIX nodes: OB_CheckFile_UX starts `ob_spi_file.sh`

Windows Systems

Checks if the following files exist in subdirectories of the Data Protector configuration directory (default: `C:\Program`

`Files\OmniBack\Config\`):

For Data Protector 5.1 and earlier:

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

For Data Protector 5.5 and later:

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

Polling interval: 15 minutes

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

```
HKLM\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\  
Common HomeDir <REG_SZ>: "C:\Program Files\OmniBack"
```

UNIX Systems

Checks if the following files exist:

For Data Protector 5.1 and earlier:

- /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

For Data Protector 5.5 and later:

- /etc/opt/omni/server/cell/cell_info
- /etc/opt/omni/server/cell/installation_servers
- /etc/opt/omni/server/users/UserList
- /etc/opt/omni/server/users/ClassSpec
- /etc/opt/omni/server/users/WebAccess
- /etc/opt/omni/server/snmp/OVdests
- /etc/opt/omni/server/snmp/OVfilter
- /etc/opt/omni/server/options/global
- /etc/opt/omni/server/options/trace
- /etc/opt/omni/client/cell_server

Polling interval: 15 minutes

Changing Monitor Parameters

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

The location of the file is:

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

UNIX: /var/opt/OV/bin/instrumentation

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

Windows: [OB_CheckFile_NT]
 \Config\client\cell_info
 \Config\client\installation_servers
 \Config\server\users\userlist
 \Config\server\users\classspec
 \Config\server\users\webaccess
 \Config\server\SNMP\OVdests
 \Config\server\SNMP\OVfilter
 \Config\server\Options\global
 \Config\server\Options\trace
 \Config\client\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/server/cell/cell_info
/etc/opt/omni/server/cell/installation_servers
/etc/opt/omni/server/users/UserList
/etc/opt/omni/server/users/ClassSpec
/etc/opt/omni/server/users/WebAccess
/etc/opt/omni/server/snmp/OVdests
/etc/opt/omni/server/snmp/OVfilter
/etc/opt/omni/server/options/global
/etc/opt/omni/server/options/trace
/etc/opt/omni/client/cell/cell_server

[DP_CheckProc_UX]
rds
crs
mmd

Monitored Objects

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

Use the OVO Policy Editor on the OVO Management Server to adjust 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, see 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

Generated when `omnisv -start` or `omnisv -stop` is executed. The date/time format is fixed and not language dependant. The format is:

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

Parameters for messages for the default logfiles are:

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

Examples:

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

Using the Data Protector Integration

Monitored Logfiles

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

inet.log

Provides security information. Messages document requests to the `inet` process from non-authorized systems. The data/time format depends on the value of the language environment variable.

Examples:

```
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

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.

Examples:

```
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.
```

Parameters for messages in the default logfiles are:

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

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, such as SNMP traps.

<code>debug.log</code>	Exception messages that have not been handled.
<code>RDS.log</code>	Raima Database service messages.
<code>readascii.log</code>	Messages generated 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>	Detailed errors during backup or restore sessions, such as errors while parsing the backup specification. No message catalog is used. The time/date format depends on the language environment variable.

4 Performance Measurement with the HP OpenView Performance Agent

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

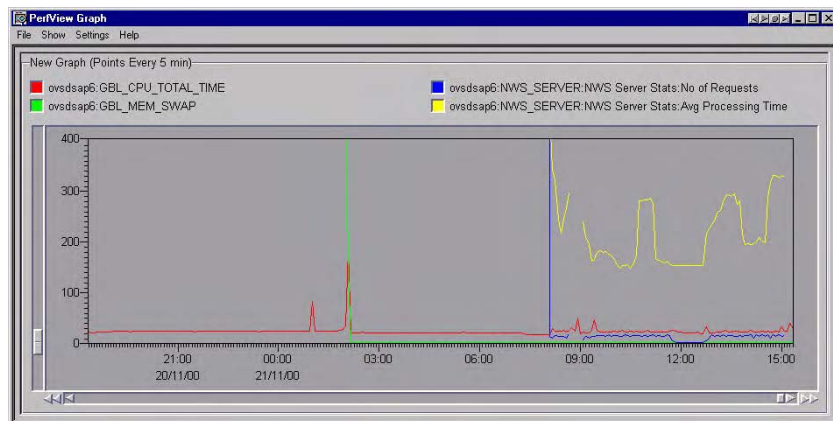
With integration into HP OpenView Performance (OVP), the HP OpenView Storage Data Protector Integration gathers performance data from Data Protector and transfers it into the Performance Agent (OVPA) for processing. This processed data can then be displayed graphically on the OVP console.

NOTE

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, such as I/O, network, and processes, and stores them in logfiles. Data Protector uses the ARM interface to measure the duration of transactions. These durations are also collected by the OVPA. It is possible to direct additional sources of performance data for the Data Protector environment into the OVPA via DSI (Data Source Integration). You can view the collected data centrally on the OVP Console to show trends. It can also be combined with internal data or data from other applications to get correlations, for example, with CPU utilization or network data.

Figure 4-1 HP OpenView Performance Console



Performance Measurement with the HP OpenView Performance Agent **Integration Overview**

You can use the performance measurement to help decide what you need to do to optimize the performance and resource usage of the Data Protector environment. You would typically perform this off-line, selecting a window of time for detailed analysis.

Installing Performance Integration Components

Installing on Windows 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 `obspi_vpp.zip`, holding all configuration files for Windows. You must distribute these OVPA configuration files manually as follows:

1. Use FTP to transfer the zip file to the managed node.
2. Install the files in the OVPA directory. Ensure that the files are copied to the appropriate OVPA directories:
 - a. Open `obspi_vpp.zip` with WinZip.
 - b. Select the parent directory of the OVPA Installation as the extraction directory, usually `C:\`.
 - c. Ensure that the `Use folder names` option is selected.
 - d. Click **Extract** to unzip the files to the chosen directories.

After unzipping, the following files are installed:

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

Installing on 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 directories 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 contain the tar file `obspi_vpp.tar` that holds all associated configuration files for HP-UX or Solaris. You must to distribute these manually, as follows:

1. Use FTP to transfer the tar file to the managed node.
2. Copy the file to the root directory
3. 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 durations of Data Protector transactions. 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:

Windows: `rpmtools\data\parm.mwc`
 `rpmtools\data\ttdconf.mwc`

UNIX: `/var/opt/perf/parm`
 `/var/opt/perf/ttd.conf`

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 that 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 the transaction parameter to:

```
transaction=correlator
```

Modifying the ttd.conf File

The default, `ttd.conf` 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 `ttd.conf` as follows:

1. 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 `ttd.conf` 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 DataProtector]
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\obspi_ttdconf.mwc
```

UNIX:

```
/opt/OV/OpC/integration/obspi/vpp/obspi_ttd.conf
```

An overview of the syntax is as follows:

Transaction Name	Additional Information	Transaction Description
BS-<Backup_spec>	Time	Duration of a backup session

Transaction Name	Additional Information	Transaction Description
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. *UNIX only:*

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

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

After modifying `ttd.conf`, you can collect transaction information about tasks executed by Data Protector listed in the table above.

Collecting Data Protector Process Data

Data Protector runs processes dedicated to 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 these 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 the following directories after the OVPA integration is installed:

Windows:

```
<Performance Agent Root>\Data\obspi_parm.mwc
```

Unix:

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

NOTE

You can 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 collect Cell Manager process data, add the following application groups to the `parm` file on the Cell Manager node:

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

NOTE

Comment the following entries on the `parm` file or move them to the end of the file. If this is not done, OVPA will log all the applications preceding this under the application history entry “`other_user_root`”:

```
Application = other_user_root
User = root
```

Modifying the parm File on a Data Protector Media Agent

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

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

Modifying the parm File on a Data Protector Disk Agent

To collect Disk Agent process data, add the following application groups to the `parm` file on the 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 collect Installation Server process data, add the following application groups to the `parm` file on the 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 it via the `dsilog` interface into the OVPA.

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:

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

Compiling the `obdsi.spec` File

To store the collected data in the OVPA database, you must create a logfile set. To do this, 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 <spec_file> <logfile_set>
```

<spec_file> The class specification file. If not in the current directory, it must be fully qualified.

<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. You can choose to store logfiles anywhere during compilation, but you *must not* move them once they have been compiled.

Examples:

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

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.

Installing the Data Protector DSI Log Service

After 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 the Data Protector DSI Log service listed, the installation was successful.

Starting the Data Protector DSI Log Service

To start collecting data, 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. Select the **Start** option in the context menu.

Specifying the Data Collection Frequency

The default data collection frequency is 12 minutes. This is configured in `obdsi.spec`, used to create the OVPA logfile set. To change the collection frequency, 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, do one of the following:

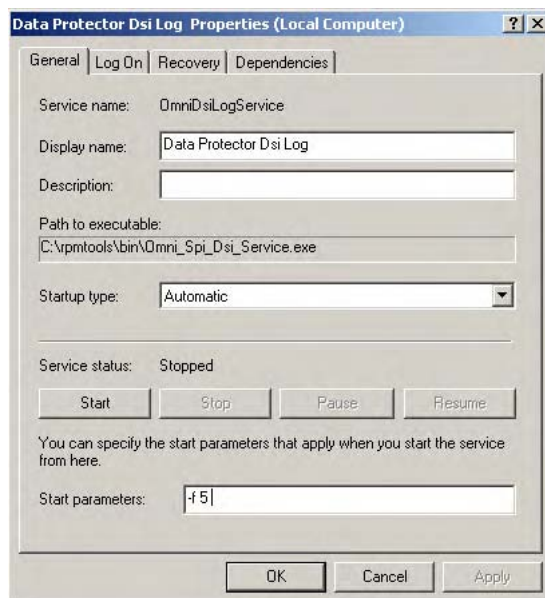
- Enter the command:

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

- From the Service Control Manager GUI, go to:

Start → Settings → Control Panel → Administrative Tools → Services

Double-click the `DataProtector Dsi Log` service, select the **General** tab and input the start parameter `-f <minutes>` in the textbox:



Configuring the Data Protector DSI Log Service

To enable tracing options for the `DataProtector Dsi Log` service, configure the service to provide the path of the trace file and the level of tracing information. Use the command:

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

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

If you omit the `-t` (tracing) option, no trace files will be written.

To specify what information should be written to the trace files, configure the trace level for the `DataProtector Dsi Log` service. There are four tracing levels:

- Level 1: Error Information
- Level 2: Function calls (for internal functions)

Performance Measurement with the HP OpenView Performance Agent Performance Agent Data Source Integration

- Level 3: Information about the current service activities
- Level 4: Important internal data to check for correct resources and configuration

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

```
Omni_Spi_Dsi_Service.exe -v <tracelevel>
```

where `<tracelevel>` must be between 1 and 4.

The `DataProtector Dsi Log` service uses another executable, the `OmniSpiDsiLogger.exe` to collect the data. After installation, this resides in the directory `<Performance Agent Root>\Bin`.

By default, the service uses this directory to find the executable. If you have relocated this file, you must specify the new path:

```
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. You can modify this data manually from the registry itself. The information is stored under the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
\OmniDsiLogService
```

To disable tracing, remove the registry value `TraceFilePath` from this registry key.

Uninstalling the Data Protector DSI Log Service

Before removing the files `Omni_Spi_Dsi_Service.exe` and `OmniSpiDsiLogger.exe`, uninstall the registered service:

```
Omni_Spi_Dsi_Service.exe -u
```


Collecting Data on UNIX Nodes

To collect 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:

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

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 ReporterLite Integration

This chapter covers integration with ReporterLite and creating Data Protector reports:

- “ReporterLite Overview”
- “ReporterLite Integration with Data Protector Architecture”
- “Installing the ReporterLite Integration”
- “Using the ReporterLite Integration with Data Protector”
- “Preconfigured Reports”

ReporterLite Overview

ReporterLite is a simplified version of OpenView Reporter (OVR). It can generate 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 ReporterLite.

ReporterLite 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

- Direct communication with Data Protector to obtain data
- Ability to view session trend reports and gain insight on the overall health of Data Protector cell servers over a selected time
- Ability to view trend reports on the data backup, backup duration and number of files backed up.
- Reporting Error Status and Session Health details over a selected 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 ReporterLite Integration with Data Protector provides the following reports:

- Backup Session Trend report (see page 110)
- Backup Duration Trend report (see page 111)
- Data Backup Trend report (see page 112)
- Number of Files Trend report (see page 113)
- Skipped Files report (see page 116)
- Backup Session Health overview (see page 114)

- Operational Error Status report (see page 115)
- Number of Successful Backups (see page 119)
- Capacity increase of Media Pool—Overview (see page 118)
- Backup Volume—Overview (see page 120)
- Number of Backup Up Files—Overview (see page 121)

ReporterLite Integration with Data Protector Architecture

This integration is completely installed on OVO for Windows. The module can communicate with the Data Protector Management System directly to obtain backup Session Details necessary to generate reports.

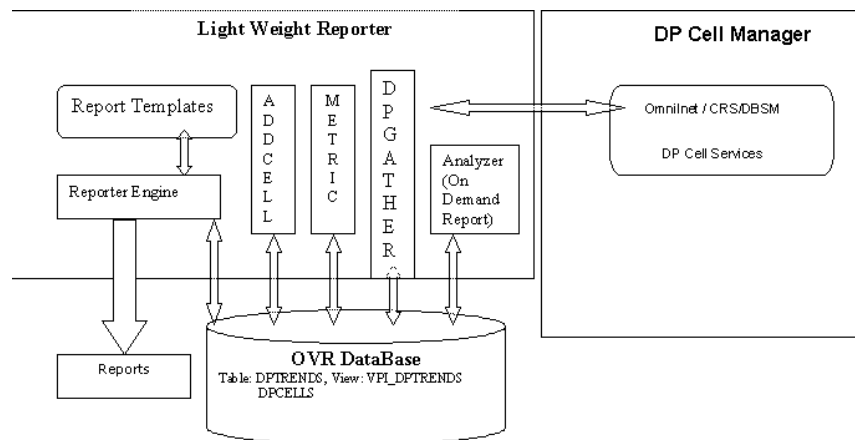
The module can access both Windows and UNIX Data Protector Cell Managers. It communicates with the following Data Protector processes to collect backup session details and stores the information in the OVO for Windows database:

- omniInet
- CRS
- DBSM

The following is a high-level representation of the integration:

Figure 5-1

ReporterLite Integration With Data Protector Architecture



1. The Add Cell utility is used to register a Data Protector management server with this module.
2. The Gatherer (DPGather), supplied as a part of this package, collects the required data from Data Protector and adds it to the database.

3. The Reporter Engine of ReporterLite generates reports using the database and the templates. The reports can be viewed using a browser

Installing the ReporterLite Integration

ReporterLite 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 and cannot be installed separately.

During installation, the following directories are created on the OVO for Windows system, where `<INSTALL_DIR>` is by default `C:\Program Files\HP Openview`:

<code><INSTALL_DIR>\bin</code>	Contains binaries
<code><INSTALL_DIR>\newconfig\Packages</code>	Contains XML and SRP files used to create database tables and views, and to add report definitions
<code><INSTALL_DIR>\data\reports\DP</code>	Contains report templates and <code>ReadMe.txt</code>

Verifying Installation

To verify the installation:

1. Open the `Add/Remove Programs` window:
Start → **Settings** → **Control Panel** → **Add/Remove Programs**
2. Check `DPSPi-OVOW75-B.06.00` appears as an installed product.

Uninstalling

Since this module is only installed as part of `DPSPi-OVOW75-B.06.00`, it cannot be uninstalled separately.

Using the ReporterLite Integration with Data Protector

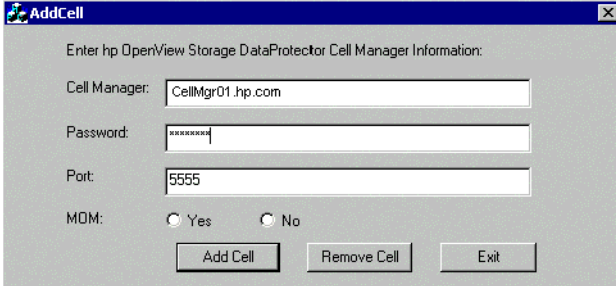
Registering a Data Protector Cell Manager with the Module

To use this module, you must register the Data Protector Cell Manager with this module. Use the executable utility `AddCell.exe` in `<INSTALL_DIR>\bin` to register the Data Protector Management System. You are asked to provide the following:

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

Figure 5-2

Add Cell Window



The screenshot shows a dialog box titled "AddCell" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Text: "Enter hp OpenView Storage DataProtector Cell Manager Information:"
- Text field: "Cell Manager:" with the value "CellMgr01.hp.com"
- Text field: "Password:" with masked characters "*****"
- Text field: "Port:" with the value "5555"
- Text: "MDM:" followed by two radio buttons: "Yes" (selected) and "No"
- Buttons: "Add Cell", "Remove Cell", and "Exit" at the bottom.

Use this to register as many Data Protector Cell Managers as required.

Troubleshooting

<i>Error message:</i>	Not able to load Reporter Database!!
<i>Description:</i>	The application cannot access the Reporter database.
<i>Action:</i>	Ensure that the reporter database is accessible.
<i>Error message:</i>	Not able to Resolve the host name!! This cell information is not updated.
<i>Description:</i>	The application cannot resolve the host name.
<i>Action:</i>	Ensure the host system exists and is accessible.
<i>Error message:</i>	Cell information is not added into database now...!! Error Code: 42502
<i>Description:</i>	The application cannot find the required database table.
<i>Action:</i>	Ensure the database table DPCELLS is present. If the tables do not exists, create/recreate them using the following commands: <code>newdb -xml <INSTALL_DIR>\newconfig\Packages\DPCELLS.xml</code> and <code>newdb -xml <INSTALL_DIR>\newconfig\Packages\DP TREND.xml</code> If
<i>Error message:</i>	Cell Manager already exists in the Reporter database!! Error Code: 23000
<i>Description:</i>	A Data Protector Cell Manager is already registered with ReporterLite, and you cannot use this application to update the information.

<i>Action:</i>	<p>To add the same Data Protector Cell Manager, with different information, remove the existing information from the database and then add the new information.</p> <p>To remove (de-register) a Cell Manager, use the <code>AddCell.exe</code> application, enter the relevant details and click Remove Cell.</p> <p>Once the Cell Manager is de-registered, data for reports can no longer be collected from it.</p>
----------------	---

Gathering Data from Data Protector

Once Data Protector Cell Managers are registered to ReporterLite, the utility `DPGather.exe` collects data from them. It is launched automatically when required.

Generating Reports

ReporterLite's utility `Repcrys.exe` generates reports. It is launched automatically when required.

Viewing Reports

Use the following link to view 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.

The logo consists of the text "hp OpenView" in white, centered on a dark blue rectangular background.

Reports in Family: Data Protector Service Level Reports



Reports for All Systems

Data Protector Trend Reports

[Amount of Data Written Trend](#)

[Backup Duration Trend](#)

[Backup Volume Usage Trend\(last 30 days\)](#)

[Media Pool Usage Trend\(last 30 days\)](#)

[Number of Files Backed up Trend\(last 30 days\)](#)

[Number of Files Trend](#)

[Sessions Trend](#)

[Successful Backup Trend\(last 30 days\)](#)

Data Protector Backup Session Reports

[Backup Session Health Overview \(Today\)](#)

[Backup Session Health Overview \(last 30 days\)](#)

[Backup Session Health Overview \(last 7 days\)](#)

[Operational Error Status \(Today\)](#)

[Operational Error Status \(last 30 days\)](#)

[Operational Error Status \(last 7 days\)](#)

[Files Skipped During Backups](#)

Click on the appropriate link to view the desired report.

Preconfigured Reports

Session Trend Report

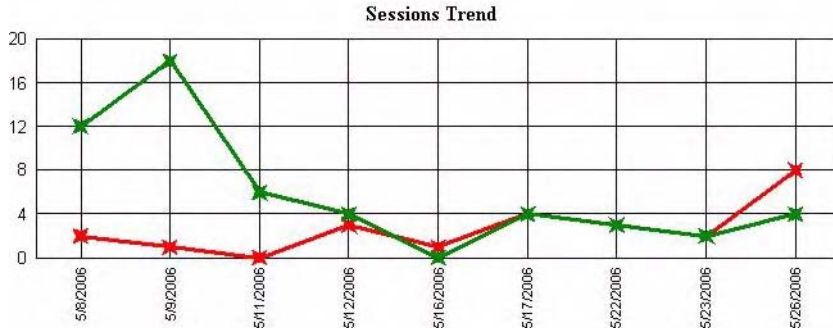
This graph shows the success and failure of backup sessions over time. The default period is 30 days. The date range is configurable by administrators. The graph shows trends for all sessions and for the individual cell manager.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Sessions Trend Report

This report was prepared on: 6/6/2006, 2:02:42 AM

This is a trend report on the general health of the backup sessions run by all Data Protector Cell Servers (cell managers) during the period 5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM. The graph shows the trend of successes to failures (failures include session aborts, session errors and session failures) for the backup sessions of Data Protector cell servers.



Graph in green indicates the successful backup session
Graph in red indicates the failed backup session

Backup Duration Trend Report

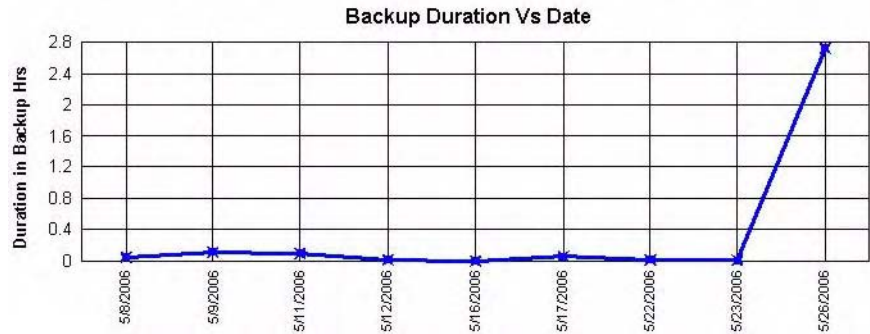
This graph shows the duration of backup sessions in hours over time. The default period is 30 days (configurable by administrators).

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Backup Duration Trend

This report was prepared on: 6/6/2006, 2:02:18 AM

This is a trend report for backup duration by all Data Protector Cell Servers (cell managers) during the period 5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM. Scroll down for individual cell server's trend graphs. Date represents session start date not the session completion date. Backup hours represents number of hours that were taken to complete the backup sessions which are started on that date.



Amount of Data Written Trend Report

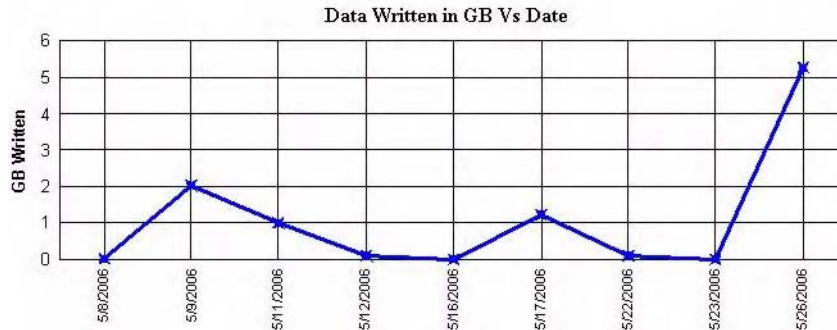
This graph shows how much data is written to backup media over time. The default period is 30 days (configurable by administrators). The graph shows trends for all sessions and for the individual cell manager.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Amount of Data Written Trend

This report was prepared on: 6/6/2006, 2:02:15 AM

This is a trend report of the backup data written to media by all Data Protector Cell Servers (cell managers) during the period **5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM**. Scroll down for individual cell server's trend graphs. Date represents session start date not the session completion date. GB Written represents amount of media space used in GB for the backup sessions which are started on that date.



The amount of data written is in gigabytes. To calculate 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 117.

Number of Files Backed Up Trend by All Backup Groups Report

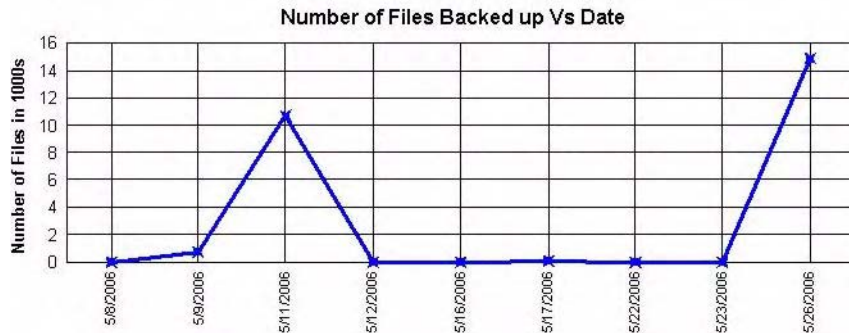
This graph shows the trend of the number of files (in 1000s) backed up by all Backup Groups over time. The default period is 30 days (configurable by administrators). The graph shows trends for all sessions and for the individual cell server.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Number of Files Backed up Trend by all Backup Groups

This report was prepared on: 6/6/2006, 2:02:39 AM

This is a trend report for number of files backed up by all Data Protector Cell Servers (cell managers) during the period 4/8/2006 12:00:00AM - 5/26/2006 12:00:00AM. Scroll down for individual cell server's trend graphs.



Backup Session Health Overview Report

This graph shows the ratio of successes to failures for backup sessions of each Data Protector Management system. Failures include session aborts, session errors and session failures.

One graph is produced for each of the sessions run during the past month, week and day.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Backup Session Health Overview

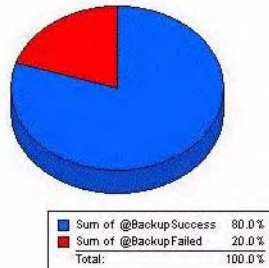
This report was prepared on: 6/7/2006, 11:34:35 AM

This is a high-level report on the general health of the backup sessions run by all Data Protector Cell Server (cell managers) during the period **5/26/2006 12:00:00AM - 5/26/2006 12:00:00AM**. The 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.

Application: HP OpenView Storage Data Protector

The "**Overall Health Status**" graph shows the combined health status of all the backup sessions across all the Data Protector Management systems.

Overall Backup Status



Operational Error Status Report

This graph shows the number of operational errors that occurred on Data Protector Cell Managers. Error status include Session Aborted, Session Error, Session Failed, Mount Errors, Mount Request (not enough free media).

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Operational Error Status

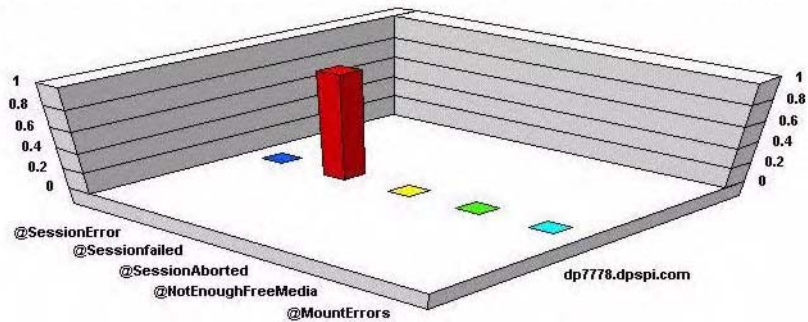
This report was prepared on: 6/7/2006, 2:01:11 AM

This report shows the number of operational errors that occurred on the Data Protector management systems (cell managers). Data is collected for the reporting interval of 5/26/2006 12:00:00AM - 5/26/2006 12:00:00AM. The "Operational Error Status for All Data Protector Management Systems" graph shows the sum of various errors on each Data Protector management system. For details of the errors relating to each Data Protector management system, see the graphs titled: for individual DP Manager Cells .

Application: HP OpenView Storage Data Protector

The "Operational Error Status for All Data Protector Management Systems" graph shows the combined operational error status for all the Data Protector management systems.

Operational Error Status for all Data Protector Management Systems



Skipped Files Report

This lists files not backed up during the backup session.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Skipped Files Report

This report was prepared on: Wed Jun 07 13:24:29 GMT+05:30 2006

Note: If the Data Protector Cell Server 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 Storage Data Protector

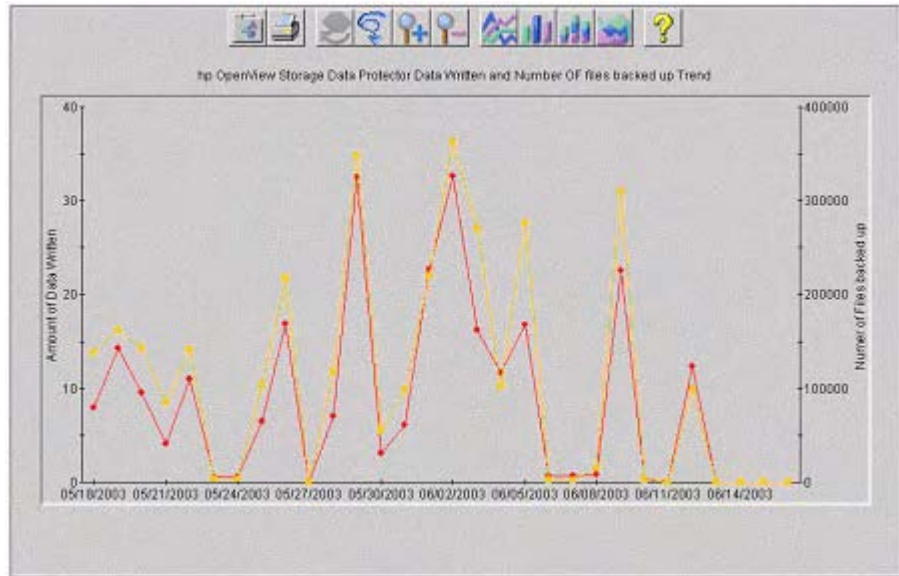
Cell Manager	Session ID	Client	Skipped File Name
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\Data\Databases\reporter_
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\Data\Databases\reporter_
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ma
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ma
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\mo
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\mo
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ms
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ms
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ten
dp7778.india.hp.com	2006/06/07-1	dp7778.dpspi.com	C:\Program Files\HP OpenView\MSSQL\$OVOPSD\data\ten

On Demand Report—Number of Files, Data Written and Date

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

- Sessions Trend
- GB Written Over Number of Files backed-up

The following is an example of a graph of GB Written Over Number of Files backed-up.



Media Pool Usage Trend

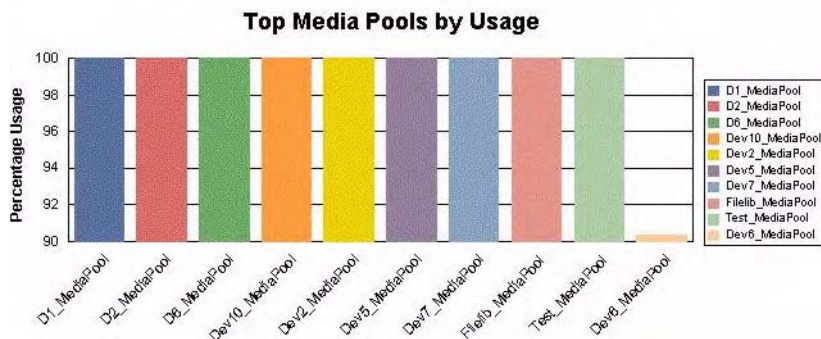
This graph shows the trend of media pool usage information for all Data Protector cell servers.

HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Media Pool Usage Trend

This report was prepared on: 6/6/2006, 2:02:24 AM

This report shows the Media Pool usage information for all Data Protector Cell Servers (cell managers) for the period 5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM. This graph shows the top ten Media Pools based on usage for all Cell Servers combined. Some Media Pools may depict a higher usage percentage but could be using a much lower space if data is not available for that Media pool for the entire reporting interval. Scroll down to the individual Cell Server graphs below for more information.



Successful Backup Trend

This shows the percentage of successful backups for each Backup Group by all Data Protector cell servers.

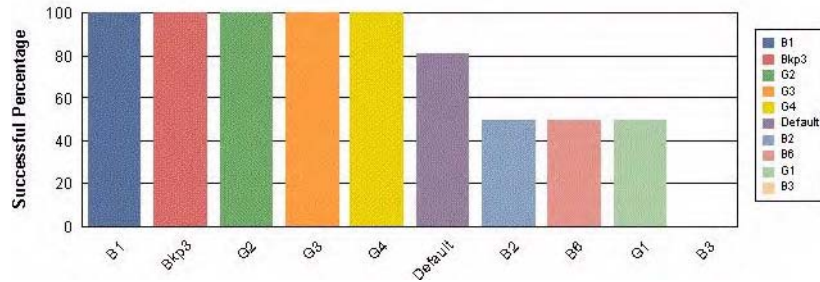
HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Successful Backup Trend

This report was prepared on: 6/6/2006, 2:02:45 AM

This report shows the Number of Successful backups percentage per Backup Group by all Data Protector Cell Servers (cell managers) for the period **5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM**. This graph shows the top ten Backup Groups based on the number of successful backups for all Cell Servers combined. Some Backup Groups may depict a higher number but could be having a much lesser success percentage if data is not available for that Backup Group for the entire reporting interval. Scroll down to the individual Cell Server graphs below for more information.

Successful Backup Percentage



Backup Volume Usage Trend

This graph shows the amount of data backed up for each Backup Group used by all Data Protector cell servers.

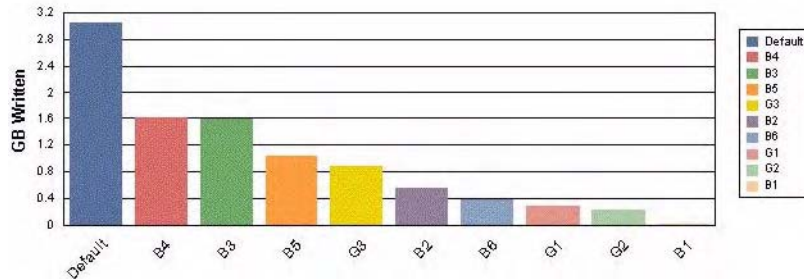
HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Backup Volume Usage Trend

This report was prepared on: 6/6/2006, 2:02:21 AM

This report shows the Backup Volume per Backup Group used by all Data Protector Cell Servers (cell managers) for the period 5/8/2006 12:00:00AM - 5/26/2006 12:00:00AM. This graph shows the top ten Backup Groups based on usage for all Cell Servers combined. Some Backup Groups may depict a higher usage percentage but could be using a much lower space if data is not available for that Backup Group for the entire reporting interval. Scroll down to the individual Cell Server graphs below for more information.

Backup Volume Usage



Number of Files Backed Up Trend

This shows the numbers of files backed up for each Backup Group by all Data Protector cell servers.

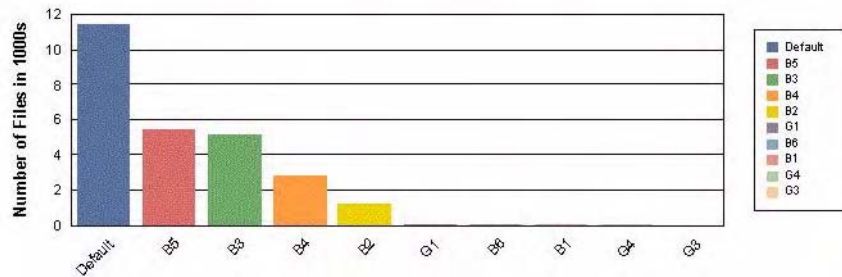
HP OpenView Storage Data Protector

hp OpenView storage Data Protector: Number of Files Backed Up Trend

This report was prepared on: 6/6/2006, 2:02:35 AM

This report shows the Number of Files Backed up per Backup Group used by all Data Protector Cell Servers (cell managers) for the period **4/8/2006 12:00:00AM - 5/26/2006 12:00:00AM**. This graph shows the top ten Backup Groups based on the number of files backed up for all Cell Servers combined. Some Backup Groups may depict a higher number but could be backing up a much lesser number of files if data is not available for that Backup Group for the entire reporting interval. Scroll down to the individual Cell Server graphs below for more information.

Number of Files Backed up Vs Date



Index

A

agent
 configuration, 28
 operations versions supported
 by OVO, 20
 performance versions
 supported by OVO, 20
alarms
 OVPA, 97
 performance agent, 97
Amount of Data Written Trend
 report, 112
application
 groups
 DPSPI_Applications, 47
 DPSPI_Reports, 46
 using, 46
architecture, 12
ARM transactions, 87

B

Backup Duration Trend report, 111
Backup Session Health
 Overview report, 114
Backup Usage Trend report, 120

C

cell manager
 permanently running
 processes, 67
 prerequisites, 19
configuration agent, 28
configuration files, monitoring, 73
configuring DSI log service, 95

D

Data Protector
 cell manager prerequisites, 19
 collecting process data, 90

 configuring the DSI log service, 95
 installing the DSI log service, 93
 OVO operators, 63
 OVO user profiles, 60
 performance agent data
 collection frequency, 94
 performance agent data source
 integration, 92
 platforms, 17
 service tree, 55
 starting the DSI log service, 94
 uninstalling the DSI log
 service, 96
 user configuration on OVO
 managed nodes, 32
 user group, 58
 versions, 17
Data Protector Integration, 11
 application groups, 46
 DPSPI_Applications, 47
 DPSPI_Reports, 46
 architecture, 12
 database logfiles, 79
 default logfiles, 77
 directories on OVO
 management server, 23, 24
 inet.log logfile, 78
 installing on OVO
 management server, 23
 message formats, 43
 message groups, 42
 monitored logfiles, 77
 monitored object, 67
 node groups, 44
 non-monitored logfiles, 80
 omnisv.log logfile, 77
 program identification, 32
 purge.log logfile, 79
 user profiles, 58
 users, 59

 data source integration, 92
 collection frequency, 94
 database monitor thresholds, 68
 deployment node manager, 50
 depot, installing on management
 server, 23
 disk space
 installing on OVO server, 22
 DP_Backup message group, 42
 DP_Interactive message group, 42
 DP_Misc message group, 42
 DP_Mount message group, 42
 DP_Restore message group, 42
 DP_SPI message group, 42
 DPSPI_Applications application
 group, 47
 DPSPI_Reports application
 group, 46
 DSI log service
 configuring, 95
 installing, 93
 starting, 94
 uninstalling, 96

F

formats, message, 43

G

groups
 application, 46
 message, 42
 node, 44

H

hardware prerequisites
 OVO management server, 19

I

installation disk space, 22
installing

- Data Protector Cell Manager prerequisites, 19
 - Data Protector Integration on OVO management server, 23
 - Data Protector versions, 17
 - depot, 23
 - DSI log service, 93
 - management server patches, 18
 - OVO managed node prerequisites, 19
 - OVO management server hardware prerequisites, 19
 - patches, 18
 - prerequisites, 18
 - software prerequisites, 18
 - OVPA integration components, 85
 - Performance integration components, 85
 - prerequisites, 17
 - RAM, 22
 - ReporterLite, 105
 - verification, 26
- L**
- logfiles
 - Data Protector database, 79
 - Data Protector default, 77
 - inet.log, 78
 - monitored, 77
 - not monitored, 80
 - omnisv.log, 77
 - purge.log, 79
 - long running backup sessions, 72
- M**
- managed nodes
 - Data Protector user configuration, 32
 - SNMP configuration on UNIX, 28
 - SNMP configuration on Windows, 30
 - management server
 - depot installation, 23
 - installation verification, 26
 - installing Data Protector Integration, 23
 - patches, 18
 - media pool size monitor thresholds, 71
 - media pool status monitor thresholds, 70
 - Media Pool Usage Trend report, 118
 - message formats, using, 43
 - message groups
 - DP_Backup, 42
 - DP_Interactive, 42
 - DP_Misc, 42
 - DP_Mount, 42
 - DP_Restore, 42
 - DP_SPI, 42
 - using, 42
 - monitored logfiles, 77
 - database logfiles, 79
 - default logfiles, 77
 - inet.log logfile, 78
 - omnisv.log logfile, 77
 - purge.log logfile, 79
 - monitored object, 67
 - configuration files, 73
 - databases, 68
 - long running backup sessions, 72
 - media pool size, 71
 - media pool status, 70
 - permanently running processes on cell manager, 67
 - monitoring configuration files, 73
- N**
- node groups, using, 44
 - non-monitored logfiles, 80
 - Number of Files Backed Up
 - Trend report, 113, 121
- O**
- obspi.spec file, 92
 - On Demand report, 117
 - OpenView Reporter, 101
 - operating system users, 58
 - Operation Error Status report, 115
 - operators, Data Protector OVO, 63
 - OVO
 - additional software for Windows nodes, 20, 21
 - Data Protector operators, 63
 - user profiles, 60
 - Data Protector Cell Manager installation prerequisites, 19
 - Data Protector Integration directories, 23, 24
 - managed nodes
 - Data Protector user configuration, 32
 - installation prerequisites, 19
 - SNMP configuration on UNIX, 28
 - SNMP configuration on Windows, 30
 - management server
 - depot installation, 23
 - hardware prerequisites, 19
 - installing prerequisites, 18
 - verification, 26
 - installing Data Protector Integration, 23
 - patches, 18
-

Index

- software prerequisites, 18
- versions, 18
- SNMP Emanate Agent for Windows nodes, 21
- SNMP service for Windows nodes, 22
- supported operations agent versions, 20
- supported performance agent versions, 20
- user profiles, 59
- OVPA**
 - alarms, 97
 - data collection frequency for Data Protector, 94
 - Data Protector process data, 90
 - data source integration for Data Protector, 92
 - installing integration components, 85
 - integration overview, 83
 - transaction times metrics, 87
- OVR**, 101
- P**
 - parm file, 87, 90, 91
 - patches
 - management server, 18
 - OVO management server, 18
 - Performance
 - agent alarms, 97
 - agent versions supported by OVO, 20
 - installing integration components, 85
 - integration overview, 83
 - transaction times metrics, 87
 - prerequisites, 17
 - Data Protector cell manager, 19
 - OVO managed node, 19
 - OVO management server, 18
- process data, 90
- profiles, user, 58
- program identification
 - Data Protector Integration, 32
- R**
 - RAM requirements, OVO server, 22
 - ReporterLite, 99
 - installation, 105
 - integration with Data Protector, 103
 - reports
 - Amount of Data Written Trend, 112
 - Backup Duration Trend, 111
 - Backup Session Health Overview, 114
 - Backup Usage Trend, 120
 - generating, 108
 - Media Pool Usage Trend, 118
 - Number of Files Backed Up Trend, 113, 121
 - On Demand, 117
 - Operation Error Status, 115
 - preconfigured, 110
 - Session Trend, 110
 - Skipped Files, 116
 - standard, 101
 - Successful Backup Trend, 119
 - viewing, 109
- S**
 - self-healing services, 13, 49
 - Service Navigator
 - Data Protector service tree, 55
 - service tree, Data Protector, 55
 - Session Trend report, 110
 - SHS, 13
 - SHS, *see* Self-Healing Services
 - Skipped Files report, 116
 - SNMP
 - configuration on UNIX OVO managed nodes, 28
 - configuration on Windows OVO managed nodes, 30
 - Emanate Agent Windows nodes, 21
 - software prerequisites, OVO management server, 18
 - starting DSI log service, 94
 - Successful Backup Trend report, 119
- T**
 - thresholds, monitored object, 67
 - transaction times metrics, 87
 - ttdconf file, 88
- U**
 - uninstalling DSI log service, 96
 - uninstalling ReporterLite, 105
 - user
 - Data Protector Integration, 59
 - groups, Data Protector, 58
 - operating system, 58
 - profiles
 - Data Protector OVO, 60
 - OVO, 59
 - using, 58
 - using
 - application groups, 46
 - applications
 - DPSPI_Applications, 47
 - DPSPI_Reports, 46
 - Data Protector
 - database logfiles, 79
 - default logfiles, 77
 - inet.log logfile, 78
 - omnisv.log logfile, 77
 - purge.log logfile, 79
 - message formats, 43
 - message groups, 42
 - monitored

- logfiles, 77
- object, 67
- node groups, 44
- non-monitored logfiles, 80
- user profiles, 58

V

- verifying management server
 - installation, 26

W

- Windows nodes
 - additional software, 20, 21
 - SNMP Emanate Agent, 21
 - SNMP service, 22