# HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations 7.1x & 7.2x for Windows

**Version: B.06.00**


**Manufacturing Part Number: B6960–96016**

**July 2006**

# Legal Notices

# Contents


**1. Introduction**

The Data Protector Integration . . . . . 11
Data Protector Integration Architecture. . . . . 12

**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 . . . . . 25
Running the Add Data Protector Cell Application . . . . . 25
Agent Configuration. . . . . 27
SNMP Configuration on UNIX. . . . . 27
SNMP Configuration on Windows . . . . . 29
Data Protector User Configuration . . . . . 31
Program Identification. . . . . 31
Uninstalling the Data Protector Integration . . . . . 33
De-configuration Tasks . . . . . 33
Undeploy All Data Protector Policies from Managed Nodes . . . . . 33

Remove Data Protector Policies from the OVO Management Server . . . . . 33
Remove Data Protector User Roles from the OVO Management Server . . . . . 34
Remove Data Protector Tools and Directory from the OVO Management Server . . . . . 34
Remove the Data Protector Service Tree from the OVO Management Server . . . . . 35
Remove Data Protector DP ALL CELLS and DP ALL MGRS Node Directories from the OVO Management Server . . . . . 36
Remove the Data Protector Integration. . . . . 37

**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
Data Protector Service Tree. . . . . 48
Users and User Roles . . . . . 51
Data Protector and Operating System Users . . . . . 51
Data Protector Integration Users . . . . . 52
OVO User Roles. . . . . 52
Data Protector OVO User Roles . . . . . 53
Data Protector OVO Operators . . . . . 56
Monitored Objects . . . . . 60
Permanently Running Processes on the Cell Manager . . . . . 60
Databases . . . . . 61
Media Pool Status . . . . . 63
Media Pool Size . . . . . 64
Monitor Status of Long Running Backup Sessions. . . . . 65
Check Important Configuration Files . . . . . 66

# Contents


Windows Systems . . . . . 66
UNIX Systems . . . . . 67
Changing Monitor Parameters . . . . . 67
Monitored Logfiles . . . . . 70
Data Protector Default Logfiles . . . . . 70
omnisv.log . . . . . 70
inet.log . . . . . 71
Data Protector Database Logfile . . . . . 72
purge.log . . . . . 72
Logfiles Not Monitored by Data Protector Integration . . . . . 73

**4. Performance Measurement with the HP OpenView Performance Agent**

Integration Overview . . . . . 77
Installing Performance Integration Components . . . . . 79
Installing on Windows Nodes . . . . . 79
Installing on UNIX Nodes . . . . . 80
Collecting ARM Transactions . . . . . 81
Modifying the parm File . . . . . 81
Modifying the ttd.conf File . . . . . 82
Collecting Data Protector Process Data . . . . . 84
Modifying the parm File on a Data Protector Cell Manager . . . . . 84
Modifying the parm File on a Data Protector Media Agent . . . . . 85
Modifying the parm File on a Data Protector Disk Agent . . . . . 85
Modifying the parm File on a Data Protector Installation Server . . . 85
Performance Agent Data Source Integration . . . . . 86
Compiling the obdsi.spec File . . . . . 86
Collecting Data on Windows Nodes . . . . . 87
Installing the Data Protector DSI Log Service . . . . . 87
Starting the Data Protector DSI Log Service . . . . . 88
Configuring the Data Protector DSI Log Service . . . . . 89
Uninstalling the Data Protector DSI Log Service . . . . . 90

# Contents

Collecting Data on UNIX Nodes. . . . . 91
Performance Alarms for the Performance Agent . . . . . 91

**5. ReporterLite Integration**

ReporterLite Overview. . . . . 95
Standard Reports . . . . . 95
ReporterLite Integration with Data Protector Architecture . . . . . 97
Installing the ReporterLite Integration . . . . . 99
Verifying Installation . . . . . 99
Uninstalling. . . . . 99
Using the ReporterLite Integration with Data Protector . . . . . 100
Registering a Data Protector Cell Manager with the Module . . . . . 100
Troubleshooting . . . . . 101
Gathering Data from Data Protector. . . . . 102
Generating Reports. . . . . 102
Viewing Reports . . . . . 103
Preconfigured Reports . . . . . 104
Session Trend Report . . . . . 104
Backup Duration Trend Report . . . . . 105
Amount of Data Written Trend Report . . . . . 106
Number of Files Backed Up Trend by All Backup Groups Report. . 107
Backup Session Health Overview Report . . . . . 108
Operational Error Status Report . . . . . 109
Skipped Files Report. . . . . 110
On Demand Report—Number of Files, Data Written and Date . . . 111
Media Pool Usage Trend. . . . . 112
Successful Backup Trend . . . . . 113
Backup Volume Usage Trend . . . . . 114
Number of Files Backed Up Trend. . . . . 115

# 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 |
| B6960–90017 | 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.

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.

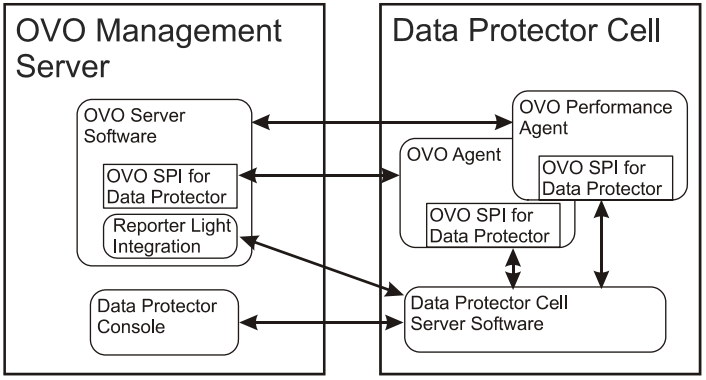
- Real-time event and configuration information (including online instructions) for fast problem resolution.
- Powerful monitors to detect potential problem areas and to keep track of system and Data Protector events.
- Performance data collectors to ensure continuous system throughput and notify any 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.

# 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 5.0, 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 11.0 | ✔ | ✔ | ✔ | ✔ |
| 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 XP Professional (32-bit) | ✔ | ✔ | ✔ | ✔ |
| Microsoft Windows 2000 | ✔ | ✔ | ✔ | ✔ |
| 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 7.1x | OVO 7.2x |
|---|---|---|
| *English and Japanese:* Microsoft Windows 2000, Windows 2003 | ✔ | ✔ |

### OVO Patches

Ensure you have installed up-to-date patches.

### 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

## 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 |
|---|---|
| 7.1*x*<br>7.2*x* | HP-UX 11.00, 11.11, 11.23 |
| | Solaris 7, 8, 9, 10 |
| | Microsoft Windows 2000, Windows XP Pro (32-bit), Microsoft Windows 2003 |
| | SUSE Linux Enterprise Server 9 (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, 10 | C.03.75, C.03.82 |
| Microsoft Windows 2000, XP, 2003 | C.03.65 |
| SUSE Linux Enterprise Server 9.x | 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-MIB2B.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 7.1x<br>OVO 7.2x | Windows 2000, 2003 | 15 MB |
| OVO Managed Node | OVO 7.1x<br>OVO 7.2x | HP-UX 11.0, 11.11, 11.23 | 2 MB |
| | | Solaris 7, 8, 9, 10 | 2 MB |
| | | SUSE Linux Enterprise Server 9.x | 2 MB |
| | | Supported Microsoft Windows Nodes | 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 `DPSPI_OVOW712-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 `DPSPI_OVOW712-B.06.00.msi` executable file.

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

| c:\Program Files\HP OpenView | |
|---|---|
| <INSTALLDIR>\install\DPSPI\ | Installation directory with subdirectories for policies and OVO configuration files |
| <INSTALLDIR>\install\DPSPI\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 *Integration Guide* and the *Product Announcements, Software Notes, and References* |

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`

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-080009EfbC2A}`

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

- `obspi.conf`
- `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.vbbs`
- `ob_spi_medialog.bat`
- `ob_spi_omnisvlog.vbs`
- `ob_spi_omnisvlog.bat`
- `ob_spi_purgelog.vbs`

- `ob_spi_purgelog.bat`

## Installation Verification

To verify the installation:

1. Open the `Add/Remove Programs`:

   **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**

2. Check `DPSPI-OVOW712-B.06.00` appears as an installed product.

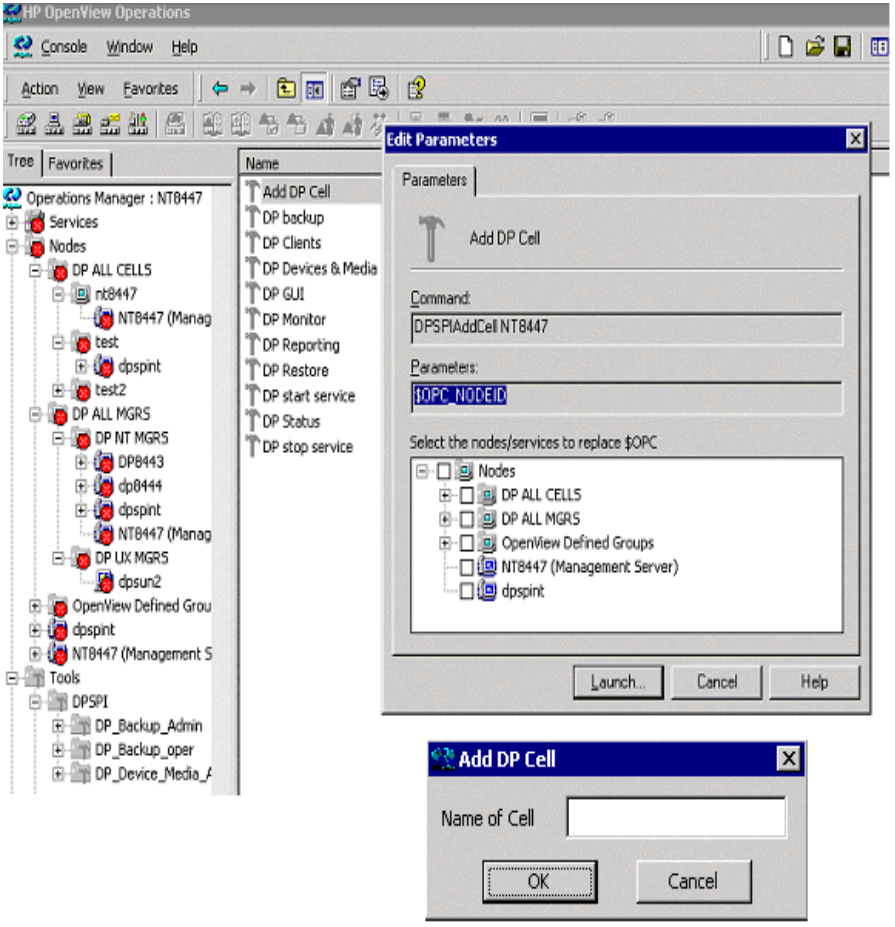
## Running the Add Data Protector Cell Application

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.

**Installing the Data Protector Integration**

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.

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 are 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

### SNMP Configuration on UNIX

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

**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

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/opcinfo` file.
   - If an `ovtrapd` process is running add:
     **`SNMP_SESSION_MODE  TRY_BOTH`**

- If no `ovtrapd` process is running add:
  **`SNMP_SESSION_MODE  NO_TRAPD`**

2. Configure the SNMP Emanate Agent to send SNMP traps to the local OVO agent by adding the following lines to the `snmpd.conf` file:

   HP-UX:

   *HP-UX:*
   `/etc/SnmpAgent.d/snmpd.conf`
   **`trap-dest: 127.0.0.1`**

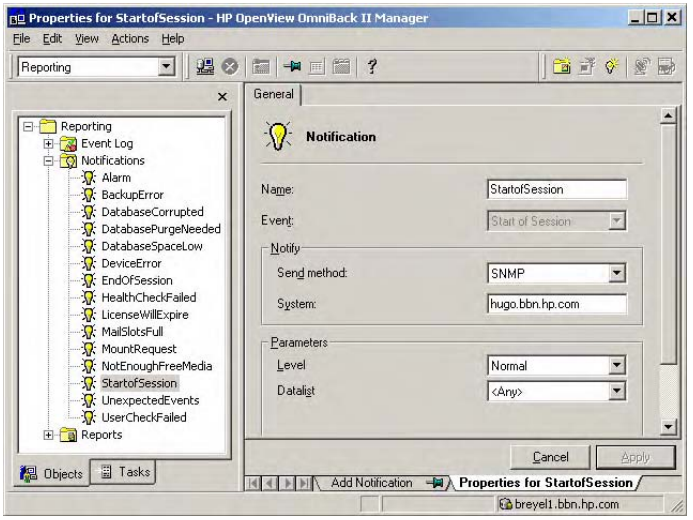
   *Solaris:*
   `/etc/snmp/conf/snmpd.conf`
   **`trap localhost`**
   **`trap-community public`**

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

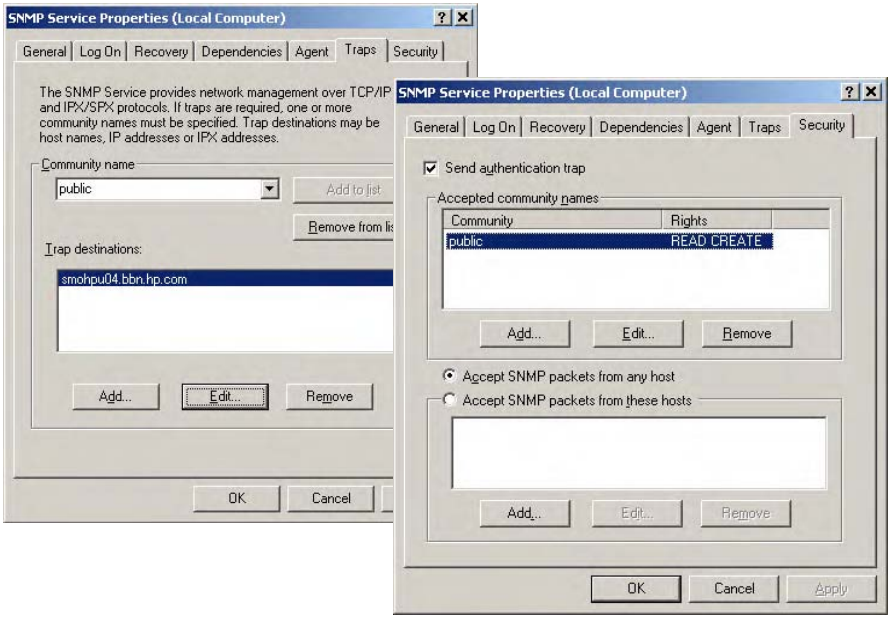
Configure the Windows system to forward its SNMP traps to the OVO Management Server as follows:

1. To enable Data Protector to send SNMP traps, run the command:
   **omnisnmp**
2. Add the following line to the
   `<Installed Package>\bin\OpC\install\opcinfo` file.
   **SNMP_SESSION_MODE NO_TRAPD**
3. Configure the SNMP Service on a Windows system to send traps to the OVO management server. The community name should be **public** (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\OmniBa
ckII\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 28.

   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:

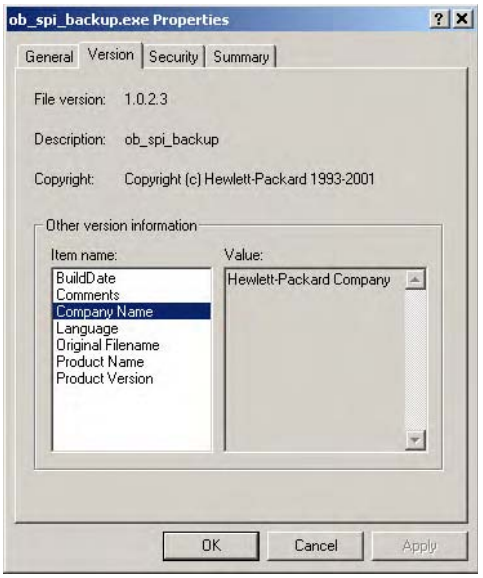
```
HP OpenView Storage Data Protector Integration into
OVO A.06.00 (<build_date>)
```

***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.

**Installing the Data Protector Integration**

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...**

   The `Uninstall policies on ...` window is displayed:


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

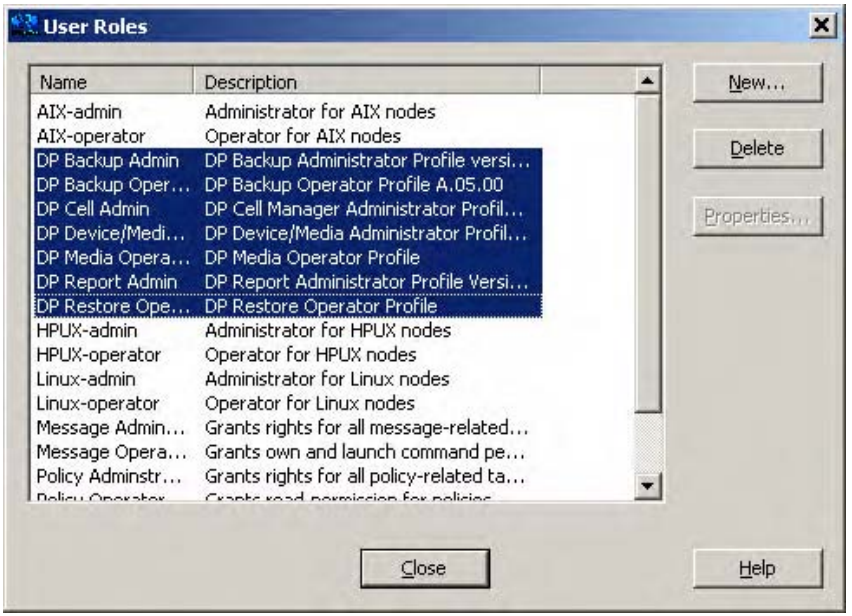
2. When asked to confirm the deletion, click **Yes** to remove the policies.

### 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, select: **Action** → **Configure** → **User roles...**

   The `User Roles` window is displayed:




2. Select all `DP*` user roles and click the **Delete** button and close this window.

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

To remove the DataProtector tools and directory from the OVO management server:

1. From the toolbar, select: **Action** → **Configure** → **Tools...**

The `Configure Tools` window is displayed:

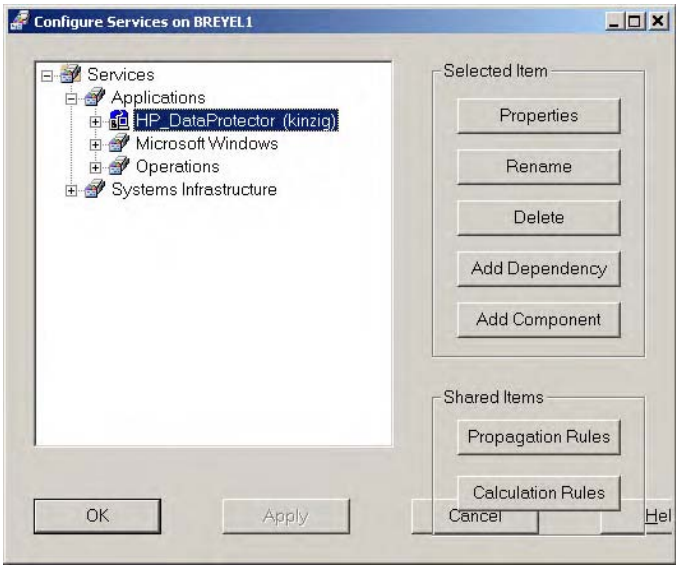

2. Right-click "`SPI for DataProtector`".
3. Select **Delete** from the pop-up menu. When asked to confirm the deletion, click **Yes**.
4. Click **Apply** and **OK** in the Configure Tools window to continue.

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

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

1. From the toolbar, select: **Action** → **Configure** → **Services...**

The `Configure Services` window is displayed:




2. 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 Data Protector DP ALL CELLS and DP ALL MGRS Node Directories from the OVO Management Server

To remove the Data Protector DP ALL CELLS and DP ALL MGRS node directories from the OVO Management Server:

1. From the toolbar, select: **Action** → **Configure** → **Nodes...**

   The `Configure Managed Nodes` window is displayed.

2. On the right side of the window, select `DP ALL CELLS`.
3. Right-click `DP ALL CELLS` and select **Delete** from the pop-up menu.
4. Follow the same procedure for `DP ALL MGRS`.

## 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-OVOW712-B.06.00` entry.
3. Click **Remove** to start the removal. This will take a short time.

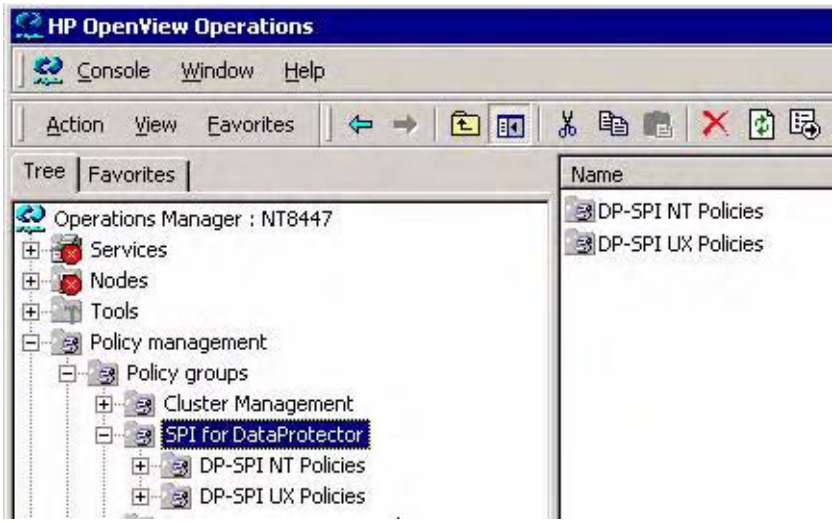
# 3 Using the Data Protector Integration

The sections in this chapter show which new components are added to OVO during the installation of the Data Protector Integration software and describe how to use them to best effect:

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

# Data Protector SPI Policies

The Data Protector Integration adds the `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:

`DP_Backup` Backup session messages

`DP_Restore` Restore session messages

`DP_Mount` Mount request messages

`DP_Misc` All other important Data Protector related messages

`DP_SPI` Messages from the Data Protector Integration

`DP_Interactive` 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

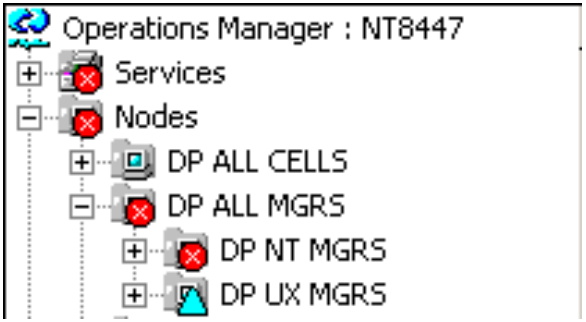
An OVO message includes the following parameters:

| | |
|---|---|
| *Message Group* | The following groups are available, as described above: `DP_Backup`, `DP_Restore`, `DP_Mount`, `DP_Misc`, `DP_SPI`, `DP_Interactive` |
| *Applications* | Set to Data Protector. |
| *Node* | Set to the hostname of the Data Protector system on which the event occurred. |
| *Severity* | 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. |
| *Service Name* | Depends on the impact the event has on a service. The value must map with a node in Data Protector's service tree. |
| *Object* | Allows the source of the event to be classified with fine granularity.<br>Data Protector SNMP traps set the parameter to `NOTIFICATION`.<br>Messages originating from a monitored logfile set this parameter to the name of the logfile.<br>• 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:

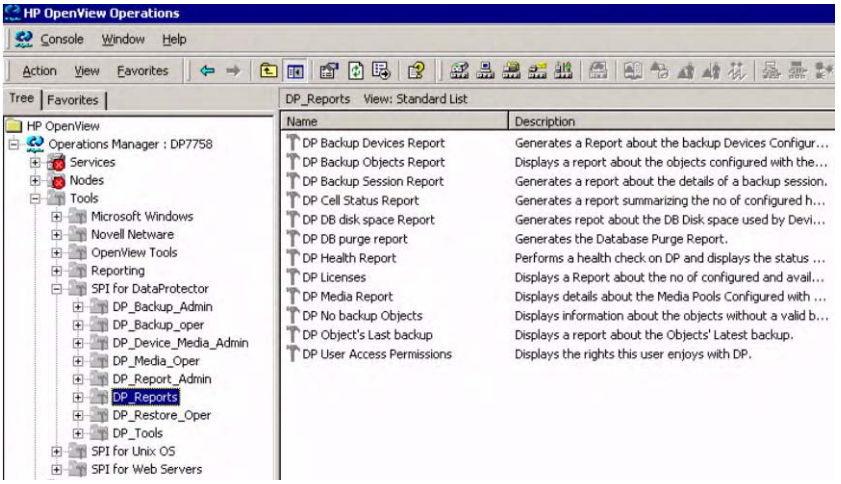
- `DP NT MGRS`
- `DP UX MGRS`

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.

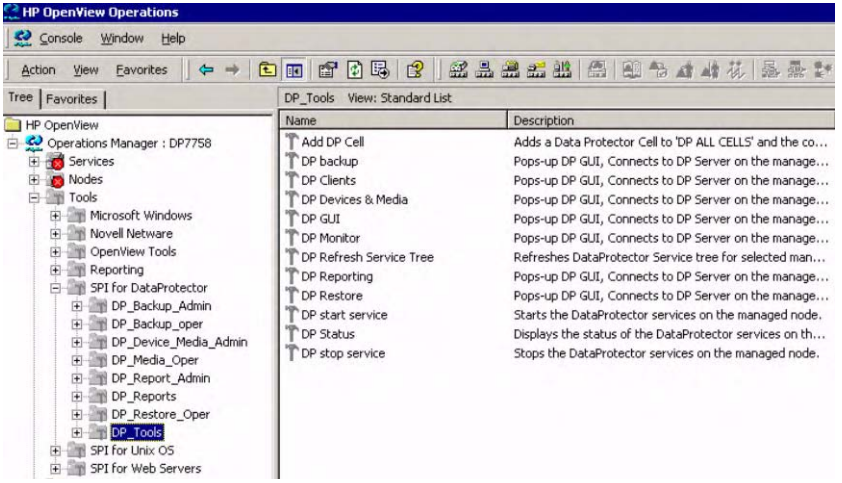
# Tools Groups

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:




- `DPSPI`, 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.

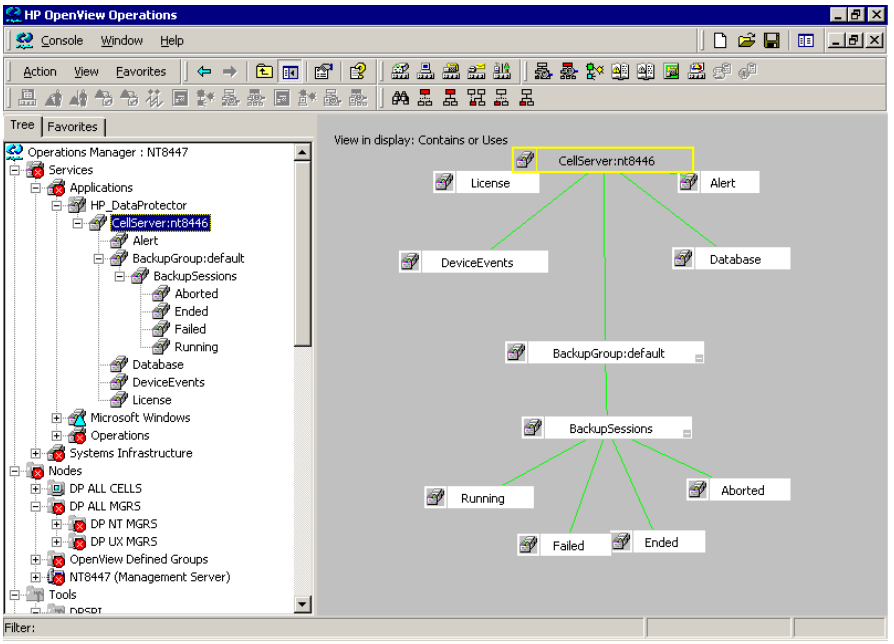
**DP Cell Status Report:**
Starts `omnicellinfo` remotely on the OVO Managed Node/DP Cell Manager.

**DP Status:**
Starts `omnisv -status` remotely on the selected Data Protector Cell Manager.

# Data Protector Service Tree

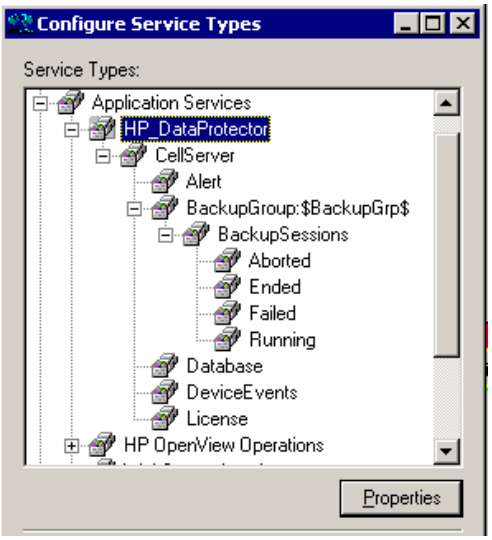
Data Protector is represented as a service tree with each cell an icon. The tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from Data Protector Integration's monitors. Figure 3-1 illustrates the `HP_Data Protector` service tree consisting of a sub-tree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

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.<br><br>Data Protector sends SNMP traps to trigger the update of these items. |
| Running | Updated by `Start of Session` SNMP trap issued by Data Protector notification. |

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

| Node | Description |
|---|---|
| Waiting | Updated by messages indicating that session is waiting because:<br>• the device is occupied<br>• the database is in use<br>• all licenses are currently allocated<br>• 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`

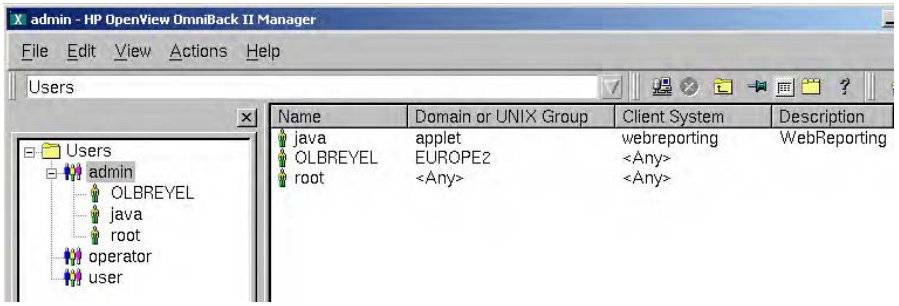
  UNIX user who's primary Unix group is marketing:
  `uid=4110(janesmith) gid=60(marketing)`

- **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 53. 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.

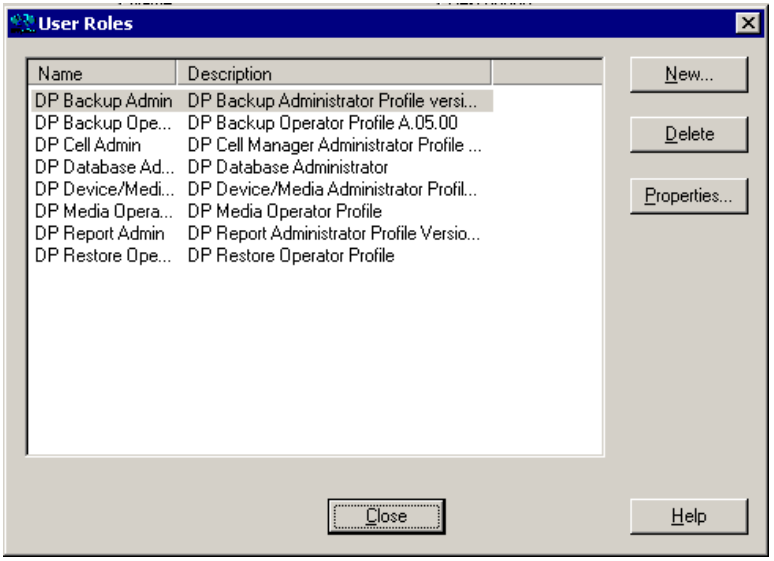
## OVO User Roles

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 56.

| | |
|---|---|
| DP Backup Admin | Restricted to a Data Protector Cell.<br>*Tool Groups:*<br>• `DP_Backup_Admin`<br>• `DP_Reports`<br>Can access messages in the OVO Message Browser, if the OVO message policy for detailed messages `DP_Detailed` is enabled. |

| | |
|---|---|
| DP Backup Operator | Restricted to a Data Protector Cell.<br>*Tool Groups:* `DP_Backup_Oper`<br>*Message Groups:*<br>• `DP_Backup`<br>• `DP_Misc`<br>• `DP_Mount`<br>These are backup session messages and mount requests of backup sessions messages. |
| DP Restore Operator | Restricted to a Data Protector Cell.<br>*Tool Groups:* `DP_Restore_Oper`<br>*Message Groups:*<br>• `DP_Restore`<br>• `DP_Misc`<br>• `DP_Mount`<br>These are restore session messages and mount requests of restore sessions messages. |
| DP Device & Media Administrator | Restricted to a Data Protector Cell.<br>*Tool Groups:* `DP_Device_Media_Admin`<br>Can access messages in the OVO Message Browser, if the OVO message policy for detailed messages `DP_Detailed` is enabled. |
| DP Media Operator | Restricted to a Data Protector Cell.<br>*Tool Groups:* `DP_Media_Oper`<br>*Messages:* Mount requests of backup and restore sessions (`DP_Mount`) messages. |

| | |
|---|---|
| DP Cell Administrator | Restricted to clients of Data Protector Cells.<br>*Tool Groups:*<br>• `DP_Reports`<br>• `DP_Tools`<br>*Message Groups:*<br>• `DP_Misc`<br>• `DP_SPI` |
| DP Report Administrator | Restricted to a Data Protector Cell.<br>*Tool Groups:* `DP_Reporting`<br>*Messages:* 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.<br>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.<br>*Note:* This is a powerful right that can affect the security of your system.<br>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 | Instals 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. *Note:* 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 | *Windows:* `DP_CheckProc_NT`<br>*UNIX:* `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:* >= 95% for error, >= 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 | ***Windows:*** `DP_CheckDB_NT`<br>***UNIX:*** `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 | *Windows:* `DP_CheckPoolStatus_NT`<br>*UNIX:* `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 | *Windows:* `DP_CheckPoolSize_NT`<br>*UNIX:* `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 | *Windows:* `DP_CheckLongBackup_NT`<br>*UNIX:* `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 `obspi.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

[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:

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

**Examples:**

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

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

### inet.log

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:

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

`debug.log` Exception messages that have not been handled.

`RDS.log` Raima Database service messages.

`readascii.log` Messages generated when the database is read from a file using `readascii`.

`writeascii.log` Messages generated when the database is written to a file with `writeascii`.

`lic.log` Unexpected licensing events.

`sm.log` 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

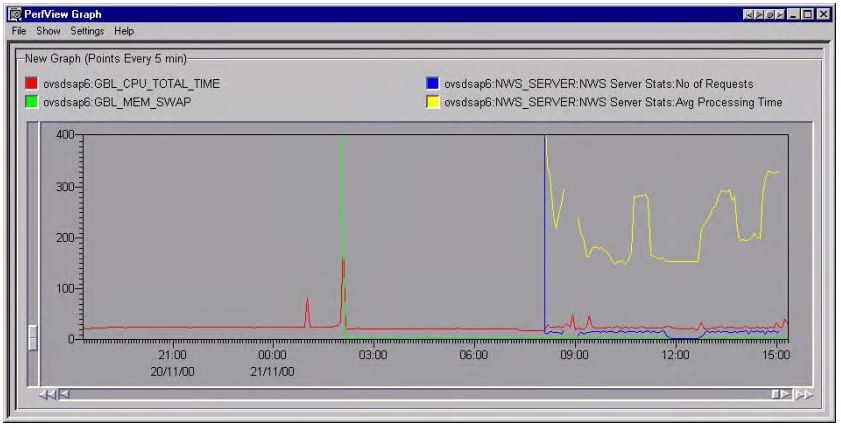
# Integration Overview

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**



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:

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

## 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. *HP-UX 11.x 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**.<br><br>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:

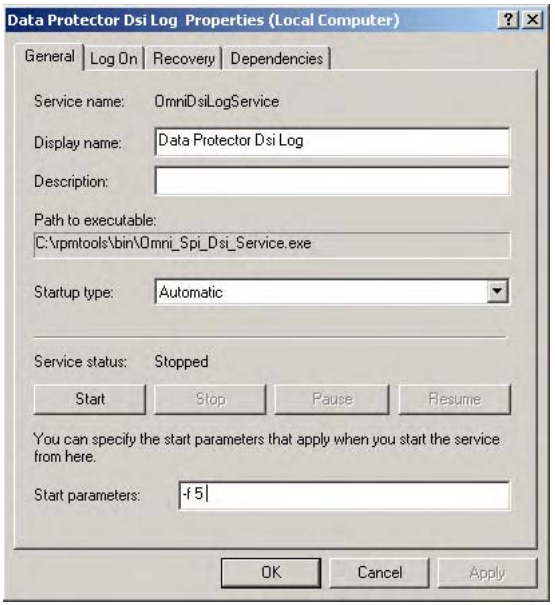
- Enter the command:

  **`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)

| | |
|---|---|
| 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.

The 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 104)
- Backup Duration Trend report (see page 105)
- Data Backup Trend report (see page 106)
- Number of Files Trend report (see page 107)
- Skipped Files report (see page 110)

- Backup Session Health overview (see page 108)
- Operational Error Status report (see page 109)
- Number of Successful Backups (see page 113)
- Capacity increase of Media Pool—Overview (see page 112)
- Backup Volume—Overview (see page 114)
- Number of Backup Up Files—Overview (see page 115)

# ReporterLite Integration with Data Protector Architecture

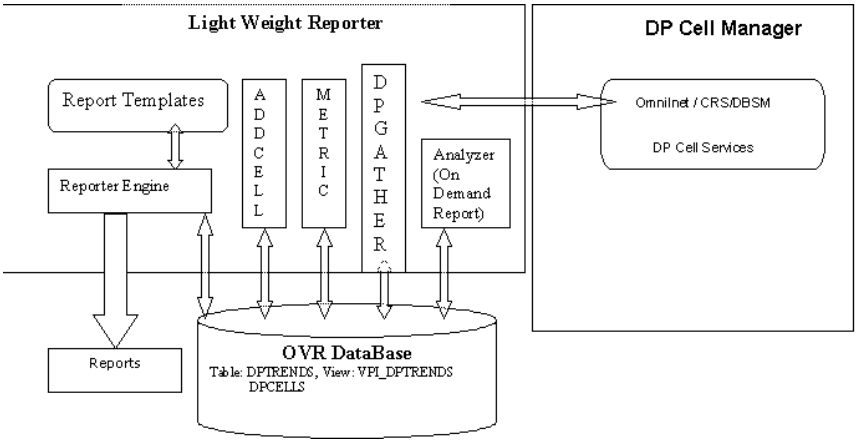
This integration is completely installed on OVO for Windows. The module can communicate with the Data Protector Management System directly to obtain backup Session Details necessary to generate reports.

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_OVOW712-B.06.00.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`:

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

## Verifying Installation

To verify the installation:

1. Open the `Add/Remove Programs` window:

   **Start → Settings → Control Panel → Add/Remove Programs**

2. Check `DPSPI-OVOW712-B.06.00` appears as an installed product.

## Uninstalling

Since this module is only installed as part of `DPSPI_OVOW712-B.06.00.msi`, it cannot be uninstalled separately.

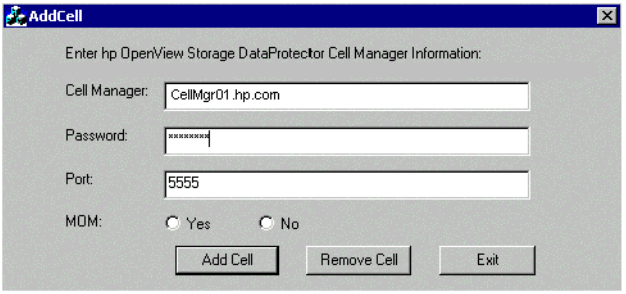
# Using the ReporterLite Integration with Data Protector

## 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**




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

### Troubleshooting

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

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

## 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
```

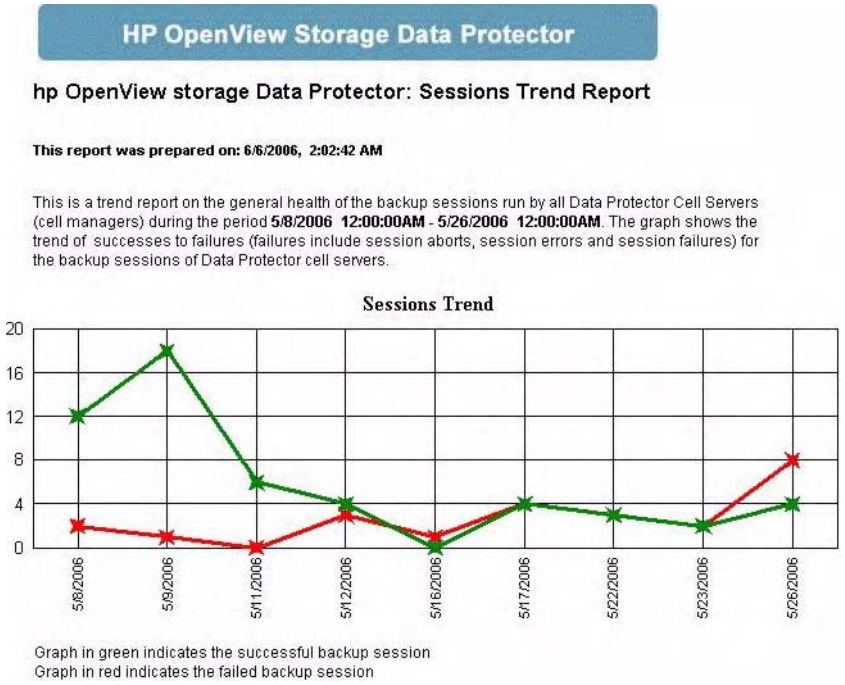
Where `PortNumber` is the port on which the web server is running.


Click on the appropriate link to view the desired report.

# Preconfigured Reports

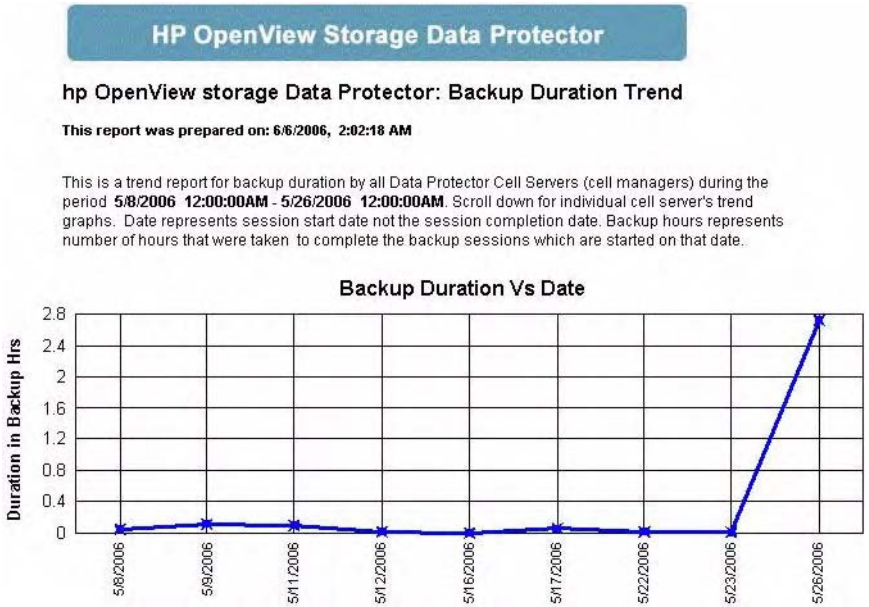
## Session Trend Report

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.



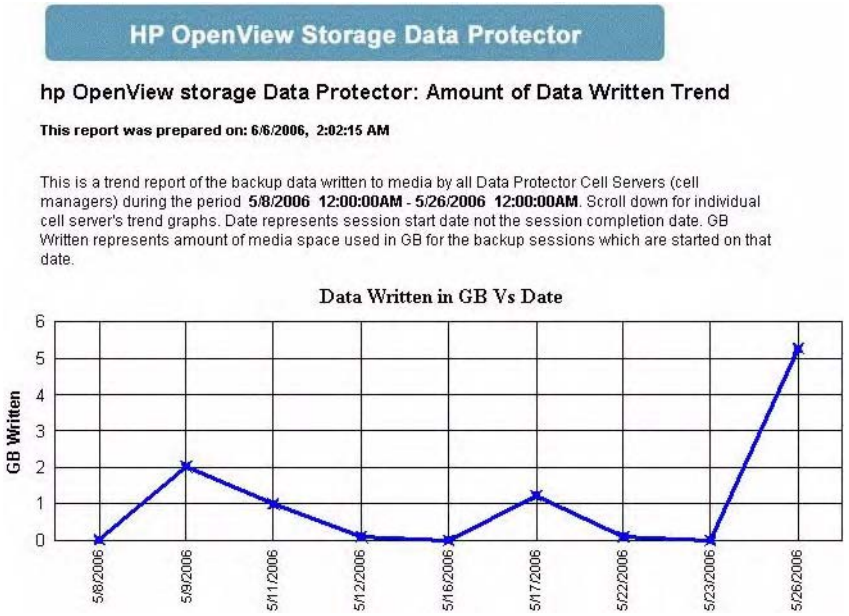
## Backup Duration Trend Report

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



## Amount of Data Written Trend Report

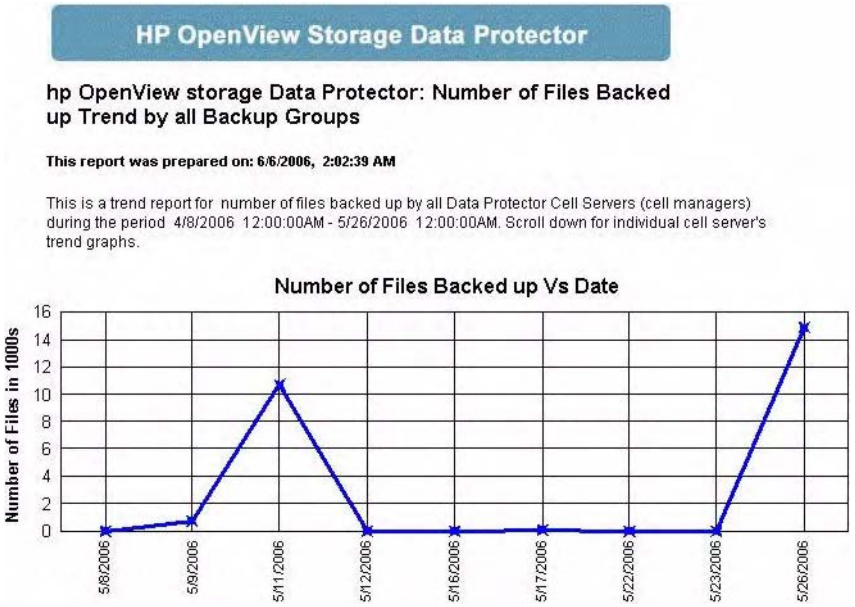
This graph shows how much data is written to backup media over time. The default period is 30 days (configurable by administrators). The graph shows trends for all sessions and for the individual cell manager.




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 111.

## Number of Files Backed Up Trend by All Backup Groups Report

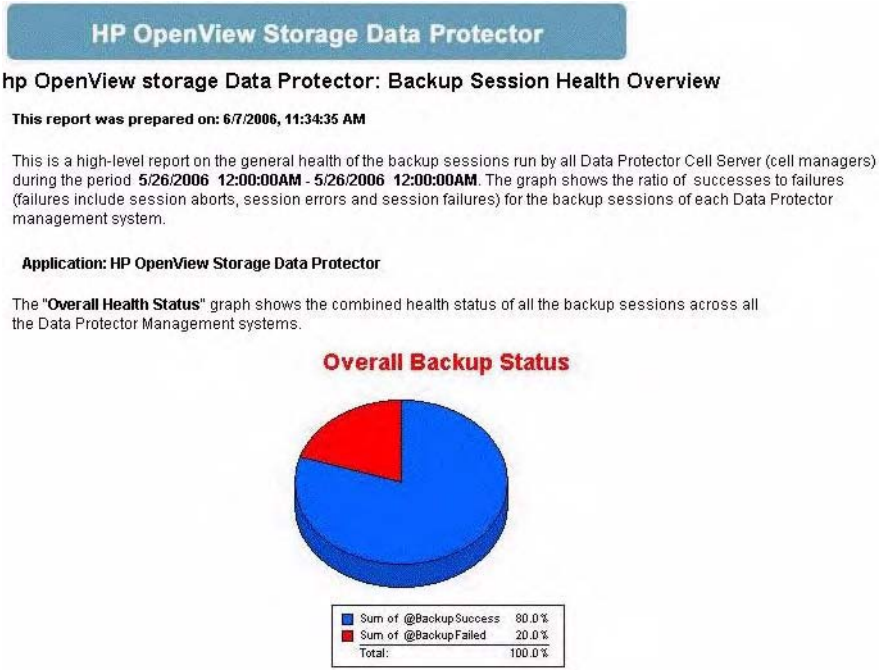
This graph shows the trend of the number of files (in 1000s) backed up by all Backup Groups over time. The default period is 30 days (configurable by administrators). The graph shows trends for all sessions and for the individual cell server.



## 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.



## 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**

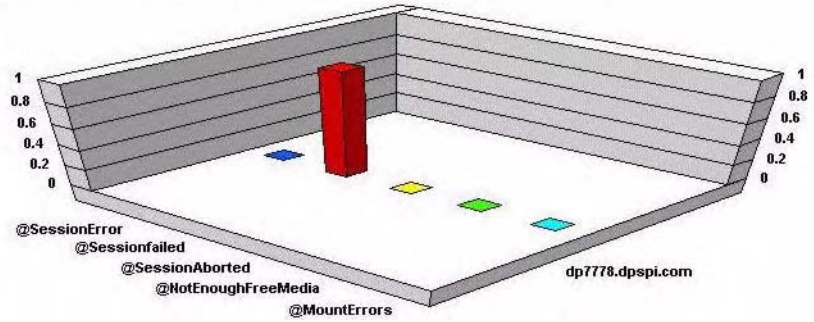
**hp OpenView storage Data Protector: Operational Error Status**

**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

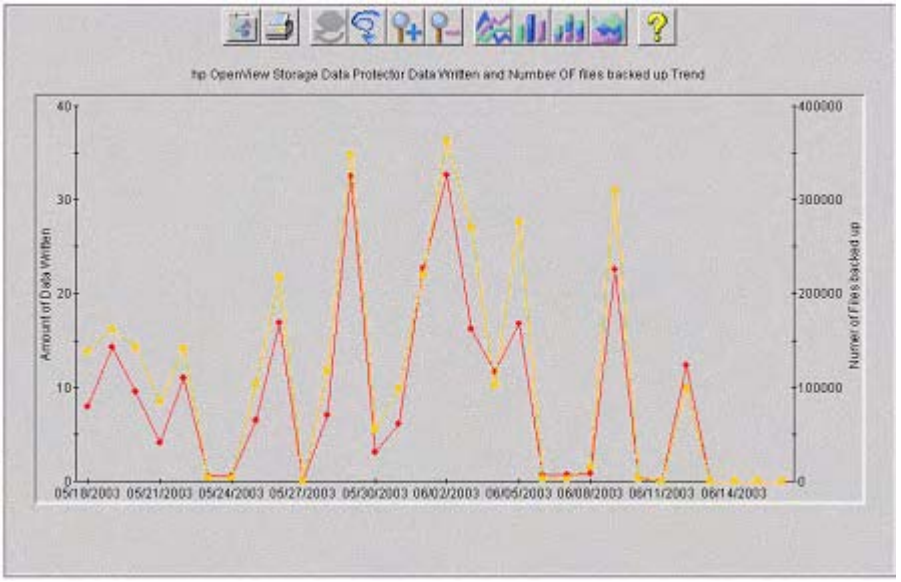
| Cell Manager | Session ID | Client | Skipped File Name |
|---|---|---|---|
| dp7778.india.hp.com | 2006/06/07-1 | dp7778.dpspi.com | C:\Program Files\HP OpenView\Data\Databases\reporter_ |
| dp7778.india.hp.com | 2006/06/07-1 | dp7778.dpspi.com | C:\Program Files\HP OpenView\Data\Databases\reporter_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

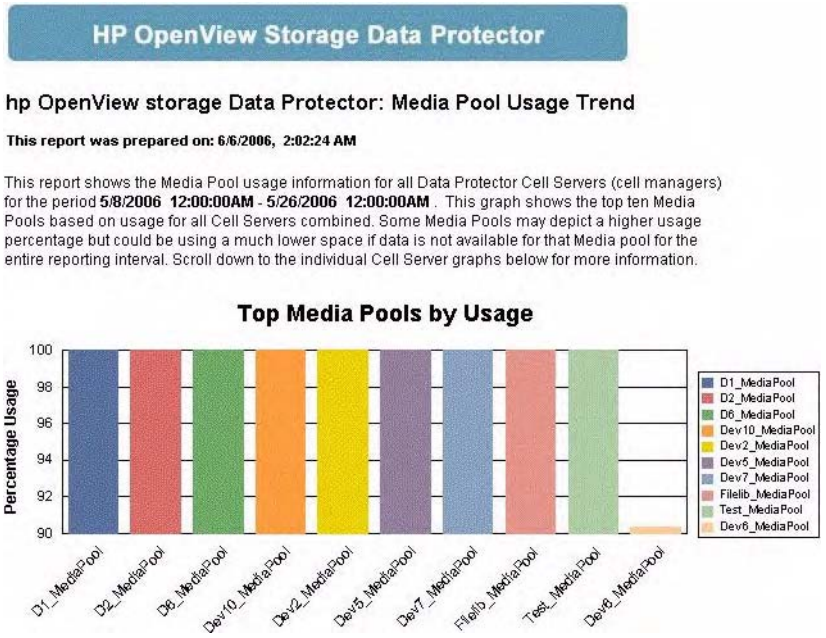
- `Sessions Trend`
- `GB Written Over Number of Files backed-up`

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



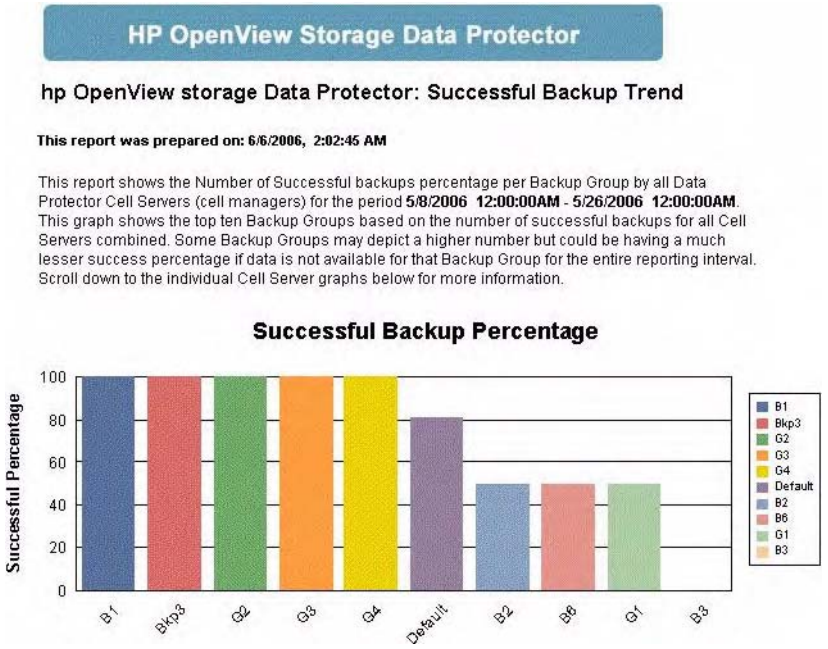
## Media Pool Usage Trend

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



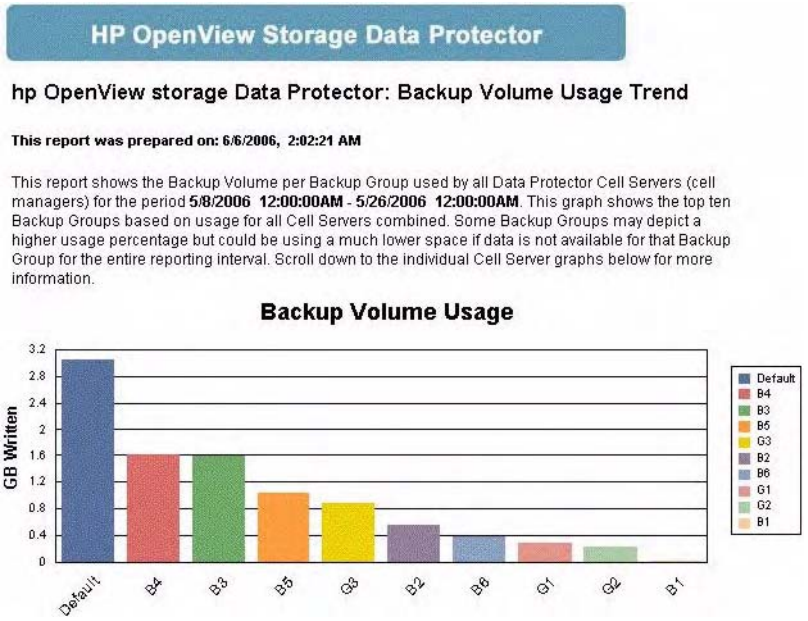
## Successful Backup Trend

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



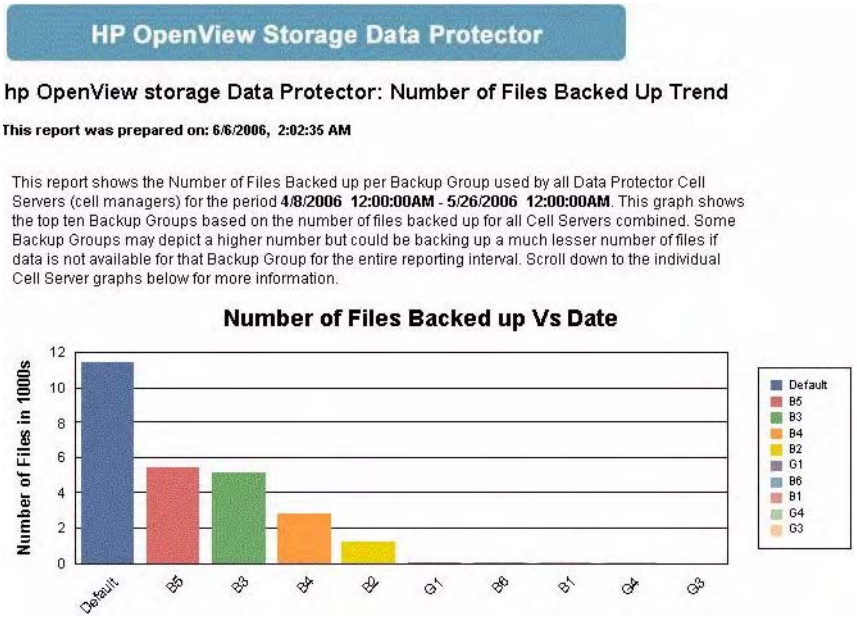
## Backup Volume Usage Trend

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



## Number of Files Backed Up Trend

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



# Index


**A**

agent
  configuration, 27
  operations versions supported by OVO, 20
  performance versions supported by OVO, 20
alarms
  OVPA, 91
  performance agent, 91
Amount of Data Written Trend report, 106
application
  groups
    DPSPI_Applications, 46
    DPSPI_Reports, 46
    using, 46
architecture, 12
ARM transactions, 81

**B**

Backup Duration Trend report, 105
Backup Session Health Overview report, 108
Backup Usage Trend report, 114

**C**

cell manager
  permanently running processes, 60
  prerequisites, 19
configuration agent, 27
configuration files, monitoring, 66
configuring DSI log service, 89

**D**

Data Protector
  cell manager prerequisites, 19
  collecting process data, 84
  configuring the DSI log service, 89
  installing the DSI log service, 87
  OVO operators, 56
  OVO user profiles, 53
  performance agent data collection frequency, 88
  performance agent data source integration, 86
  platforms, 17
  service tree, 48
  starting the DSI log service, 88
  uninstalling the DSI log service, 90
  user configuration on OVO managed nodes, 31
  user group, 51
  versions, 17
Data Protector Integration, 11
  application groups, 46
    DPSPI_Applications, 46
    DPSPI_Reports, 46
  architecture, 12
  database logfiles, 72
  default logfiles, 70
  directories on OVO management server, 23, 24
  inet.log logfile, 71
  installing on OVO management server, 23
  message formats, 43
  message groups, 42
  monitored logfiles, 70
  monitored object, 60
  node groups, 44
  non-monitored logfiles, 73
  omnisv.log logfile, 70
  program identification, 31
  purge.log logfile, 72
  user profiles, 51
  users, 52
data source integration, 86
  collection frequency, 88
database monitor thresholds, 61
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, 46
DPSPI_Reports application group, 46
DSI log service
  configuring, 89
  installing, 87
  starting, 88
  uninstalling, 90

**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

# Index


prerequisites, 19
Data Protector Integration on OVO management server, 23
Data Protector versions, 17
depot, 23
DSI log service, 87
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, 79
Performance integration components, 79
prerequisites, 17
RAM, 22
ReporterLite, 99
verification, 25

**L**

logfiles
Data Protector database, 72
Data Protector default, 70
inet.log, 71
monitored, 70
not monitored, 73
omnisv.log, 70
purge.log, 72
long running backup sessions, 65

**M**

managed nodes
Data Protector user configuration, 31
SNMP configuration on UNIX, 27
SNMP configuration on Windows, 29
management server
depot installation, 23
installation verification, 25
installing Data Protector Integration, 23
patches, 18
media pool size monitor thresholds, 64
media pool status monitor thresholds, 63
Media Pool Usage Trend report, 112
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, 70
database logfiles, 72
default logfiles, 70
inet.log logfile, 71
omnisv.log logfile, 70
purge.log logfile, 72
monitored object, 60
configuration files, 66
databases, 61
long running backup sessions, 65
media pool size, 64
media pool status, 63
permanently running processes on cell manager, 60
monitoring configuration files, 66

**N**

node groups, using, 44
non-monitored logfiles, 73
Number of Files Backed Up Trend report, 107, 115

**O**

obspi.spec file, 86
On Demand report, 111
OpenView Reporter, 95
operating system users, 51
Operation Error Status report, 109
operators, Data Protector OVO, 56
OVO
additional software for Windows nodes, 20, 21
Data Protector
operators, 56
user profiles, 53
Data Protector Cell Manager installation prerequisites, 19
Data Protector Integration directories, 23, 24
managed nodes
Data Protector user configuration, 31
installation prerequisites, 19
SNMP configuration on UNIX, 27
SNMP configuration on Windows, 29
management server
depot installation, 23
hardware prerequisites, 19
installing
prerequisites, 18
verification, 25
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, 52
OVPA
alarms, 91
data collection frequency for Data Protector, 88
Data Protector process data, 84
data source integration for Data Protector, 86
installing integration components, 79
integration overview, 77
transaction times metrics, 81
OVR, 95

**P**

parm file, 81, 84, 85
patches
management server, 18
OVO management server, 18
Performance
agent alarms, 91
agent versions supported by OVO, 20
installing integration components, 79
integration overview, 77
transaction times metrics, 81
prerequisites, 17
Data Protector cell manager, 19
OVO managed node, 19
OVO management server, 18
process data, 84
profiles, user, 51
program identification
Data Protector Integration, 31

**R**

RAM requirements, OVO server, 22
ReporterLite, 93
installation, 99
integration with Data Protector, 97
reports
Amount of Data Written Trend, 106
Backup Duration Trend, 105
Backup Session Health Overview, 108
Backup Usage Trend, 114
generating, 102
Media Pool Usage Trend, 112
Number of Files Backed Up Trend, 107, 115
On Demand, 111
Operation Error Status, 109
preconfigured, 104
Session Trend, 104
Skipped Files, 110
standard, 95
Successful Backup Trend, 113
viewing, 103

**S**

Service Navigator
Data Protector service tree, 48
service tree, Data Protector, 48
Session Trend report, 104
Skipped Files report, 110
SNMP
configuration on UNIX OVO managed nodes, 27
configuration on Windows OVO managed nodes, 29
Emanate Agent Windows nodes, 21
software prerequisites, OVO management server, 18
starting DSI log service, 88
Successful Backup Trend report, 113

**T**

thresholds, monitored object, 60
transaction times metrics, 81
ttdconf file, 82

**U**

uninstalling DSI log service, 90
uninstalling ReporterLite, 99
user
Data Protector Integration, 52
groups, Data Protector, 51
operating system, 51
profiles
Data Protector OVO, 53
OVO, 52
using, 51
using
application groups, 46
applications
DPSPI_Applications, 46
DPSPI_Reports, 46
Data Protector
database logfiles, 72
default logfiles, 70
inet.log logfile, 71
omnisv.log logfile, 70
purge.log logfile, 72
message formats, 43
message groups, 42
monitored
logfiles, 70
object, 60

node groups, 44
non-monitored logfiles, 73
user profiles, 51

**V**

verifying management server
installation, 25

**W**

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