HP OpenView Storage Data Protector

Integration Guide
for
HP OpenView Operations for UNIX

Version: A.06.00

HP-UX, Solaris and Windows

invent

Manufacturing Part Number: B6960–96015

July 2006

Legal Notices

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

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

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

UNIX ® is a registered trademark of The Open Group.

Contents

1. Introduction

2. Installing the Data Protector Integration

3. Integration into HP OpenView Service Navigator

4. Using the Data Protector Integration

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
B6960–90068	July 2002	HP OpenView Storage Data Protector A.05.00
B6960–90089	April 2003	HP OpenView Storage Data Protector A.05.10
B6960–90118	October 2004	HP OpenView Storage Data Protector A.05.05
B6960–90016	July 2006	HP OpenView Storage Data Protector A.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), HP OpenView Service Navigator, 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.

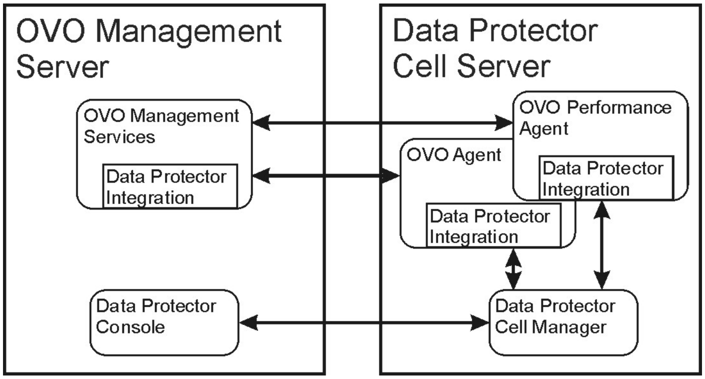
The Data Protector Integration offers the following key features:

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

The main benefits of the integration are:

- Centralized problem management using OVO agents at Data Protector managed nodes.Using a central management server avoids duplicated administrative effort.
- Real-time event and configuration information (including online instructions) for fast problem resolution.
- Powerful monitors to detect potential problem areas and to keep track of system and Data Protector events.
- Performance data collectors to ensure continuous system throughput and notify any performance bottlenecks.
- A complement to 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.

Architecture


OVO Management Server
OVO Management Services
Data Protector Integration
Data Protector Console
Data Protector Cell Server
OVO Performance Agent
Data Protector Integration
OVO Agent
Data Protector Integration
Data Protector Cell Manager

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 also installed on the OVO management server, so the OVO user can start the Data Protector GUI as an OVO application and connect to any available Data Protector Cell Manager. Both Windows and UNIX Data Protector Cell Managers are accessible from the same OVO Application Bank. This is facilitated by the Data Protector Console using Data Protector's communication protocol on port 5555 to exchange data.

Data Protector OVO templates configure the OVO agent on a Data Protector Cell Manager. They monitor:

- Data Protector logfiles
- Data Protector SNMP traps

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

Self-Healing Services

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

1. The software detects a problem.
2. It collects relevant information relating to the problem.
3. The information is sent to HP, where it is analyzed for possible solutions.
4. A web page is published on eCare with the analysis results and any relevant documents relating to the problem.
5. You are sent an email notifying you a problem has been detected and a web page prepared.

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

See “Using Self-Healing Services” on page 62 for details of how the Self-Healing Services are used with DPSPI.

For more information on SHS see http://www.managementsoftware.hp.com/service/selfheal/index.html.

2 Installing the Data Protector Integration

In this chapter you will find information on:

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

Supported Platforms and Installation Prerequisites

Only install the HP OpenView Storage Data Protector Integration in an environment consisting of:

- One or more systems running OVO management server
- OVO agent running on systems with the Data Protector Cell manager

It is only guaranteed to work in these environments.

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 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		✔	✔	✔
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 OVO server can run on a different host system from the system on which the Data Protector Cell Manager is installed.

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

Table 2-2 **OVO Management Server Supported Versions**

Application	Supported Versions
OVO UNIX	*English and Japanese:* OVO/Unix 7.x including Service Navigator 7.x is supported on HP-UX 11.0, 11.11, 11.23, Solaris 8, Solaris 9
	English and Japanese: OVO/Unix 8.x including Service Navigator 8.x is supported on HP-UX 11.0, 11.11, 11.23, Solaris 8, Solaris 9

OVO Patches

Ensure that up-to-date patches are installed.

To support SUSE Linux Enterprise Server 9 nodes, install the following patches on the OVO Management server:

O/S	Patch Number	Description
HP-UX 11.x	PHSS_33692	Consolidated patch for Linux OVO Agents and to support SUSE Linux Enterprise Server 9.x
Solaris 7, 8, 9	ITOSOL_00453	Consolidated patch for Linux OVO Agents and to support SUSE Linux Enterprise Server 9.x

Software Prerequisites on the OVO Management Server

Ensure the following software is installed on the OVO management server system:

- HP OpenView Operations, version A.07.xx or A.08.xx. 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.

  The `swlist DATA-PROTECTOR` command returns:

  ```
  DATA-PROTECTOR          A.06.00HP OpenView Storage Data Protector
  DATA-PROTECTOR.OMNI-CCA.06.00HP OpenView Storage Data Protector Cell
  Console
  DATA-PROTECTOR.OMNI-COREA.06.00HP OpenView Storage Data Protector Core
  ```

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

NOTE The OVO and OVPA patches must be installed on the OVO management server and distributed to the managed node systems by the OVO administrator before the Data Protector Integration is distributed.

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**

Agent	Operating System
OVO/Unix Agent 7.x	HP-UX 11.0, 11.11, 11.23 Solaris 7, Solaris 8, Solaris 9 Win 2000, Windows 2003 Server, Win XP Pro (32-bit) SUSE Linux Enterprise Server 9.x
OVO/Unix Agent 8.x:	
HTTPS Agents	HP-UX 11.0, 11.11, 11.23 Solaris 7, Solaris 8, Solaris 9, Solaris 10 Win 2000, Win XP Pro (32-bit), Win Server 2003 SUSE Linux Enterprise Server 9.x
DCE Agents	HP-UX 11.0, 11.11, 11.23 Solaris 8, Solaris 9, Solaris 10 Win 2000, Win XP Pro (32-bit), Win Server 2003 SUSE Linux Enterprise Server 9.x

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, C.03.86
Solaris 7, 8, 9, 10	C.03.82, C.03.82
Microsoft Windows 2000, Windows XP Pro (32-bit), Windows Server 2003	C.03.65
SUSE Linux Enterprise Server 9 (x64)	C.03.86

Additional Software for HP-UX Managed Nodes

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

SNMP Emanate Agent (required)

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

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

- The solution scales better. Additional Data Protector Cell Managers do not put additional load on the management server because SNMP traps are processed on the managed node.
- Any automatic action configured as a response to an SNMP trap can be triggered and run locally on the managed node without involving the management server.
- Since SNMP traps are not sent from the managed node to the management server, the network load decreases, and the probability that traps are lost is significantly reduced. Security over public networks is also improved. OpC messages are sent by the OVO agent to the OVO management server using either HTTPS and DCE/RPCs, which allow authentication and encryption.

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

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

You should see the following entry:

```
OVSNMPAgent        "SNMP Agent functionality"
```

Additional Software for Windows Managed Nodes

The following required and optional software 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.

FTP Service (optional)

If the Data Protector Cell Manager is installed on a number of Windows systems, consider installing the Windows FTP service. This provides the most convenient way of deploying the OVO Agent from the Unix OVO Management Server to a Windows system.

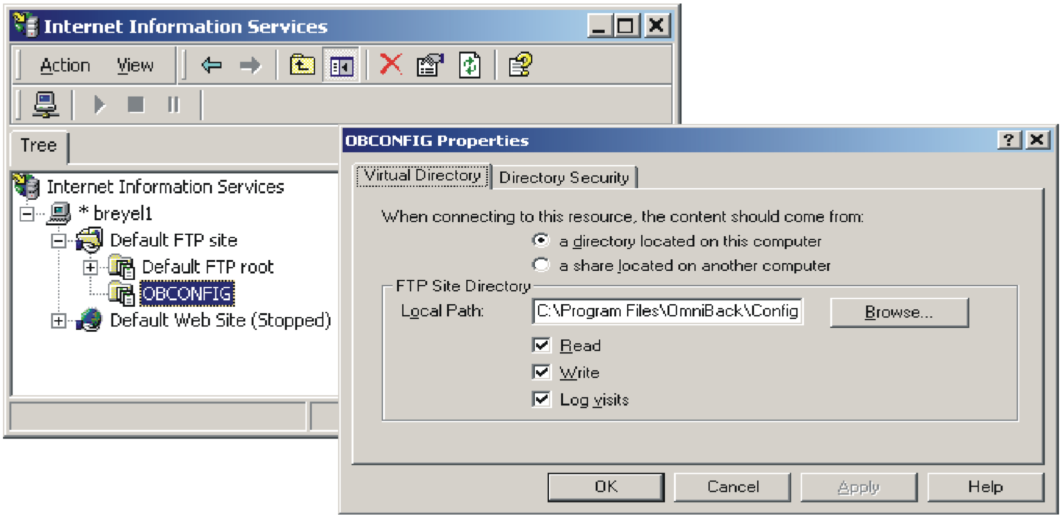
NOTE For details of other ways of deploying the OVO Agent to a Windows system, see the *HP OpenView Operations Installation Guide for the Management Server* and the *HP OpenView Operations Administrator's Reference* guides.

The Windows FTP service is also a convenient way of distributing Data Protector configuration files from a central system to all Data Protector Cell Managers.

The FTP service is required for the `obusergrp.pl` utility to work, since it reads, modifies and writes the `ClassSpec` file. This file resides in Data Protector's configuration directory.

The FTP service is part of the Internet Service Manager Windows Component on Windows 2000. Configure the directory `C:\Program Files\OmniBack\Config` (or equivalent directory, if you have chosen a custom path) as a Virtual Directory with the name "`OBCONFIG`". The `obusergrp.pl` tool requires this name.

Figure 2-1 **Configuring the Windows FTP Service**



When connecting to this resource, the content should come from:

● a directory located on this computer
○ a share located on another computer

FTP Site Directory

Local Path: C:\Program Files\OmniBack\Config

☑ Read
☑ Write
☑ Log visits

remsh Daemon (optional)

To run the Data Protector Start Service, Data Protector Stop Service and Data Protector Status applications on a Windows managed node from the OVO Application Bank, install a `remsh` daemon on the Windows system. Use the daemon supplied with the Windows Resource Kit or another, such as from the MKS Toolkit.

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 the managed node.

Machine	OVO Version	Operating System	Total
OVO Management Server	OVO 7.x, 8.x	HP-UX 11.00, 11.11, 11.23	15 MB
		Solaris 7, 8, 9, 10	15 MB

Machine	OVO Version	Operating System	Total
OVO Managed Node	OVO 7.x, 8.x	HP-UX 11.00, 11.11, 11.23	2 MB
		Solaris 7, 8, 9, 10	2 MB
		SUSE Linux Enterprise Server 9	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 as a Software Distributor (SD) depot used to install the integration onto the OVO management server system through SD. 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.

Limitations

- Cluster installations are not supported.
- On HP-UX 11.23 (Itanium), there is no GUI for Data Protector, so some Data Protector Integration applications will not work. See page 61 for a list.

Upgrading the DPSPI

Before installing the latest version of DPSPI, uninstall any older DPSPI. During this process, the existing configuration is unaltered and can be retained for use with the latest SPI.

Installation

Data Protector Integration software is split into SD filesets and includes the following components:

- Monitoring and administration programs
- OVO configuration data (including message groups, templates, and user profiles)
- Data Protector Integration applications
- Data Protector Integration documentation

To install the software on the management server, execute the following command on the server:

```
# swinstall -s <depot_location> SPI-DATAPROTECTOR-OVO
```

The following filesets are installed on an OVO Management Server on UNIX:

`SPI-DP-AGT-HP` OVO agent files for the DP Cell Manager on

	HP-UX
`SPI-DP-AGT-NT`	OVO agent files for the DP Cell Manager on Windows
`SPI-DP-AGT-SOL`	OVO agent files for the DP Cell Manager on Solaris
`SPI-DP-CONF`	OVO templates and configuration files for the OVO Management Server
`SPI-DP-DOC`	Data Protector Integration’s documentation in PDF format

The following fileset is installed on an OVO Management Server on HP-UX:

`SPI-DP-SRV-HP`	Data Protector Integration’s executables and scripts for the OVO Management Server on HP-UX

The following fileset is installed on an OVO Management Server on Solaris:

`SPI-DP-SRV-SOL`	Data Protector Integration’s executables and scripts for the OVO Management Server on Solaris

The following directories are created on the OVO management server system:

`/opt/OV/OpC/integration/obspi/bin`	Binary and script files
`/opt/OV/OpC/integration/obspi/etc`	XML template files for Service Navigation tree
`/opt/OV/OpC/integration/obspi/lib`	Libraries and message catalogs
`/opt/OV/OpC/integration/obspi/vpp`	Configuration files for Performance Agent
`/opt/OV/OpC/integration/obspi/doc`	Documentation
`/var/opt/OV/log/obspi`	Logfiles
`/var/opt/OV/share/tmp/obspi`	Temporary and runtime files
`/var/opt/OV/share/tmp/OpC_appl/obspi`	OVO files in uploadable format

`/etc/opt/OV/share/obspi/conf`	XML files uploaded by Service Manager
`/etc/opt/OV/share/bitmaps/C/omniback`	Icons and bitmaps
`/etc/opt/OV/share/registration/C/DPSPI`	Application registration file

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

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`
- `ob_spi_backup.exe`
- `ob_spi_db.exe`
- `ob_spi_file.exe`
- `ob_spi_poolsize.exe`
- `ob_spi_poolstatus.exe`
- `ob_spi_proc.exe`
- `DPCmd.exe`
- `DPPath.exe`

- `dpsvc.pl`
- `ob_spi_medialog.vbs`
- `ob_spi_medialog.bat`
- `ob_spi_omnisvlog.vbs`
- `ob_spi_omnisvlog.bat`
- `ob_spi_purgelog.vbs`
- `ob_spi_purgelog.bat`

Installation Verification

Check the following logfiles for errors:

- `/var/adm/sw/swagent.log`
- `/var/opt/OV/log/OpC/mgmt_sv/obspicfgupld.log`

To check the Software Distributor installation, enter the following:

```
# swlist -a revision -a state -a title -l fileset
SPI-DATAPROTECTOR-OVO
```

You should get the following response.

```
# SPI-DATAPROTECTOR-OVO                  SPI-DATAPROTECTOR-OVO
                                         HP OpenView Storage Data Protector Integration
                                         into OVO
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-HP      A.06.00  Configured   Data Protector Integration's
                                                               files for the DP Cell Manager
                                                               on HP-UX 11.x
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-NT      A.06.00  Configured   Data Protector Integration's
                                                               files for the DP Cell Manager
                                                               on Windows
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-SOL     A.06.00  Configured   Data Protector Integration's
                                                               files for the DP Cell Manager
                                                               on Solaris 7, 8, 9 and 10
SPI-DATAPROTECTOR-OVO.SPI-DP-CONF        A.06.00  Configured   Data Protector Integration's
                                                               templates for the Mgmt. Server
SPI-DATAPROTECTOR-OVO.SPI-DP-DOC         A.06.00   Configured  Data Protector Integration's
                                                               documentation
```

On HP-UX OVO Management Server:

```
SPI-DATAPROTECTOR-OVO.SPI-DP-SRV-HP      A.06.00  Configured   Data Protector Integration's
                                                               executables and scripts for the
                                                               Management Server
```

On Solaris OVO Management Server:

```
SPI-DATAPROTECTOR-OVO.SPI-DP-SRV-SOL     A.06.00  Configured   Data Protector Integration's
                                                               executables and scripts for the
                                                               Management Server
```

Agent Installation

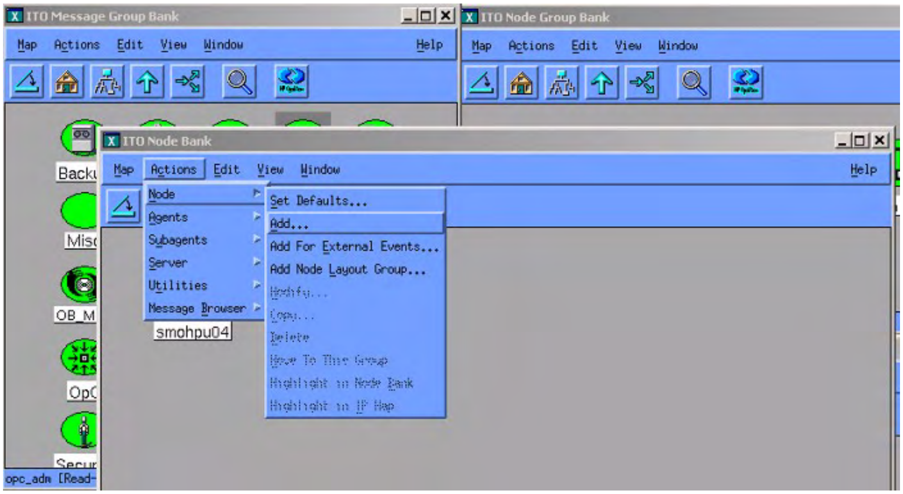
Distribute agent software to managed nodes in three stages:

1. Add the Data Protector Cell manager host system to the OVO managed environment as a managed node.
2. Run the `Add Data Protector Cell` application for each Data Protector Cell manager node.
3. Distribute software, actions, commands, monitors and templates to the Data Protector Cell Manager managed node.

Adding the Data Protector Cell Manager System as an OVO Node

To add the DP Cell manager host system to the OVO managed environment as a managed node:

1. Login to OVO as user `opc_adm`.
2. Open the `Node Bank`.

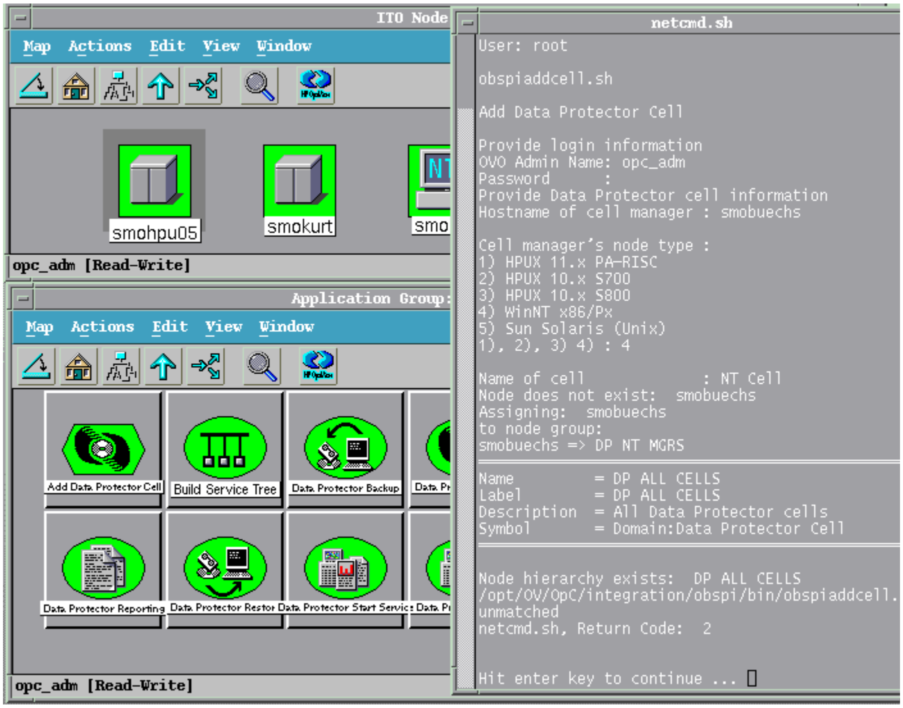


3. Select **Actions** → **Node** → **Add...**
4. Add the label and hostname of the new node in the `Add Node` window.

Running the Add Data Protector Cell Application

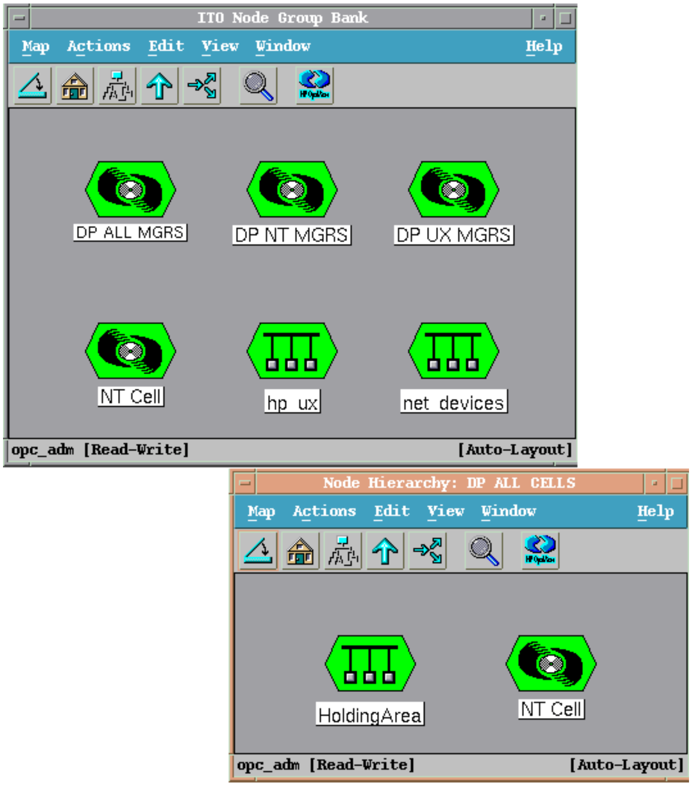
1. As user `opc_adm`, open the `Node Bank` and the `DPSPI_Applications` window.
2. Select the **Data Protector Cell Manager** node from the `Node Bank`. Drag and drop it onto the **Add Data Protector Cell** application.

   This opens a terminal window where you are asked to input some information:



```
User: root

obspiaddcell.sh

Add Data Protector Cell

Provide login information
OVO Admin Name: opc_adm
Password       :
Provide Data Protector cell information
Hostname of cell manager : smobuechs

Cell manager's node type :
1) HPUX 11.x PA-RISC
2) HPUX 10.x S700
3) HPUX 10.x S800
4) WinNT x86/Px
5) Sun Solaris (Unix)
1), 2), 3) 4) : 4

Name of cell               : NT Cell
Node does not exist:  smobuechs
Assigning:  smobuechs
to node group:
smobuechs => DP NT MGRS

Name         = DP ALL CELLS
Label        = DP ALL CELLS
Description  = All Data Protector cells
Symbol       = Domain:Data Protector Cell


Node hierarchy exists:  DP ALL CELLS
/opt/OV/OpC/integration/obspi/bin/obspiaddcell.
unmatched
netcmd.sh, Return Code:  2


Hit enter key to continue ... 
```

As a result, a new node group is added to the `Node Group Bank` and a new layout group is added to the `DP ALL MGRS` node hierarchy (`NT CELL` in the example below):

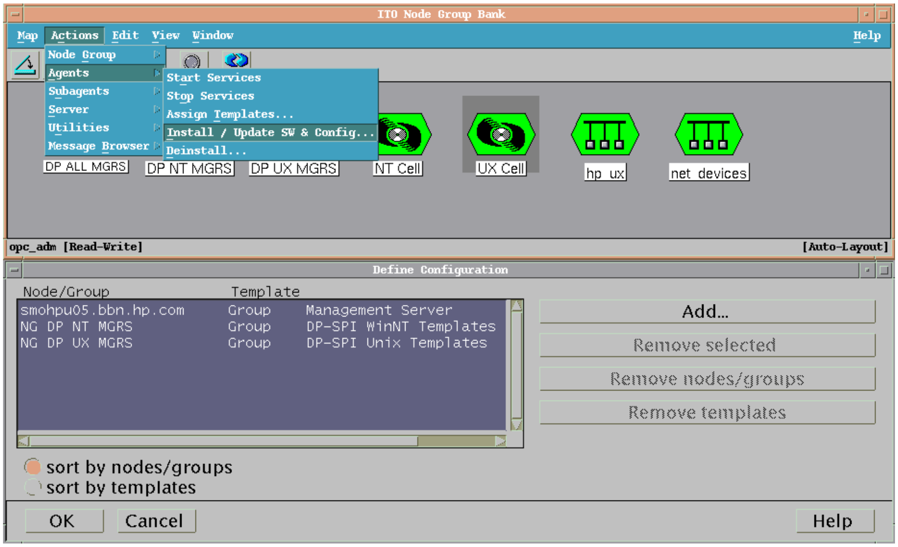


Distributing Software, Actions, Commands, Monitors and Templates to the Data Protector Cell Manager

To distribute items to the DP Cell Manager managed node (appropriate assignments should have been made during installation):

1. Log in as user `opc_adm`.
2. Select the appropriate node group from the `Node Group Bank`. The node group `DP ALL MGRS` contains all Data Protector Cell Managers.
3. From the `Node Group Bank`, select:

Actions → Agents → Install / Update SW & Config...



opc_adm [Read-Write] [Auto-Layout]

Node/Group	Template	
smohpu05.bbn.hp.com	Group	Management Server
NG DP NT MGRS	Group	DP-SPI WinNT Templates
NG DP UX MGRS	Group	DP-SPI Unix Templates

● sort by nodes/groups
○ sort by templates

4. Follow any instructions displayed in the terminal window.

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 HP-UX nodes to receive SNMP traps from Data Protector:

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

   - If an `ovtrapd` process is running add:
     `SNMP_SESSION_MODE    TRY_BOTH`

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

2. Configure the SNMP Emanate Agent to send SNMP traps to the local OVO agent by adding the following line to the `/etc/SnmpAgent.d/snmpd.conf` file:

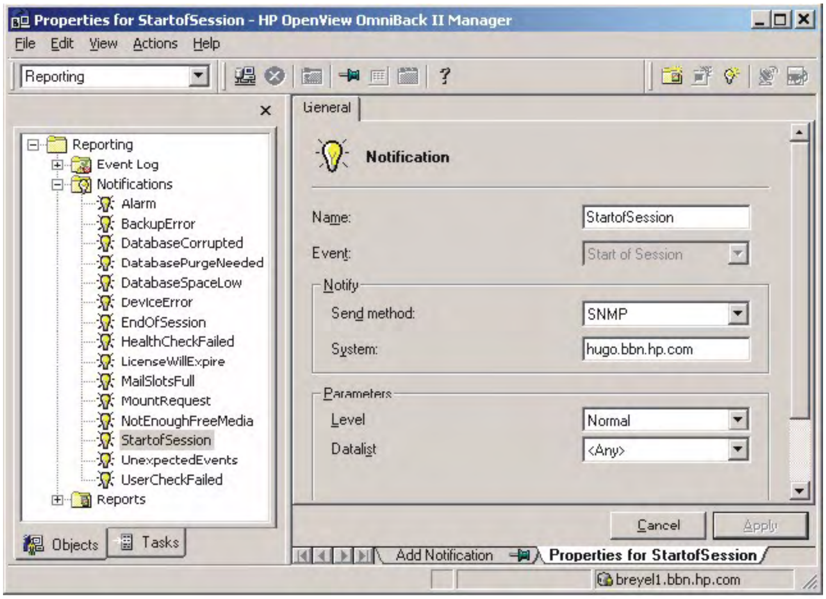
   `trap-dest: 127.0.0.1`

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



Name: StartofSession

Event: Start of Session

Send method: SNMP

System: hugo.bbn.hp.com

Level: Normal

Datalist: <Any>

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:

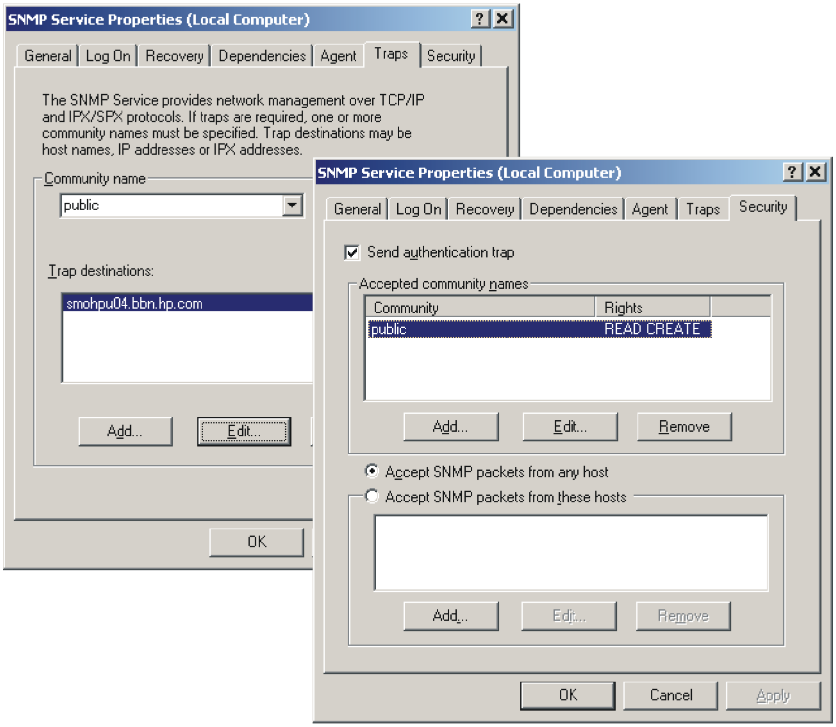
1. For DCE agent nodes, add the following line to the `\usr\opt\OV\bin\OpC\install\opcinfo` file:
   `SNMP_SESSION_MODE   NO_TRAPD`

   For HTTPS agent nodes, add the following line to the `\Program Files\HP OpenView\bin\OpC\install\opcinfo` file:
   `SNMP_SESSION_MODE   NO_TRAPD`

2. Configure the SNMP Service on an NT4.0 or Win2000 system to send traps to the OVO management server. The community name should be **`public`** (the default community name Data Protector's SNMP traps use). The trap destination must be the IP address or the hostname of the OVO Management Server and the rights of the community must be **`READ CREATE`**.

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

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



SNMP Service Properties (Local Computer)

General | Log On | Recovery | Dependencies | Agent | Traps | Security

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations: smohpu04.bbn.hp.com

SNMP Service Properties (Local Computer)

General | Log On | Recovery | Dependencies | Agent | Traps | Security

☑ Send authentication trap

Accepted community names

Community	Rights
public	READ CREATE

● Accept SNMP packets from any host
○ Accept SNMP packets from these hosts

3. Configure Data Protector to send SNMP traps to the OVO management server system:

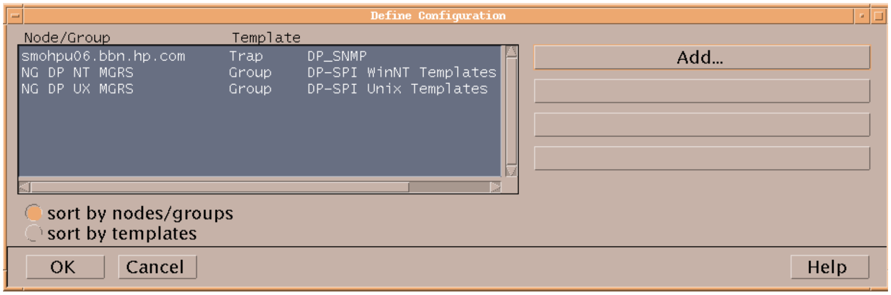
   a. Using the Data Protector GUI’s **Reporting** context window, set up all Notification events to use:

      - SNMP as delivery method
      - OVO management server system as the destination

   b. Add the OVO management server hostname as trap destination to the `OVdests` file in `<Data Protector Root>/Config/SNMP`.

   c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `<Data Protector Root>/Config/SNMP`.

4. Configure the OVO management sever to intercept SNMP traps sent by Windows Cell Manager. To do this, use the OVO GUI to assign and distribute the template “DP_SNMP” to the OVO management server.



Node/Group	Template	
smohpu06.bbn.hp.com	Trap	DP_SNMP
NG DP NT MGRS	Group	DP-SPI WinNT Templates
NG DP UX MGRS	Group	DP-SPI Unix Templates

● sort by nodes/groups
○ sort by templates

Data Protector User Configuration

HP-UX nodes: Check the local root user is in Data Protector’s `admin` user group.

Windows: Add the local `HP ITO account` user 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:

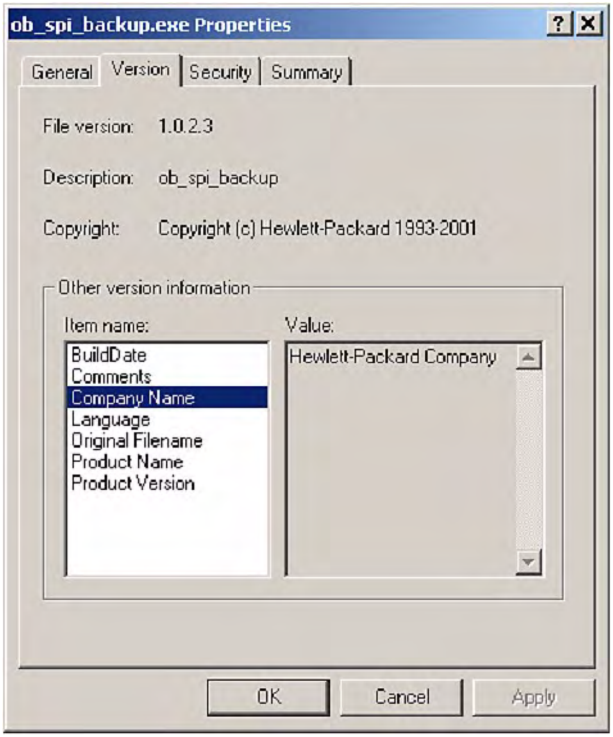
```
HP OpenView Storage Data Protector Integration into
OVO A.06.00 (<build_date>)
```

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

1. Right-click the `ob_spi_backup.exe` file.

2. Select **Properties** from the popup menu.

3. Select the Version tab. The following screen is displayed.



ob_spi_backup.exe Properties

File version: 1.0.2.3

Description: ob_spi_backup

Copyright: Copyright (c) Hewlett-Packard 1993-2001

Other version information

Item name: Company Name

Value: Hewlett-Packard Company

Uninstalling the Data Protector Integration

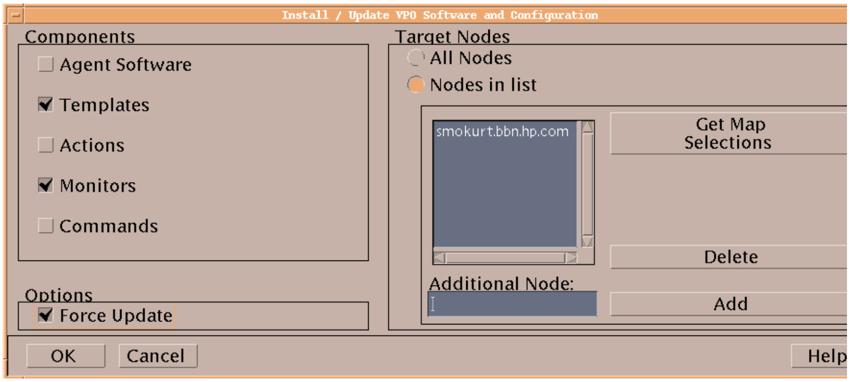
You need to remove components from:

- Managed node systems (Data Protector Cell Manager)
- HP OpenView Operations management server system

Uninstalling from Managed Nodes

1. Unassign the Data Protector Integration’s OVO templates and monitors from the Data Protector Cell Manager system (OVO managed node). To do that, remove the Data Protector Cell Manager from the `DP NT` or `UX MGRS` group.
2. Redistribute the templates to the managed node with the force update option set, to ensure that the templates and monitors do not reside on the managed node anymore.

Figure 2-2 **Redistribute with Force Update Option**



Install / Update VPO Software and Configuration

Components
□ Agent Software
☑ Templates
□ Actions
☑ Monitors
□ Commands

Options
☑ Force Update

Target Nodes
○ All Nodes
● Nodes in list

smokurt.bbn.hp.com

Additional Node:

3. Remove the Data Protector Cell manager from the OVO managed environment using the `Delete Data Protector Cell` application from the `DPSPI_Applications` group.

Uninstalling from the Management Server System

If the OVO management server is using the default Administrator login name and password, uninstall with the command:

```
swremove SPI-DATAPROTECTOR-OVO
```

With a different Administrator login name or a changed password, uninstall as follows:

1. Use the command: `swask SPI-DATAPROTECTOR-OVO`.
2. Enter the OVO management server administrator login name and password.
3. Uninstall: `swremove SPI-DATAPROTECTOR-OVO`

Upgrading the Omniback 4.1 Integration to Data Protector Integration

1. Uninstall the product using `swremove` and remove all Omniback II Integration elements from the OVO database:

   ```
   swremove SPI-OMNIBACK-OVO
   ```

2. Manually remove the GUI elements on the management server in the following order:

   - Users
   - User profiles
   - Message groups
   - Node hierarchies
   - Node groups
   - Application groups
   - Template groups

3. Install the Data Protector Integration:

   ```
   swinstall -s <SD Depot path> SPI-DATAPROTECTOR-OVO
   ```

4. Use the OVO GUI to configure the Integration:

   a. Drag and drop all managed nodes that are Data Protector Cell Managers into the `DP ALL MGRS` group.

   b. Drag and drop all managed nodes that are Data Protector Cell Managers and Windows platforms into the `DP NT MGRS group`.

   c. Drag and drop all managed nodes that are Data Protector Cell Managers and UX platforms into the `DP UX MGRS` group

5. Redistribute the templates and monitors to the managed nodes with the **Force Update** option (see Figure 2-2 on page 38).

3 Integration into HP OpenView Service Navigator

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

- Introduction to HP OpenView Service Navigator
- Using HP OpenView Service Navigator for Data Protector management
- Installation
- Uninstallation

What Is HP OpenView Service Navigator?

HP OpenView Service Navigator is an add-on component of the OVO Java-based operator GUI. Service Navigator lets you map the problems discovered by OVO to the IT services you want to monitor, enabling you to manage the environment by focusing on IT services for which you are responsible.

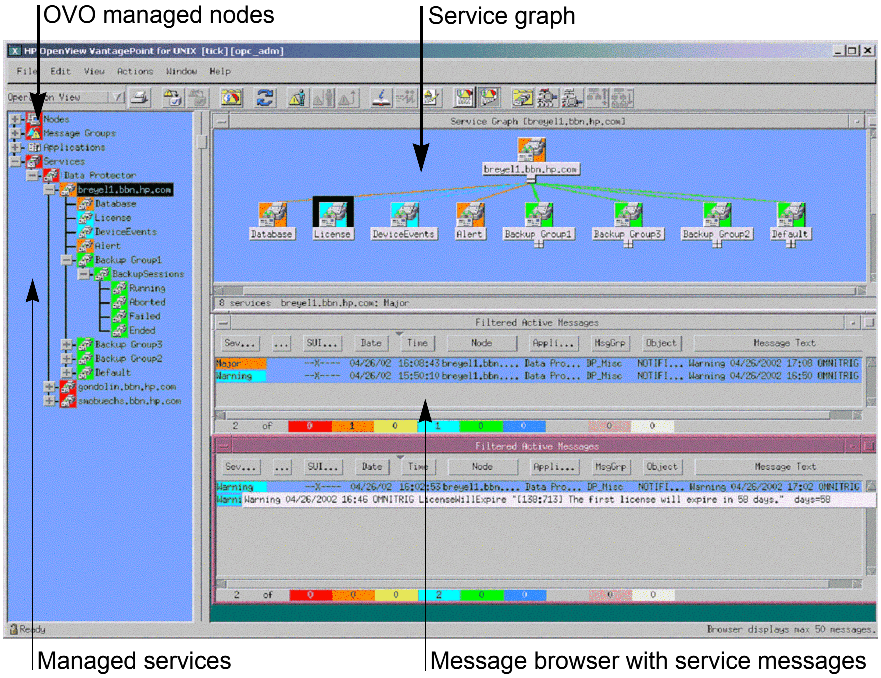
With OVO, if a problem occurs on one of the objects, a message is sent to the user responsible for the area concerned. With Service Navigator, the message is mapped to the service impacted by the problem, and sent to the user responsible for that service.

The severity status of the problem also changes the severity status of the service so you can easily identify services in a problematic state. To solve service-related problems, OVO’s problem resolution capabilities are extended to include service-specific analysis operations and actions.

Optionally, Service Navigator logs each change of status in the database so you can generate reports about service availability.

Figure 3-1 on page 44 shows the Service Navigator main window. In addition to the customary OVO managed nodes and message groups, managed services are displayed in the scoping pane on the left. The content area on the right is split into two sections. The upper section shows the service hierarchy with each service represented by an icon. The lower section contains the standard OVO message browser configured to display only messages relevant to your service.

Figure 3-1 The Service Navigator GUI



```
8 services  breyel1.bbn.hp.com: Major
Major    --X----  04/26/02  16:08:43 breyel1.bbn.... Data Pro... DP_Misc  NOTIFI... Warning 04/26/2002 17:08 OMNITRIG
Warning  --X----  04/26/02  15:50:10 breyel1.bbn.... Data Pro... DP_Misc  NOTIFI... Warning 04/26/2002 16:50 OMNITRIG
2   of   0  1  0  1  0  0   0  0

Warning  --X----  04/26/02  16:02:53 breyel1.bbn.... Data Pro... DP_Misc  NOTIFI... Warning 04/26/2002 17:02 OMNITRIG
Warni Warning 04/26/2002 16:46 OMNITRIG LicenseWillExpire "[138:713] The first license will expire in 58 days."  days=58
2   of   0  0  0  2  0  0   0  0
```

How Does Service Navigator Work?

Service Navigator is based on a service hierarchy, a structure that reflects relationships and dependencies between service-relevant managed objects in your IT environment.

A **service hierarchy** is a logical organization of services you provide; a higher level covers a wider or more general service area than a lower level. There are two kinds of relationship between services in a hierarchy:

- **Containment** — a service is part of, and defined within, another service. The contained service cannot exist without the containing service. A service can contain more than one subservice.
- **Usage** — a service is contained in a service but is also used or referenced, by another service. The used service can exist without the using service; the using service depends on the used service.

For the purposes of status propagation and calculation it is irrelevant whether a service is contained in or used by another service.

NOTE A service can be defined only once but can be used or contained many times.

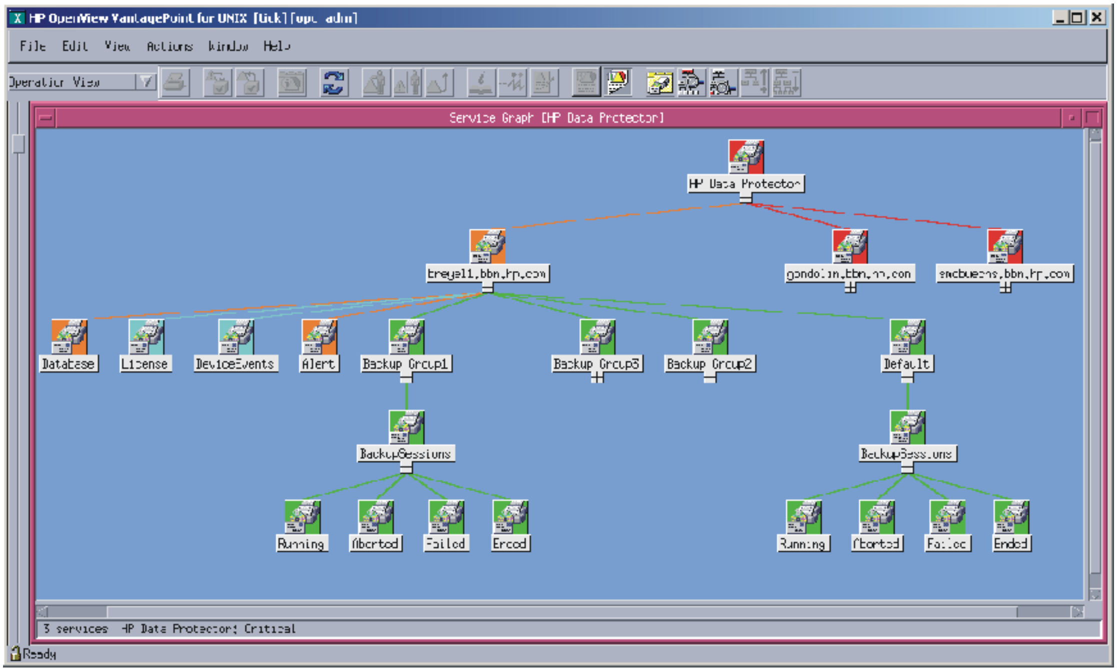
Service Navigator supports up to 256 hierarchical levels.

Figure 3-2 shows an example of a service hierarchy for a Data Protector Cell Manager. The Cell Manager service includes the cell systems and their components:

- Database
- License
- Device Events
- Alert
- Default Backup Group plus any additional Backup Group with Backup Sessions grouped by status

Each of these subservices is divided into further elements.. All relationships are of the containment type.

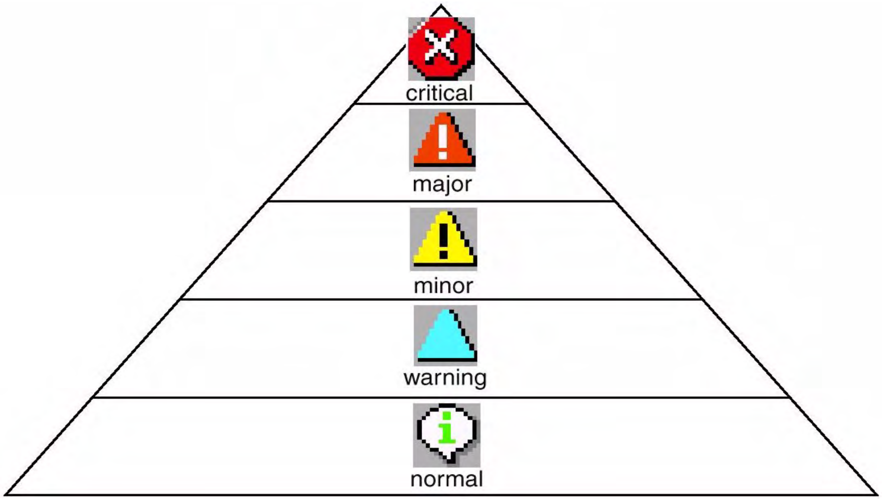
Figure 3-2 Example: Data Protector Service Hierarchy



Because OVO allows one service to use another subservice, you do not need to set up specific subservices for each of your service hierarchies. You can set up a generic service, for example monitoring the operating system on a Data Protector Cell Manager system, that can be used by any other service hierarchy responsible for monitoring a Data Protector Cell Manager system.

OVO Severity Pyramid

The status of a service is the current operational status. Each severity has its own color and icon:



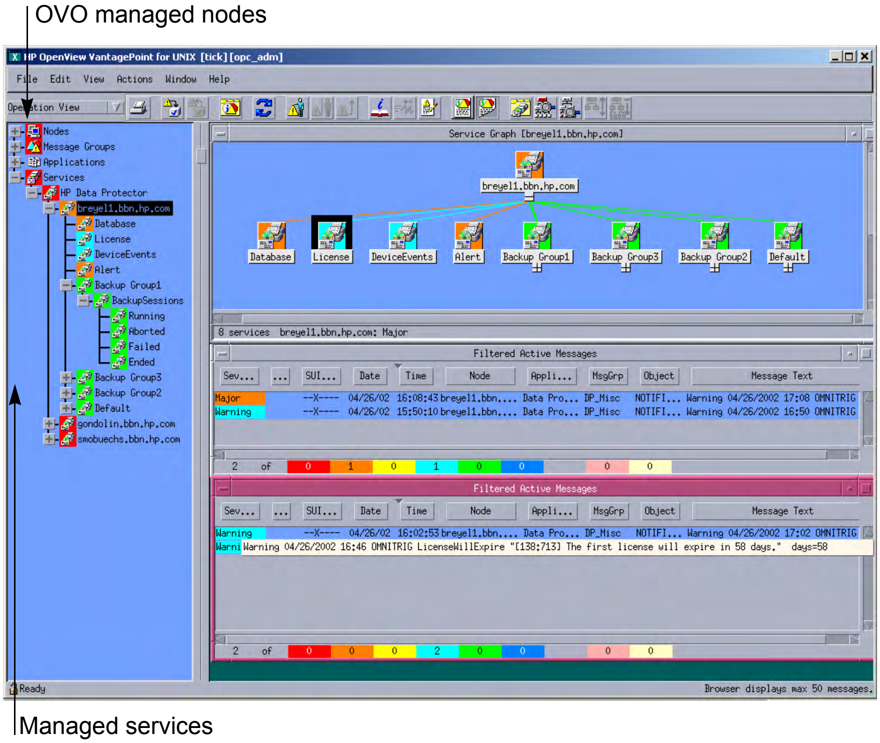
The severity status of the service is determined from the severity status of its subservices according to a set of rules. These are defined in the service configuration file; see the *HP OpenView Service Navigator Concepts and Configuration Guide* for more information.

Data Protector Service Tree

The Data Protector Integration uses Service Navigator to help monitor the status and health of Data Protector cells.

Data Protector is represented as a service in Service Navigator and each Data Protector cell by an icon within that service. The service tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from the Data Protector Integration's monitors. Figure 3-3 illustrates the Data Protector service tree with three Data Protector Cell Managers.

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



```
8 services  breyel1.bbn.hp.com: Major

Filtered Active Messages
Major      --X----  04/26/02  16:08:43 breyel1.bbn....  Data Pro...  DP_Misc  NOTIFI...  Warning 04/26/2002 17:08 OMNITRIG
Warning    --X----  04/26/02  15:50:10 breyel1.bbn....  Data Pro...  DP_Misc  NOTIFI...  Warning 04/26/2002 16:50 OMNITRIG
2  of  0  1  0  1  0  0    0  0

Filtered Active Messages
Warning    --X----  04/26/02  16:02:53 breyel1.bbn....  Data Pro...  DP_Misc  NOTIFI...  Warning 04/26/2002 17:02 OMNITRIG
Warni Warning 04/26/2002 16:46 OMNITRIG LicenseWillExpire "[138:713] The first license will expire in 58 days."  days=58
2  of  0  0  0  2  0  0    0  0
```

The service tree nodes available for each cell are as follows:

Node	Description
<Backup Group>. Backup Sessions	Contains Running, Waiting, Aborted, Failed, Completed, Completed with Failures, and Completed with Errors. Data Protector sends SNMP traps to trigger the update of these items.
Running	Updated by `Start of Session` SNMP trap issued by Data Protector notification.
Waiting	Updated by messages indicating that session is waiting because: • a device is occupied • the database is used • all licenses are currently allocated • too many backup sessions are running in parallel
Aborted	Updated by `Session Aborted` trap.
Failed	Updated by `Session Failed` SNMP trap.
Ended	Updated by `Session Completed`, `Completed with Errors`, or `Completed with Failures` SNMP trap.
Database	Updated by `DB*` SNMP traps issued by Data Protector notification and by messages resulting from database logfile monitoring.
Device Events	Updated by `Device Error-`, `Mount Request-`, `Mail Slots-`, and `Full-` SNMP traps issued by Data Protector notification.
Alert	Updated by `Alarm-`, `Health Check Failed-`, `User Check Failed-`, `Unexpected Events-`, `Not Enough Media-` SNMP traps issued by Data Protector notification.
Licence	Updated by `License` trap.

Applying the Data Protector Service to a User

The Data Protector service tree is assigned to the `opc_adm` and `opc_op` users during installation.

To apply this service to an additional user, use the command:

```
opcservice -assign <username> "Data Protector"
```

Starting the Service Navigator GUI

To start the Service Navigator GUI, run:

```
ito_op
```

and log in with a user name.

Generating the Detailed Service Tree

To generate the detailed service tree for a Data Protector Cell Manager below the Data Protector service:

1. Select the icon of the Data Protector Cell Manager node in the `Node Bank` or in the `Managed Nodes` window.
2. Drag and drop it on the Build Service Tree application in the `Application Bank` window.

Removing the Data Protector Service Tree

When you install the HP OpenView Storage Data Protector Integration, `SPI-DATAPROTECTOR-OVO` is removed and the complete Data Protector service tree is unassigned from all its users and then removed.

You can remove the tree manually by:

```
opcservice -remove -services "Data Protector"
```

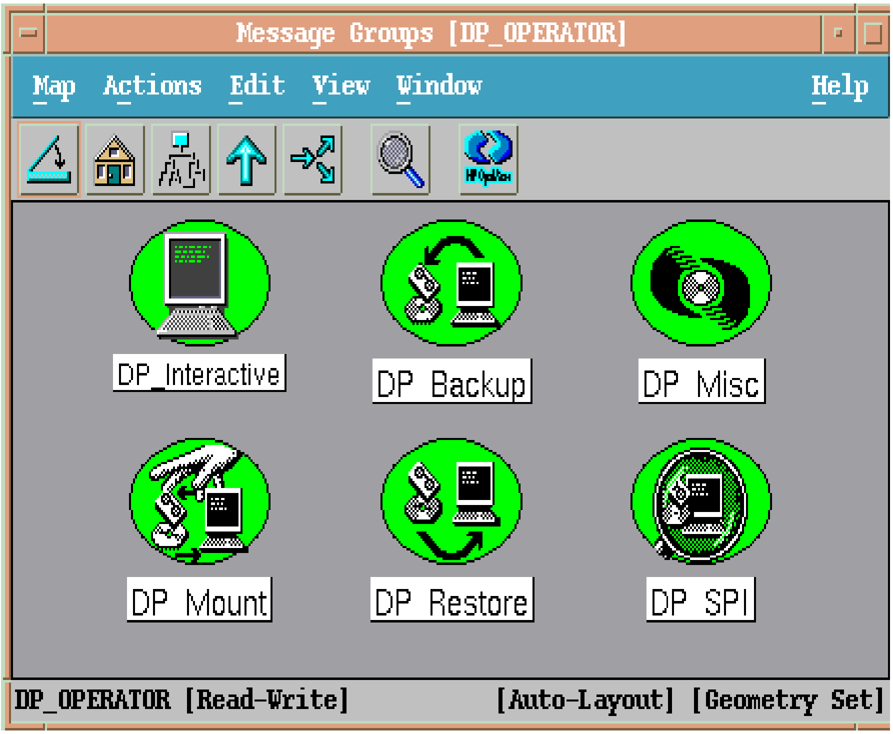
4 Using the Data Protector Integration

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:

- “Message Groups”
- “Node Groups”
- “Application Groups”
- “Using Self-Healing Services”
- “Users and User Profiles”
- “Monitored Objects”
- “Monitored Logfiles”

Message Groups

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



Where appropriate, the Data Protector Integration assigns 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:

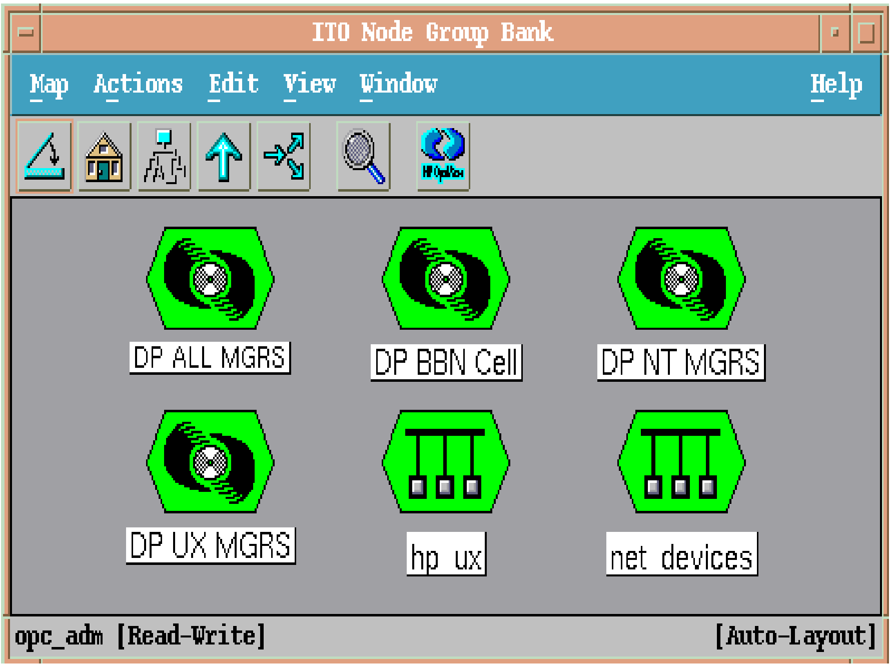
Message Group	The following groups are available, as described above: `DP_Backup`, `DP_Restore`, `DP_Mount`, `DP_Misc`, `DP_SPI`, `DP_Interactive`
Applications	Set to Data Protector.
Node	Set to the hostname of the Data Protector system on which the event occurred.
Severity	Reflection of the impact that 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. Data Protector SNMP traps set the parameter to `NOTIFICATION`. Messages originating from a monitored logfile set this parameter to the name of the logfile. 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 Add Data Protector Cell action adds a node below the DP ALL MGRS node group. This node group is automatically created during installation. The Cell Manager nodes are contained in this node group:

Figure 4-1 **Data Protector Integration Node Groups for opc_adm**

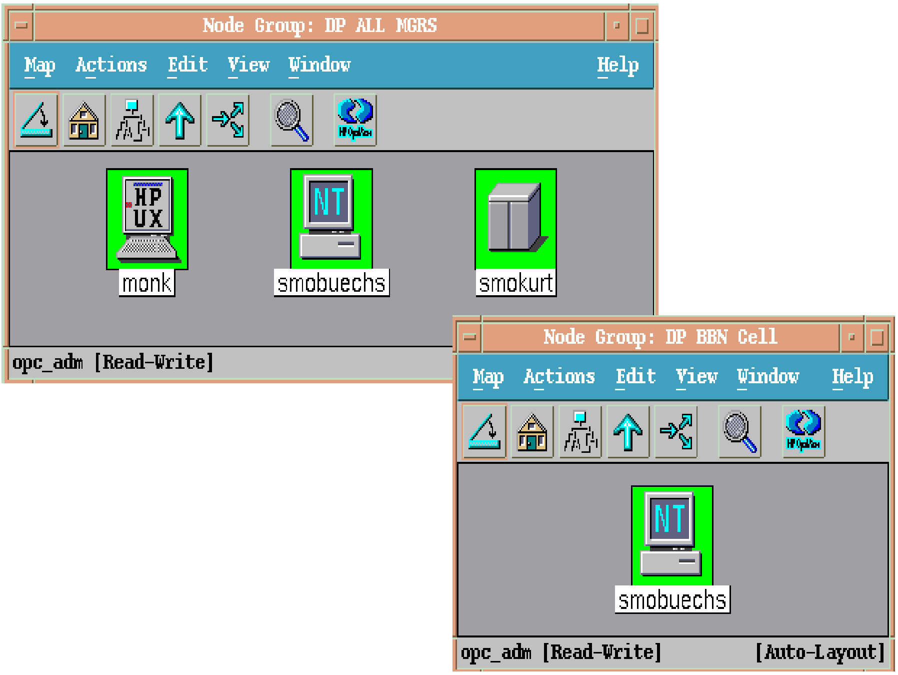


Node groups determine which nodes a user receives messages from. Together with message groups, they define:

- the user's responsibilities
- which messages the user sees in the message browser

The content of DP ALL MGRS Node Group and of the DP BBN Cell Node Group are illustrated in Figure 4-2.

Figure 4-2 **DP ALL MGRS Node Group and DP BBN Cell Node Groups**



The predefined user profiles of the Data Protector Integration use message groups and node groups.

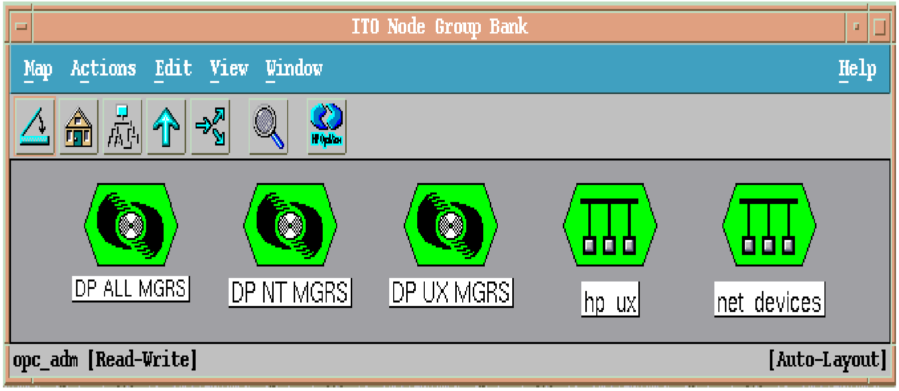
Two further node groups are created during installation of the Data Protector Integration:

- DP NT MGRS
- DP UX MGRS

These can be used by any OVO administrator to help assign and distribute templates 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.

If the cell administrator deletes the node with the `Delete Data Protector Cell` application, it is also automatically deleted from the corresponding node group. The Data Protector Integration node groups are illustrated in Figure 4-3.

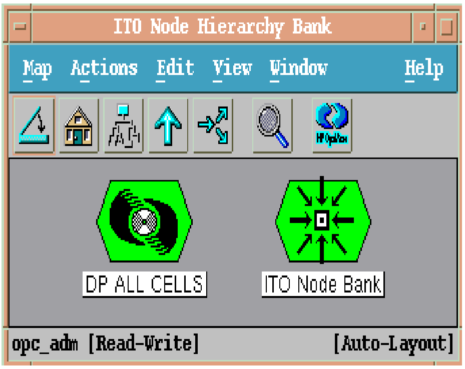
Figure 4-3 **DP Node Groups Created During Installation**



Node Hierarchies

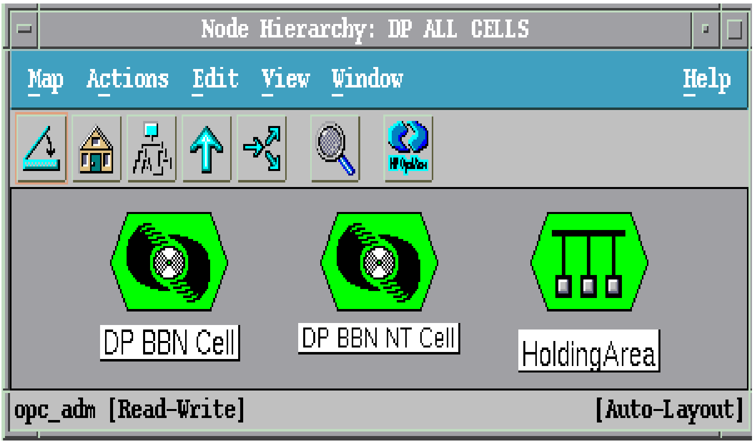
Node hierarchies are used to organize each operator's `Managed Node` window and are directly assigned to OVO users (rather than to profiles). Each hierarchy is represented by an icon in the `Node Hierarchy Bank` window. It represents an organization of nodes and node layout groups.

Figure 4-4 Data Protector Integration Node Hierarchy Bank for opc_adm



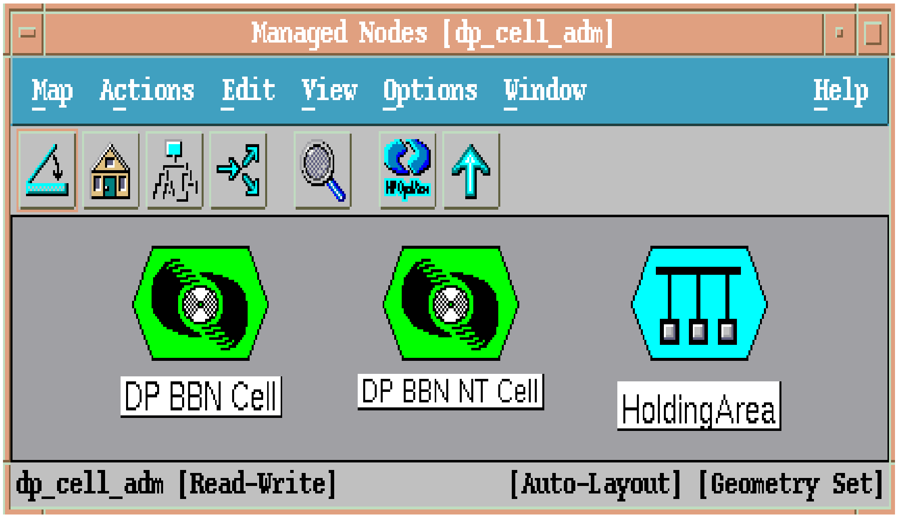
The Add Data Protector Cell action adds a node layout group for a Data Protector cell below the DP ALL CELLS node hierarchy, which is automatically created during installation.

Figure 4-5 **DP ALL CELLS Node Hierarchy Bank**



The content of the Managed Nodes window of the DP_cell_adm user who has been assigned the DP ALL CELLS Node Hierarchy by opc_adm in illustrated in Figure 4-6.

Figure 4-6 **DP_cell_adm User Managed Nodes Window**


Managed Nodes [dp_cell_adm]
Map Actions Edit View Options Window Help
DP BBN Cell
DP BBN NT Cell
HoldingArea
dp_cell_adm [Read-Write]
[Auto-Layout] [Geometry Set]

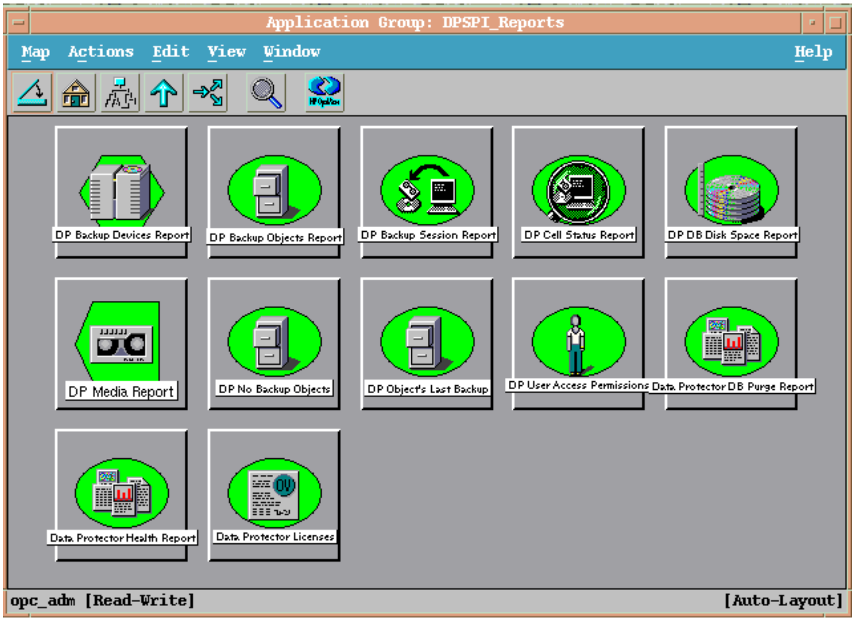
Application Groups

Installing the Data Protector Integration adds a new application group, `Data Protector Integration Applications` to the OVO `Application Bank` window. Each OVO user profile has its own set of Data Protector Integration applications matching the responsibilities of OVO users assigned the profile.

The two new Data Protector Integration application groups are `DPSPI_Reports` and `DPSPI_Applications`.

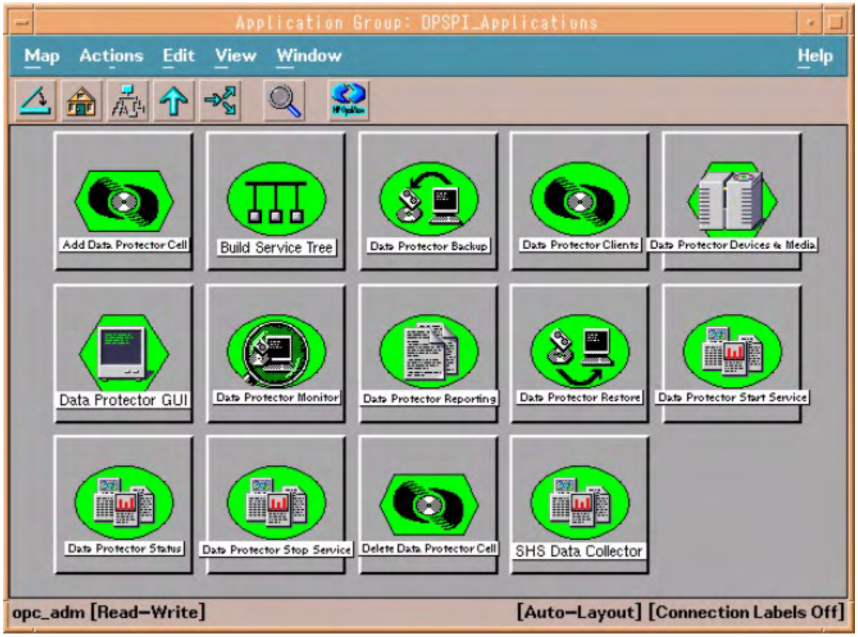
DPSPI_Reports Application Group

`DPSPI_Reports` contains applications for monitoring the health and performance of the Data Protector environment:



DPSPI_Applications Application Group

`DPSPI_Applications` contains applications for managing the Data Protector environment:



NOTE

On HP-UX 11.23 itanium, there is no GUI for Data Protector so the following Data Protector Integration applications will not work:

- Data Protector Backup
- Data Protector Clients
- Data Protector Devices and Media
- Data Protector GUI
- Data Protector Monitor
- Data Protector Restore
- Data Protector Reporting

Using Self-Healing Services

Self-Healing Services can be used in two ways:

- Tools
- Self-Healing Services Client

Tools

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

Using DPSPI SHS Data Collector Self-Healing Services Client

To use DPSPI SHS Data Collector through the Self-Healing Services client, ensure the client is running. After deploying the policies on the managed node, you need to run the following command:

On Windows Managed Node:

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

On UNIX Managed Node:

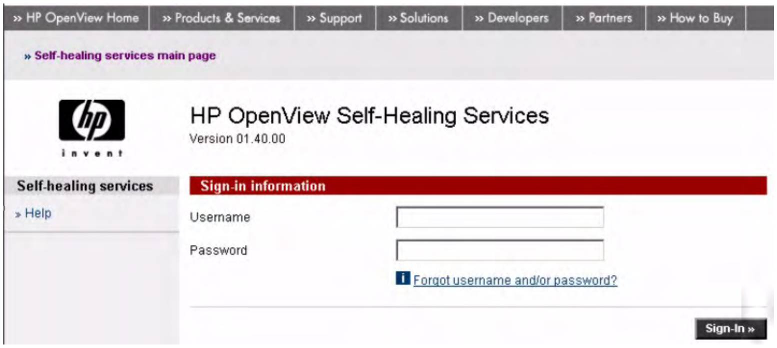
```
/opt/hpsupport/bin/recon.sh
```

To use DPSPI SHS Collector, follow these steps:

1. On a web browser, open the link:

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

The following page opens:



HP OpenView Self-Healing Services
Version 01.40.00

Sign-in information

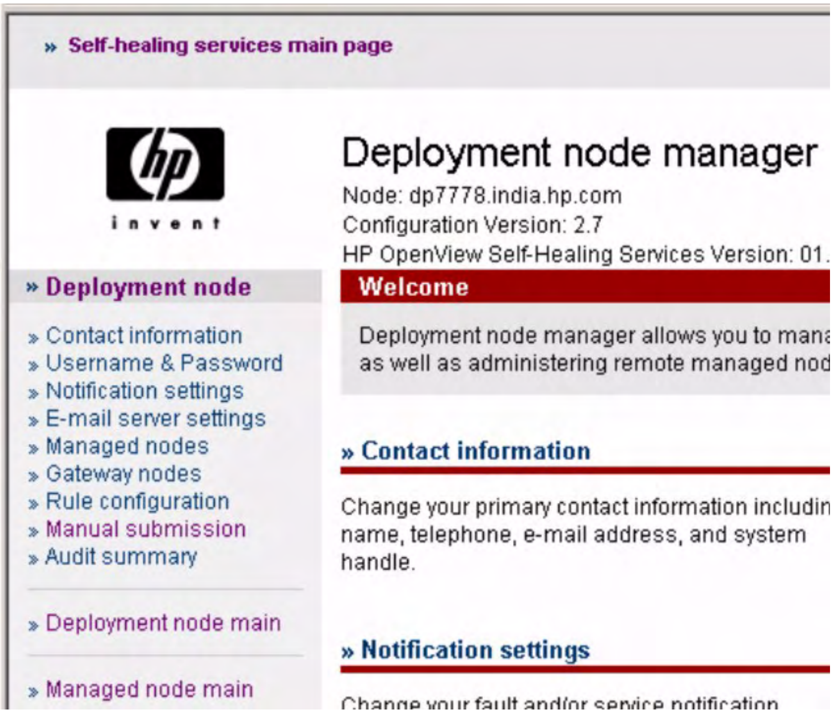
Username

Password

Forgot username and/or password?

2. Log in. The default username is `admin` with password `admin`.

   The Deployment Node Manager is displayed:



Deployment node manager
Node: dp7778.india.hp.com
Configuration Version: 2.7
HP OpenView Self-Healing Services Version: 01.

Welcome

Deployment node manager allows you to mana
as well as administering remote managed nod

» Contact information

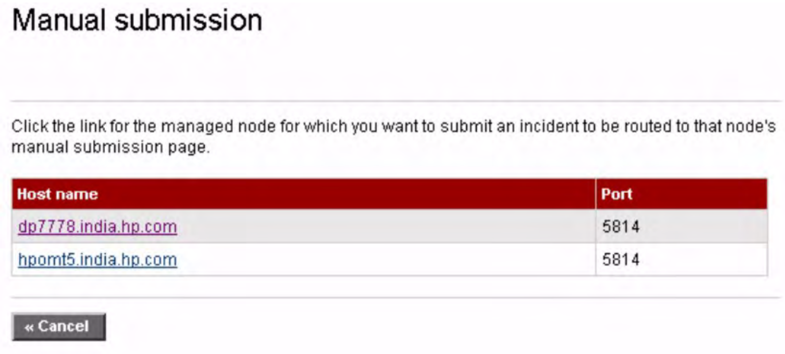
Change your primary contact information includin
name, telephone, e-mail address, and system
handle.

» Notification settings

Change your fault and/or service notification

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

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

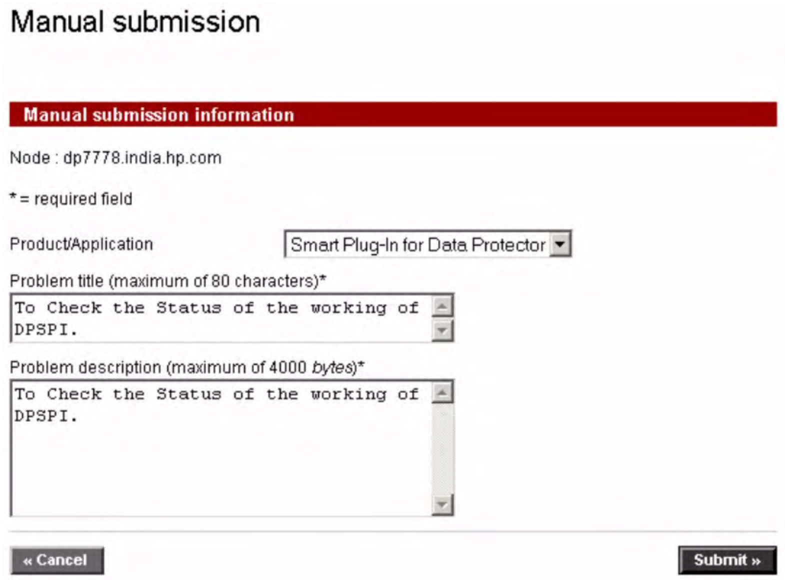


Manual submission

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

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

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



Manual submission

Manual submission information

Node : dp7778.india.hp.com

* = required field

Product/Application: Smart Plug-In for Data Protector

Problem title (maximum of 80 characters)*

```
To Check the Status of the working of
DPSPI.
```

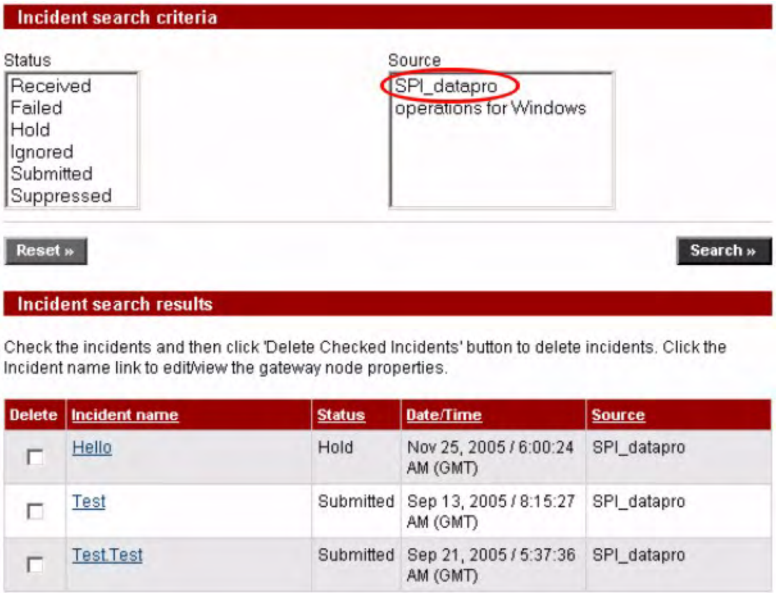
Problem description (maximum of 4000 *bytes*)*

```
To Check the Status of the working of
DPSPI.
```

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

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

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



Incident search criteria

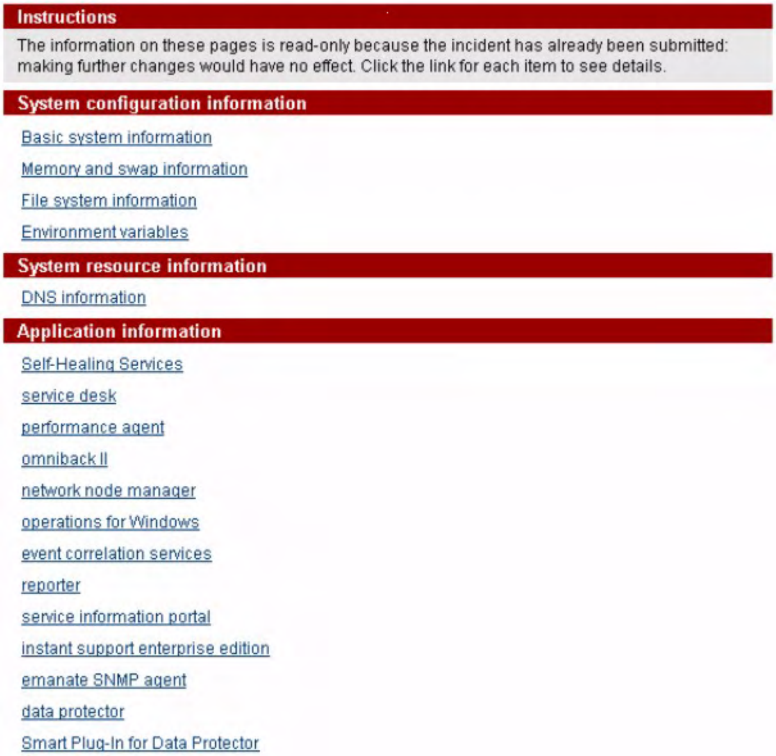
Incident search results

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

Delete	Incident name	Status	Date/Time	Source
□	Hello	Hold	Nov 25, 2005 / 6:00:24 AM (GMT)	SPI_datapro
□	Test	Submitted	Sep 13, 2005 / 8:15:27 AM (GMT)	SPI_datapro
□	Test.Test	Submitted	Sep 21, 2005 / 5:37:36 AM (GMT)	SPI_datapro

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

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



Instructions

The information on these pages is read-only because the incident has already been submitted: making further changes would have no effect. Click the link for each item to see details.

System configuration information

Basic system information
Memory and swap information
File system information
Environment variables

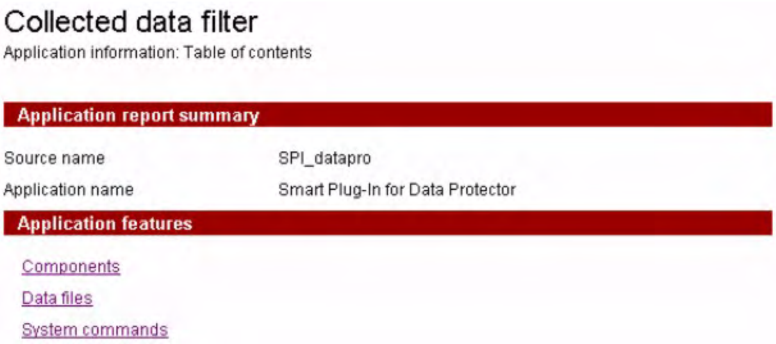
System resource information

DNS information

Application information

Self-Healing Services
service desk
performance agent
omniback II
network node manager
operations for Windows
event correlation services
reporter
service information portal
instant support enterprise edition
emanate SNMP agent
data protector
Smart Plug-In for Data Protector

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



Collected data filter

Application information: Table of contents

Application report summary

Source name	SPI_datapro
Application name	Smart Plug-In for Data Protector

Application features

Components
Data files
System commands

There are three application features:

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

Users and User Profiles

This section describes the types of user in OVO, Data Protector and the Data Protector Integration. It also describes the users and profiles installed by the Data Protector Integration and suggests the most appropriate uses for them.

Data Protector, OVO and Operating System Users

Data Protector and OVO have two types of users:

- **Operating System Users**, required to log in to the operating system. A user requires a valid user login to start Data Protector or log in to 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)`

- **OVO Users**, requiring a login to OVO. Any operating system user can log in as an OVO user if they have the OVO user password.

  Example: `opc_adm` and `opc_op` are the default OVO users.

  The Data Protector Integration generally does not set up any OVO users apart from `obspi_template_admin`. User profiles are provided instead.

Data Protector also uses **user groups** to define access rights for their 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.

For OVO, it does not matter who the operating system user is. The OVO user used to log in to OVO determines which applications are available in the Application Bank window and which message groups and node groups are used for displaying messages in the message browser.

Data Protector Integration Users

Both the operating system user and the OVO user are required by the Data Protector Integration. The OVO user determines the layout of the OVO GUI:

- Applications shown in the Application Bank window
- Data Protector cell managers shown in the Managed Nodes window
- Which message 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 the Application Bank window, the layout of the Data Protector GUI and the permissions this user has in Data Protector are determined by the operating system user used when logging into OVO, not by the OVO user itself.

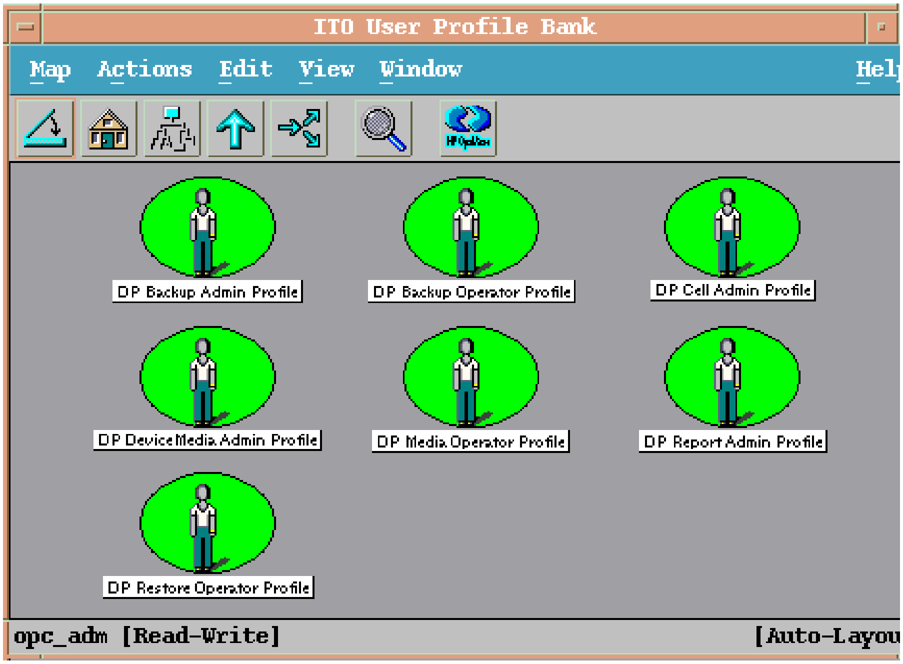
OVO User Profiles

OVO uses **User Profiles** 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 profiles suitable for use with different OVO-Data Protector operator roles. All the OVO administrator needs to do is to assign the appropriate default user profiles and the `DP ALL CELLS` node hierarchy to existing OVO users. He may also copy the default user profiles and modify them as required.

Data Protector OVO User Profiles

During installation, Data Protector Integration adds seven new user profiles to the OVO `User Profile Bank` window— four administrators and three operators:


ITO User Profile Bank
Map Actions Edit View Window Help
DP Backup Admin Profile
DP Backup Operator Profile
DP Cell Admin Profile
DP Device Media Admin Profile
DP Media Operator Profile
DP Report Admin Profile
DP Restore Operator Profile
opc_adm [Read-Write]
[Auto-Layou

The following table lists for each user, applications available through icons on the Application Window and message groups through the OVO Message Browser. Roles for each user are listed in Table 4-2.

Table 4-1 **Data Protector OVO User Profiles**

Admin/Operator Profiles	Description
DP Backup Administrator	Restricted to a Data Protector Cell. *Applications:* Data Protector Backup *Messages:* Enable the OVO message template for detailed messages, `DP_Detailed`.

Table 4-1 Data Protector OVO User Profiles (Continued)

Admin/Operator Profiles	Description
DP Backup Operator	Restricted to a Data Protector Cell. *Applications:* Data Protector Backup *Message Groups:* • `DP_Backup` • `DP_Misc` • `DP_Mount` These are backup session messages and mount requests of backup sessions messages.
DP Restore Operator	Restricted to a Data Protector Cell. *Applications:* Data Protector Restore *Message Groups:* • `DP_Restore` • `DP_Misc` • `DP_Mount` These are restore session messages and mount requests of restore sessions messages.
DP Device & Media Administrator	Restricted to a Data Protector Cell. *Applications:* Data Protector Devices & Media *Messages:* Enable the OVO message template for detailed messages, `DP_Detailed`.
DP Media Operator	Restricted to a Data Protector Cell. *Applications:* • Data Protector Backup • Data Protector Restore *Messages:* Mount requests of backup and restore sessions (`DP_Mount`) messages.

Table 4-1 Data Protector OVO User Profiles (Continued)

Admin/Operator Profiles	Description
DP Cell Administrator	Restricted to clients of Data Protector Cells. *Applications:* • Data Protector Clients • Data Protector Start Service • Data Protector Stop Service • Data Protector Monitor Enterprise (in a MoM cell) • Build Data Protector Service Tree • Add Data Protector Cell • Delete Data Protector Cell *Message Groups:* • `DP_Misc` • `DP_SPI`
DP Report Administrator	Restricted to a Data Protector Cell. *Applications:* Data Protector Reporting *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 4-2 defines the roles a Data Protector OVO Operator might have and describes the appropriate access rights of an equivalent Data Protector user.

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

OVO users are not created by the Data Protector Integration. The roles described in Table 4-2 are examples of possible roles you may create and use to manage Data Protector.

Table 4-2 Data Protector OVO Operators and their Roles

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

Table 4-2 Data Protector OVO Operators and their Roles (Continued)

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

Table 4-2 Data Protector OVO Operators and their Roles (Continued)

Role	DP Privileges	Description
Restore Operator	Starts restore on demand (from which device, what to restore, to which system), monitors the status of the restore session, and responds to mount requests by providing media to devices.	
	Restore to other clients	Allows a user to restore an object to a system other than the one where the object was backed up.
	Restore from other users	Allows a user to restore objects belonging to another user. This is a UNIX specific user right.
	Restore as root	Allows a user to restore objects with the rights of the root UNIX user. Note that this is a powerful right that can affect the security of your system. This user right is required to restore on NetWare clients.
	Start restore	Allows a user to restore own data, to monitor and abort own restore sessions. A user that has this user right is able to view their own and public objects on the Cell Manager.
	Mount request	Allows a user to respond to mount requests for any active session in the cell.
	Monitor	Allows a user to view information about any active session in the cell, and also allows a user to access the Data Protector database to view past sessions. A user with monitor rights can use the Data Protector database context.
Device & Media Administrator	Creates and configures logical devices and assigns media pools to devices, creates and modifies media pools and assigns media to media pools.	
	Device configuration	Allows a user to create, configure, delete, modify and rename devices. This includes the ability to add a mount request script to a logical device.
	Media configuration	Allows a user to manage media pools and the media in the pools, and to work with media in libraries, including ejecting and entering media.

Table 4-2 Data Protector OVO Operators and their Roles (Continued)

Role	DP Privileges	Description
Media Operator	Responds to mount requests by providing media to the devices.	
	Mount request	Allows a user to respond to mount requests for any active session in the cell.
Cell Administrator	Installs and updates Data Protector client systems, adds, deletes, or modifies Data Protector users and groups, and administers the Data Protector database.	
	Client configuration	Allows a user to install and update of client systems.
	User configuration	Allows a user to add, delete and modify users or user groups. *Note:* This is a powerful right.
	Monitor	Allows a user to view information about any active session in the cell, and access the Data Protector database to view past sessions. The user can use the Data Protector database context.
	See private object	Allows a user to see private objects. Database administrators require this right.
Report Administrator	Creates and modifies Data Protector reports.	
	Reporting and notifications	Allows a user to create Data Protector reports. To use Web Reporting, you also need a java user under applet domain in the admin user group.

obusergrp.pl User Groups Tool

The Data Protector Integration provides the `obusergrp.pl` tool to set up user groups in Data Protector for the above user roles. It resides on the OVO management server in the directory:

```
/opt/OV/OpC/integration/obspi/bin
```

It uses the `/opt/OV/OpC/integration/obspi/etc/host_list` file to distribute predefined settings to each cell manager listed in the file.

It uses `ftp.sh` to acquire, modify and replace the `classSpec` file in Data Protector’s configuration directory.

NOTE

No equivalent user groups are configured by default in Data Protector. If such user groups are required, an administrator must set them up directly.

The `host_list` file must be edited directly by the user.

The Data Protector Cell Manager system must have a running FTP service.

Data Protector Template Administrator

The Data Protector Template Administrator user is an OVO user and not a profile. It allows you to create, modify, and delete Data Protector Integration templates and monitors. With the Data Protector Template Administrator, you use configuration tools to set up message collection and monitoring services, and define message filters and suppression criteria. You can also determine how matched and unmatched messages are handled by OVO.

OVO Administrator

The pre-defined OVO administrator, `opc_adm`, is responsible for installing and configuring OVO software and the Data Protector Integration on OVO managed nodes. Data Protector Cell Managers are managed nodes in OVO.

The `Application` window shows additional icons for these applications:

- Add Data Protector Cell
- Delete Data Protector Cell
- Build Data Protector Service Tree

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 min.

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` *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 and also the status of the database.

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 min.

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` ***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 min.

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` *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 min.

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` *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 min.

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` *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

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 min.

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 min.

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 Message Source Templates window of the OVO administrator's GUI.

Four Data Protector logfiles are monitored for warning and error patterns. For basic information, see the *HP OpenView Storage Data Protector Troubleshooting Guide*, or Data Protector online Help index: "log files, Data Protector".

Data Protector Default Logfiles

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

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

omnisv.log

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

```
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) `inet.log` (Waning)
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

This logfile provides security information. The messages document requests to the `inet` process from non-authorized systems. The data/time format depends on 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
```

Data Protector Database Logfile

On Cell Manager systems only, there is a logfile `purge.log`. These systems contain a catalog and media management database.

purge.log

This logfile contains purge session messages. Purge sessions are used to clean up the database. The data/time format depends on the 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 for the default logfiles are:

Message Group	`DP_Misc`
Applications	`Data Protector`
Note	`<name_system>` on which logfile resides
Severity	Purge start/finish messages (Normal) 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 handled
`RDS.log`	Raima Database service messages
`readascii.log`	Messages generated during 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, that is, errors while parsing the backup specification. No message catalog is used. The time/date format depends on the language environment variable.

5 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:

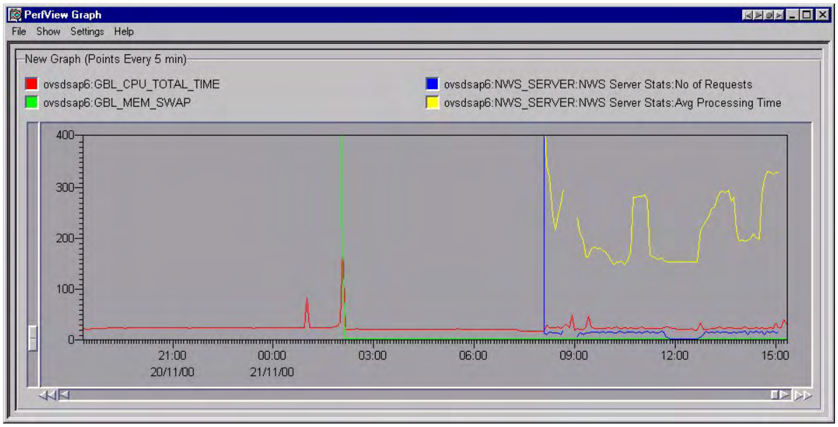
- Storing of Performance data
- Configuration
- Installation
- Uninstallation

Integration Overview

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

The OVPA also collects many metrics from the operating environment, such as I/O, network, and processes, and stores them in logfiles. It also collects the durations of transactions, measured through the ARM interface. Additional sources of performance data can be directed into the OVPA via DSI (Data Source Integration). Collected data can be viewed centrally by the OVP Console to show trends and can also be combined with the internal data or data from other applications to get correlations with, for example, CPU utilization or network data.

Figure 5-1 **HP OpenView Performance Console**


PerfView Graph
File
Show
Settings
Help
New Graph (Points Every 5 min)
🟥 ovsdsap6:GBL_CPU_TOTAL_TIME
🟩 ovsdsap6:GBL_MEM_SWAP
🟦 ovsdsap6:NWS_SERVER:NWS Server Stats:No of Requests
🟨 ovsdsap6:NWS_SERVER:NWS Server Stats:Avg Processing Time
400
300
200
100
0
21:00
20/11/00
00:00
21/11/00
03:00
06:00
09:00
12:00
15:00

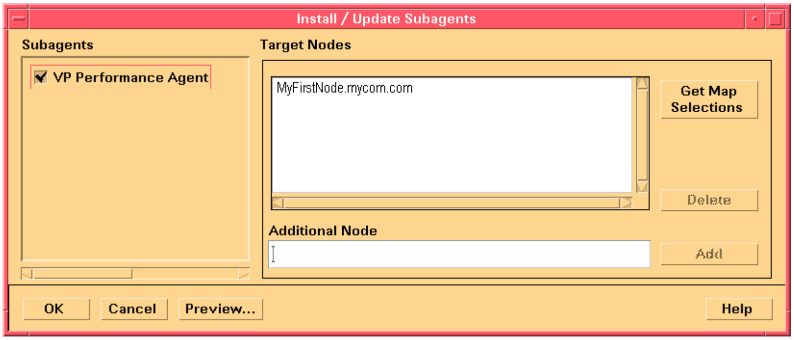
Performance measurement forms the basis for evaluating what corrective actions are needed to optimize performance and resource utilization of the Data Protector environment. Typically, this is an off-line operation where a window of time is selected for detailed analysis of system performance, behavior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

Installing Performance Agent

The OVPA must run on all agent nodes running Data Protector Cell Managers.

To distribute and start the HP OpenView Performance subagent:

Actions → **Subagents** → **Install/Update** → **VP Performance Agent** (activate checkbox) → **OK**



Install / Update Subagents

Subagents

☑ VP Performance Agent

Target Nodes

MyFirstNode.mycom.com

Additional Node

Installing Performance Integration Components

Installation on Window Nodes

When the Data Protector Integration is installed on the OVO management server, the configuration files for the OVPA integration reside in the directory:

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

In this directory, the zip file `obspi_vpp.zip` contains all configuration files for Windows. You need to distribute the OVPA configuration files manually:

1. Transfer the zip file to the managed node using FTP.
2. Install the files in the OVPA directory, ensuring files are extracted to the appropriate directories:
   a. Open `obspi_vpp.zip` with WinZip.
   b. Select the parent directory of the OVPA Installation (usually `C:\`) as the extraction directory.
   c. Ensure the "`Use folder names`" box is checked.
   d. Click the extract button to unzip the files.

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`

Installation Steps for UNIX Nodes

When Data Protector Integration is installed on the OVO management server, the configuration files for the OVPA integration reside in the directory:

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

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

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

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

After decompression, the following files reside in the directory `/opt/OV/OpC/integration/obspi/vpp/`:

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

Collect ARM Transactions

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

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

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

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 which specifies the types of data the OVPA is to log. The entry has the form:
   ```
   log global process application transaction
   dev=disk
   ```
3. Set transaction parameter to: **`transaction=correlator`**

Modifying the ttd.conf File

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

1. Shut down:
   - the HP OpenView Performance Agent service
   - all ARM instrumented applications.

   See the HP OpenView Performance Agent handbook *Tracking your Transactions* for further information.
2. Open the `ttd.conf` file in an editor.
3. Delete the default line:
   `tran=* range=0.5,1,2,3,5,10,30,120,300 slo=5.0`
4. Add the following to collect all Data Protector ARM transactions:

   ```
   [HP OpenView Storage Data Protector]
   tran=BS*
   tran=RS*
   tran=BO*
   tran=DP
   tran=DC
   ```

   The complete syntax for monitoring the Data Protector ARM transactions is in the following files, after installing the Data Protector OVPA integration:

   Windows:
   `<Performance Agent Root>\Data\obspi_ttdconf.mwc`

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

   The following gives an overview of the syntax:

Transaction	Additional Info	Description
`BS-<Backup_specification>`	Time	Duration of a backup session
`RS-<Session_ID>`	Time	Duration of a restore session
`BO-<Object_name>`	Time	Duration of a backup of a specified object
`DP`	# purged records DB size (MB)	Duration of the Data Protector database purge
`DC`	DB size (MB)	Duration of the Data Protector database check

5. *UNIX only:* Replace `/opt/omni/lib/arm/libarm.sl [.so]` with a softlink of the same name to `/opt/perf/lib/libarm.sl [.so]`
6. Restart all ARM instrumented applications and the OVPA services.

After modifying the `ttd.conf` file, you can collect transaction information about the tasks.

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. By modifying the `parm` file, you can use the OVPA to collect process data from these tasks.

The complete syntax for monitoring the Data Protector processes is in the parm files, located in the following directory after installing the Data Protector OVPA integration:

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

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

Modifying the parm File on a Data Protector Media Agent

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

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

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 Disk Agent

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

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

Modifying the parm File on a Data Protector Installation Server

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

```
application Installation_Server
file OmniInet bmsetup
```

Performance Agent Data Source Integration

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

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

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. Use the OVPA command `sdlcomp` to compile the `obdsi.spec` class specification file and 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 obdsi.spec

You must create a logfile set to store collected data in the OVPA database. To do this, compile the class specification file `obdsi.spec` with the OVPA command `stdlcomp`. The files are in the following directory after installing the Data Protector OVPA integration:

Windows: `<Performance Agent Root>\Data\Datafiles`

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

The `sdlcomp` command has the following syntax:

```
sdlcomp specification_file logfile_set
```

`specification_file` The class specification file. Qualify it fully if it is not in the current directory.

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

Unless you specify a path, the set is created in the current directory. You can choose to store logfiles anywhere during compilation, but you must *not* move them after they have been compiled.

Example: Using `sdlcomp` to compile the Data Protector specification file:

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

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

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

Editing the perflbd File

On Unix:

- Stop the mwa services and take a backup of the file `/var/opt/perf/perflbd.rc`
- Edit the file `perfldb.rc` and replace the existing line with the following:

  ```
  DATASOURCE=OMNIBACKII
     LOGFILE=/var/opt/perf/datafiles/omniback
  ```

On Windows:

- Stop the mwa services and take a backup of the file: `C:\Program Files\HP OpenView\Data\perflbd.mwc`
- Edit the file `perfldb.mwc` and replace the existing line with the following:

  ```
  DATASOURCE=OMNIBACKII
     LOGFILE=C:\rpmtools\data\datafiles\omniback
  ```

Collecting Data on Windows Nodes

Installing the Data Protector DSI Log Service

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

After installing 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:

```
Omni_spi_dsi_service.exe -i
```

This registers the service in the Service Control Manager.

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

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

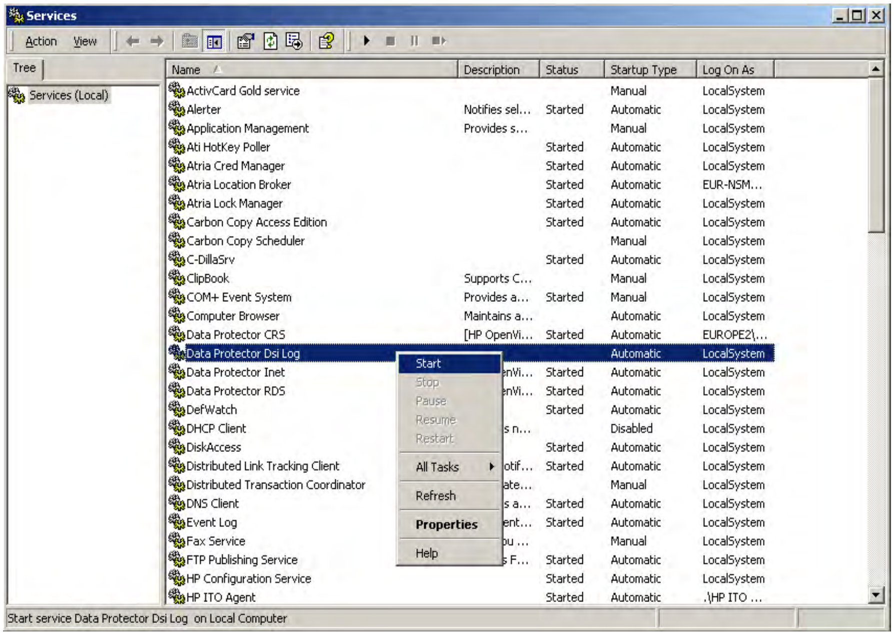
If you find the Data Protector `DSI Log` service listed, the installation was successful.

Starting the Data Protector DSI Log Service

To start collecting data, 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**

Right-click the Data Protector `Dsi Log` service and select the start option in the context menu:



Name	Description	Status	Startup Type	Log On As
ActivCard Gold service			Manual	LocalSystem
Alerter	Notifies sel...	Started	Automatic	LocalSystem
Application Management	Provides s...		Manual	LocalSystem
Ati HotKey Poller		Started	Automatic	LocalSystem
Atria Cred Manager		Started	Automatic	LocalSystem
Atria Location Broker		Started	Automatic	EUR-NSM...
Atria Lock Manager		Started	Automatic	LocalSystem
Carbon Copy Access Edition		Started	Automatic	LocalSystem
Carbon Copy Scheduler			Manual	LocalSystem
C-DillaSrv		Started	Automatic	LocalSystem
ClipBook	Supports C...		Manual	LocalSystem
COM+ Event System	Provides a...	Started	Manual	LocalSystem
Computer Browser	Maintains a...		Automatic	LocalSystem
Data Protector CRS	[HP OpenVi...	Started	Automatic	EUROPE2\...
Data Protector Dsi Log			Automatic	LocalSystem
Data Protector Inet	enVi...	Started	Automatic	LocalSystem
Data Protector RDS	enVi...	Started	Automatic	LocalSystem
DefWatch		Started	Automatic	LocalSystem
DHCP Client	s n...		Disabled	LocalSystem
DiskAccess		Started	Automatic	LocalSystem
Distributed Link Tracking Client	otif...	Started	Automatic	LocalSystem
Distributed Transaction Coordinator	ate...		Manual	LocalSystem
DNS Client	s a...	Started	Automatic	LocalSystem
Event Log	ent...	Started	Automatic	LocalSystem
Fax Service	ou ...		Manual	LocalSystem
FTP Publishing Service	s F...	Started	Automatic	LocalSystem
HP Configuration Service		Started	Automatic	LocalSystem
HP ITO Agent		Started	Automatic	.\HP ITO ...

Start service Data Protector Dsi Log on Local Computer

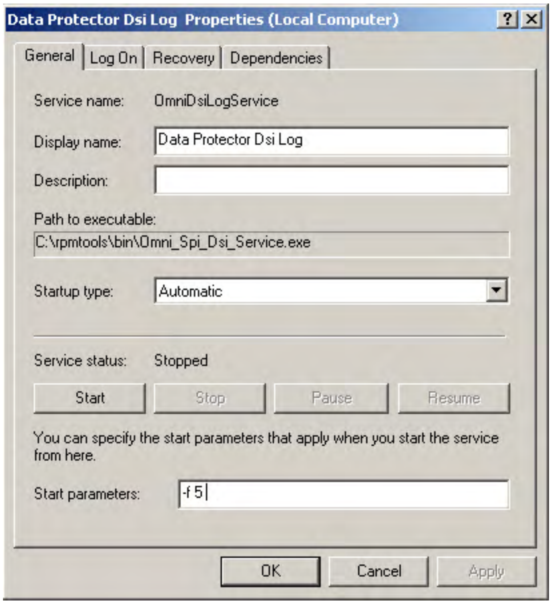
Specifying the Data Collection Frequency

The default data collection frequency is 12 minutes. This is the same time configured in the `obdsi.spec` file used to create the OVPA logfile set. To change the 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 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 `Data Protector Dsi Log` service, select the **General** tab and input the `start parameter -f` minutes in the textbox:



Data Protector Dsi Log Properties (Local Computer)

Service name: OmniDsiLogService

Display name: Data Protector Dsi Log

Description:

Path to executable:
C:\rpmtools\bin\Omni_Spi_Dsi_Service.exe

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters: -f 5

Configuring the Data Protector DSI Log Service

To enable tracing options for the `Data Protector Dsi Log` service, configure the service to provide the path of the trace file and the level of tracing information:

`Omni_Spi_Dsi_Service.exe -t [TracePath]`

`[TracePath]` is the fully qualified path of the trace file's destination directory, and is optional. By default, the `temp` directory from the system environment (usually `C:\Temp`) is used.

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

To specify the type of information that is written to the trace files, configure the trace level for the `Data Protector Dsi Log` service. There are four levels, containing the following information.

Trace Level 1:	Error Information
Trace Level 2:	Function calls (shows call of internal functions)

Trace Level 3: Information about the current service activities.

Trace Level 4: Important internal data to check for correct resources and configuration.

If you use the -t option to enable tracing, the default tracing level is 1. Change the level with the command:

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

where tracelevel must be between 1 and 4.

The Data Protector Dsi Log service uses OmniSpiDsiLogger.exe to collect the data. After installation, this executable resides in:

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

If you have relocated this file, you must specify the new path to the file. Use the command:

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

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

Configuration data is stored in the registry, where it can be modified manually. It is stored under the registry key:

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

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

Uninstalling the Data Protector DSI Log Service

Before you can remove the files Omni_Spi_Dsi_Service.exe and OmniSpiDsiLogger.exe, you must uninstall the registered service:

```
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, 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

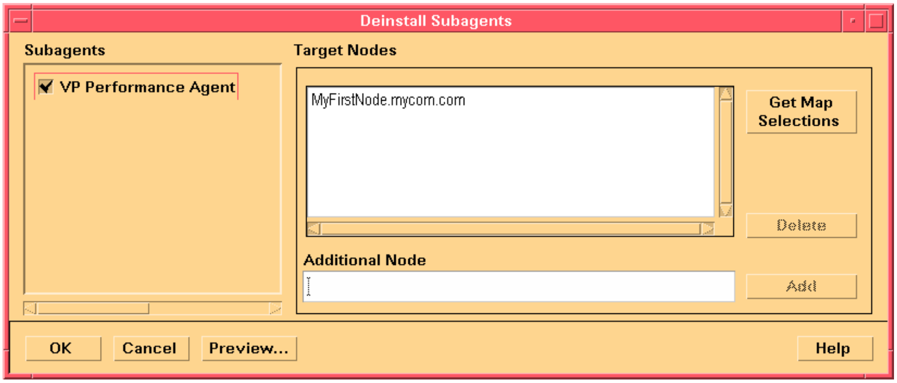
No alarms based on these new metrics are defined, but you can extend the `alarmdef` file to define alarms using these new metrics for the MeasureWare agent.

Uninstalling the Performance Agent

If it is not being used by other solutions, you can uninstall the HP OpenView Performance Agent after uninstalling the Data Protector Integration. To do this:

Delete running HP OpenView Performance subagents as follows:

Actions → **Subagents** → **Deinstall** → **VP Performance Agent** (activate checkbox) → **OK**



☑ VP Performance Agent

MyFirstNode.mycom.com

Index