HP Data Protector 7.00 Integration Guide for HP Operations Manager for UNIX

HP Part Number: n/a
Published: October 2012
Edition: Fourth

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

Contents

Publication history

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

Table 1 Edition history

Part number	Guide edition	Product
N/A	March 2012	Data Protector Release 7.00
N/A	April 2012	Data Protector Release 7.00
N/A	August 2012	Data Protector Release 7.00
N/A	October 2012	Data Protector Release 7.00

About this guide

This guide provides information about how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager for UNIX.

Intended audience

This guide is intended for users of HP Operations Manager for UNIX, with knowledge of:

- HP Data Protector concepts
- HP Operations Manager for UNIX concepts

Documentation set

Other guides and Help provide related information.

Guides

Data Protector guides are available in the electronic PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `English Documentation (Guides, Help)` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the guides reside in the *`Data_Protector_home`*`\docs` directory on Windows and in the `/opt/omni/doc/C` directory on UNIX.

You can find these documents from the Manuals page of the HP support website:

http://support.openview.hp.com/selfsolve/manuals

In the Storage section, click **Storage Software** and then select your product.

- *HP Data Protector Concepts Guide*

  This guide describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented Help.

- *HP Data Protector Installation and Licensing Guide*

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

- *HP Data Protector Troubleshooting Guide*

  This guide describes how to troubleshoot problems you may encounter when using Data Protector.

- *HP Data Protector Disaster Recovery Guide*

  This guide describes how to plan, prepare for, test, and perform a disaster recovery.

- *HP Data Protector Integration Guides*

  These guides describe how to configure and use Data Protector to back up and restore various databases and applications. They are intended for backup administrators or operators. There are six guides:

  - *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server*

    This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server.

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

    This guide describes the integrations of Data Protector with Oracle Server, SAP R/3, and SAP MaxDB.

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

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

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

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

  - *HP Data Protector Integration Guide for Virtualization Environments*

    This guide describes the integrations of Data Protector with virtualization environments: VMware Virtual Infrastructure, VMware vSphere, VMware vCloud Director, Microsoft Hyper-V, and Citrix XenServer.

  - *HP Data Protector Integration Guide for Microsoft Volume Shadow Copy Service*

    This guide describes the integration of Data Protector with the Microsoft Volume Shadow Copy Service. This guide also documents application writer specifics.

- *HP Data Protector Integration Guide for HP Operations Manager for UNIX*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX.

- *HP Data Protector Integration Guide for HP Operations Manager for Windows*

  This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager on Windows.

- *HP Data Protector Zero Downtime Backup Concepts Guide*

  This guide describes Data Protector zero downtime backup and instant recovery concepts and provides background information on how Data Protector works in a zero downtime backup environment. It is intended to be used with the task-oriented *HP Data Protector Zero Downtime Backup Administrator's Guide* and the *HP Data Protector Zero Downtime Backup Integration Guide*.

- *HP Data Protector Zero Downtime Backup Administrator's Guide*

  This guide describes how to configure and use the integration of Data Protector with HP P4000 SAN Solutions, HP P6000 EVA Disk Array Family, HP P9000 XP Disk Array Family, HP P10000 Storage Systems, and EMC Symmetrix Remote Data Facility and TimeFinder. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.

- *HP Data Protector Zero Downtime Backup Integration Guide*

  This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle Server, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases.

- *HP Data Protector Granular Recovery Extension User Guide for Microsoft Exchange Server*

  This guide describes how to configure and use the Granular Recovery Extension for Microsoft Exchange Server 2010 environments. Graphical user interface of the Data Protector Granular Recovery Extension for Microsoft Exchange Server is integrated into the Microsoft Management Console. This guide is intended for Microsoft Exchange Server administrators and Data Protector backup administrators.

- *HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for Microsoft SharePoint Server. The Data Protector Granular Recovery Extension is integrated into Microsoft SharePoint Server Central Administration and enables you to recover individual items. This guide is intended for Microsoft SharePoint Server administrators and Data Protector backup administrators.

- *HP Data Protector Granular Recovery Extension User Guide for VMware vSphere*

  This guide describes how to configure and use the Data Protector Granular Recovery Extension for VMware vSphere. The Data Protector Granular Recovery Extension is integrated into VMware vCenter Server and enables you to recover individual items. This guide is intended for VMware vCenter Server users and Data Protector backup administrators.

- *HP Data Protector Media Operations User Guide*

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

- *HP Data Protector Product Announcements, Software Notes, and References*

  This guide gives a description of new features of HP Data Protector 7.00. It also provides information on installation requirements, required patches, and limitations, as well as known issues and workarounds.

- *HP Data Protector Product Announcements, Software Notes, and References for Integrations to HP Operations Manager*

  This guide fulfills a similar function for the HP Operations Manager integration.

- *HP Data Protector Media Operations Product Announcements, Software Notes, and References*

  This guide fulfills a similar function for Media Operations.

- *HP Data Protector Command Line Interface Reference*

  This guide describes the Data Protector command-line interface, command options, and their usage as well as provides some basic command-line examples.

Help

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

You can access the Help from the top-level directory of any installation DVD-ROM without installing Data Protector:

Windows systems: Open `DP_help.chm`.

UNIX systems: Unpack the zipped tar file `DP_help.tar.gz`, and access the Help system through `DP_help.htm`.

Documentation map

Abbreviations

Abbreviations in the documentation map that follows are explained below. The documentation item titles are all preceded by the words “HP Data Protector”.

Abbreviation	**Documentation item**
CLI	Command Line Interface Reference
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
GRE-Exchange	Granular Recovery Extension User Guide for Microsoft Exchange Server
GRE-SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	Help
IG-IBM	Integration Guide for IBM Applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration Guide for Microsoft Applications: SQL Server, SharePoint Server, and Exchange Server
IG-O/S	Integration Guide for Oracle and SAP
IG-OMU	Integration Guide for HP Operations Manager for UNIX
IG-OMW	Integration Guide for HP Operations Manager for Windows
IG-Var	Integration Guide for Sybase, Network Node Manager, and Network Data Management Protocol Server
IG-VirtEnv	Integration Guide for Virtualization Environments
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	Installation and Licensing Guide
MO-GS	Media Operations Getting Started Guide
MO-PA	Media Operations Product Announcements, Software Notes, and References
MO-UG	Media Operations User Guide
PA	Product Announcements, Software Notes, and References
Trouble	Troubleshooting Guide
ZDB-Admin	ZDB Administrator's Guide
ZDB-Concept	ZDB Concepts Guide
ZDB-IG	ZDB Integration Guide

Map

The following table shows where to find information of different kinds. Shaded squares are a good place to look first.

								Integration Guides								ZDB			GRE			MO			
	Help	GS	Concepts	Install	Trouble	DR	PA	MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	Concept	Admin	IG	Exchange	SPS	VMware	GS	UG	PA	CLI
Backup	X	X	X					X	X	X	X	X	X			X	X	X							
CLI																									X
Concepts/ techniques	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X				
Disaster recovery	X		X			X																			
Installation/ upgrade	X	X		X			X							X	X							X	X		
Instant recovery	X		X													X	X	X							
Licensing	X			X			X																X		
Limitations	X				X		X	X	X	X	X	X	X					X						X	
New features	X						X																	X	
Planning strategy	X		X													X									
Procedures/ tasks	X			X	X	X		X	X	X	X	X	X	X	X		X	X	X	X	X		X		
Recommendations			X				X									X								X	
Requirements				X			X	X	X	X	X	X	X	X	X							X	X	X	
Restore	X	X	X					X	X	X	X	X	X				X	X	X	X	X				
Supported configurations																X									
Troubleshooting	X			X	X			X	X	X	X	X	X	X	X		X	X	X	X	X				

Integrations

Look in these guides for details of the integrations with the following software applications:

Software application	Guides
HP Network Node Manager (NNM)	IG-Var
HP Operations Manager	IG-OMU, IG-OMW
IBM DB2 UDB	IG-IBM
Informix Server	IG-IBM
Lotus Notes/Domino Server	IG-IBM
Media Operations	MO-UG
Microsoft Exchange Server	IG-MS, ZDB IG, GRE-Exchange
Microsoft Hyper-V	IG-VirtEnv
Microsoft SharePoint Server	IG-MS, ZDB-IG, GRE-SPS
Microsoft SQL Server	IG-MS, ZDB-IG
Microsoft Volume Shadow Copy Service (VSS)	IG-VSS
Network Data Management Protocol (NDMP) Server	IG-Var
Oracle Server	IG-O/S, ZDB-IG
SAP MaxDB	IG-O/S
SAP R/3	IG-O/S, ZDB-IG
Sybase Server	IG-Var

Software application	Guides
VMware vCloud Director	IG-VirtEnv
VMware vSphere	IG-VirtEnv, GRE-VMware

Look in these guides for details of the integrations with the following families of disk array systems:

Disk array family	Guides
EMC Symmetrix	all ZDB
HP P4000 SAN Solutions	ZDB-Concept, ZDB-Admin, IG-VSS
HP P6000 EVA Disk Array Family	all ZDB, IG-VSS
HP P9000 XP Disk Array Family	all ZDB, IG-VSS
HP P10000 Storage Systems	ZDB-Concept, ZDB-Admin, IG-VSS

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text: "Document conventions" (page 12)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

General Information

General information about Operations Manager can be found at http://www.hp.com/go/dataprotector

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/software
- http://support.openview.hp.com/selfsolve/manuals
- http://www.hp.com/support/downloads

1 Introduction

This chapter provides an overview of the HP Data Protector Smart Plug-in (SPI) integration, its key features and its architecture.

For descriptions of HP Data Protector and HP Operations Manager, see the *HP Data Protector Concepts Guide* and the *HP Operations Manager 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 Operations Manager and HP Service Navigator.

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 Performance Agent (PA) helps to detect and eliminate bottlenecks in a distributed environment. It also assists system optimization well as service level monitoring.

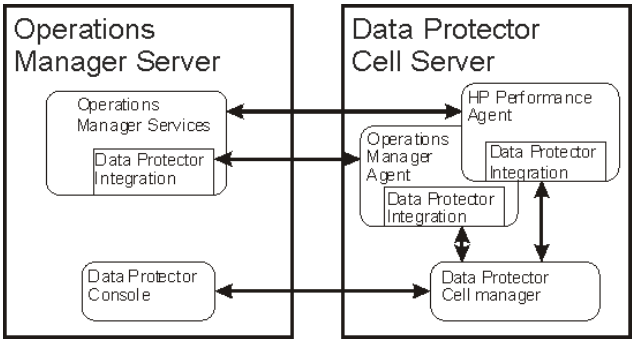
The Data Protector Integration offers the following key features:

- HP Operations Manager agents on a Data Protector Cell Manager system monitor the health and performance of Data Protector.
- A single HP Operations Manager Server can monitor multiple Data Protector Cell Managers.
- The integration also integrates into HP Service Navigator to depict the functionality of Data Protector as a service tree.
- Messages sent to the Operations Manager Server are channeled according to users-profiles. Operations Manager users see only messages they need.
- The Data Protector Cell Manager and the Operations Manager Server should be installed on different systems.
- You can run Data Protector functionality from the **Operations Manager Application Bank** window.
- Data Protector Integration messages sent to the Operations Manager Server include instructions that help you correct the problem.

The main benefits of the integration are:

- Centralized problem management using Operations Manager 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


Operations Manager Server
Operations Manager Services
Data Protector Integration
Data Protector Console
Data Protector Cell Server
HP Performance Agent
Data Protector Integration
Operations Manager Agent
Data Protector Integration
Data Protector Cell manager

The Data Protector Integration is installed on the Operations Manager Server system and is deployed to implement its Operations Manager Agent on the Data Protector Cell Manager system, which is an Operations Manager Managed Node. The Data Protector Cell Manager system must have the Operations ManagerAgent and should have the HP Performance Agent (PA) installed. The Data Protector Console must be installed on the Operations Manager Server, so the Operations Manager user can start the Data Protector GUI as an Operations Manager application and connect to any available Data Protector Cell Manager. Both Windows and UNIX Data Protector Cell Managers are accessible from the same Operations Manager Application Bank. This is facilitated by the Data Protector Console using Data Protector's communication protocol on port 5555 to exchange data.

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

- Data Protector vital Cell Manager processes
- Data Protector logfiles
- Data Protector events through SNMP traps

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

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 HP Operations Manager Server system.
- Installing Data Protector Integration components on Operations Manager Managed Node (Data Protector Cell Manager) system.
- Uninstalling Data Protector Integration components from the HP Operations Manager Server system.
- Uninstalling the Data Protector Integration from the system where the HP Operations Manager Server software is installed.

Supported platforms and installation prerequisites

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

- One or more systems running Operations Manager Server
- Operations Manager 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 a range of HP Data Protector versions:

Table 3 HP Operations Manager – HP Data Protector compatibility

HP Operations Manager for UNIX version	HP Data Protector Versions
9.0 (with patches, if available)	6.20, 7.00 On all Data Protector Cell Manager platforms for which the Operations Manager application agent is available
8.1 (with patches, if available)	A.06.10, A.06.11 On all Data Protector Cell Manager platforms for which the Operations Manager application agent is available

Operations Manager Server system

HP Operations Manager Servers are supported on the following platforms. The Operations Manager Server can run on a different host system from the system on which the Data Protector Cell Manager is installed.

HP Operations Manager is installed and configured on a system running one of the following operating systems. For details, please consult the associated product documents and product web-page.

Table 4 Operations Manager Server supported versions

Application	Supported versions
Operations Manager UNIX	*English and Japanese:* Operations Manager/UNIX 8.x including Service Navigator 8.x is supported on HP-UX 11.11, 11.23 IA PA, 11.31 IA PA, Solaris 8, Solaris 9, Solaris 10

Operations Manager patches

Ensure that up-to-date patches are installed on the OMU/OML Server and required OM Agent patches have been deployed from the server to the managed node system.

Software prerequisites on the Operations Manager Server

Ensure the following software is installed on the Operations Manager Server system:

- HP Operations Manager for UNIX. The console is installed and configured on the HP Operations Manager Server system or other appropriate systems.
- The HP Data Protector console is installed on the HP Operations Manager Server system.

  The `swlist DATA-PROTECTOR` command returns:

  ```
  DATA-PROTECTOR A.06.20

  DATA-PROTECTOR.OMNI-CC A.06.20

  DATA-PROTECTOR.OMNI-CORE A.06.20
  ```

Managed node systems (Data Protector Cell Manager)

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

- HP Operations Manager Agent

NOTE: The Operations Manager patches must be installed on the OM Server and distributed to the OM Agent node systems by the OM administrator before the Data Protector Integration is distributed.

Supported Operations Manager Agent versions

Ensure the Data Protector Cell Manager system runs on a platform for which the Operations Manager Agent is available. Please check the associated OM product documentation.

Additional software for HP-UX managed nodes (Data Protector Cell Manager)

The following software is required, but is not installed as part of the Operations Manager 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 and to let the Operations Manager Agent, which runs on the same system, forward any matching SNMP trap events as OpC messages to the Operations Manager Server. This is called *Distributed Event Interception*, since the SNMP traps are intercepted on the managed node and filtered and forwarded to the Operations Manager Server by the Operations Agent.

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. The messages are sent by the Operations Manager agent to the Operations Manager Server using either HTTPS or DCE/RPCs.

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

Additional software for Windows managed nodes (Data Protector Cell Manager)

The following required and optional software is not installed as part of the Operations Manager Server installation nor as part of the Data Protector Integration installation.

SNMP service (required)

To send Data Protector SNMP traps to the Operations Manager Server you must install the Windows SNMP service.

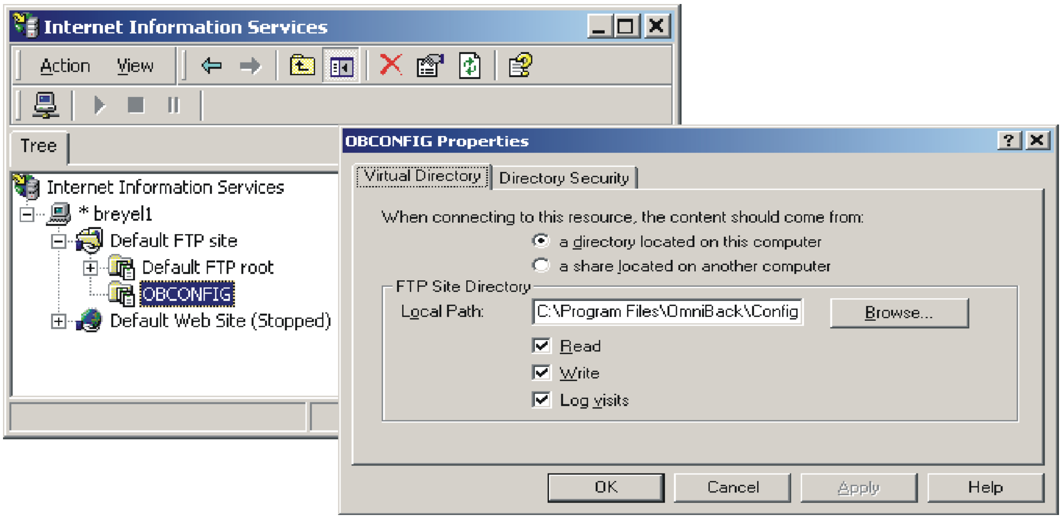
FTP service (optional)

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 Operations Manager Agent from the UNIX Operations Manager Server to a Windows system.

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

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 Information Service (IIS) Windows Component on Windows. Configure the directory *system_drive*`\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 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

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 Operations Manager 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 Operations Manager Server and the managed node.

Machine	Operations Manager version	Operating system	Total
Operations Manager Server	8.x	HP-UX 11.11, 11.23 IA PA, 11.31 IA PA. Solaris 8,9,10	15 MB
Operations Manager Server	9.x	HP-UX 11.31 IA-64 RedHat Enterprise Linux 5.2, 5.3 x64 Solaris 10 Sparc	15 MB
Operations Manager Managed Node	8.x, 9.x	HP-UX, Solaris, Linux, Windows supported as managed node and DP Cell Manager	2 MB

Memory (RAM) requirements

There are no specific requirements for RAM on the Operations Manager Server or Managed Nodes, beyond the requirements of Operations Manager 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 Operations Manager 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 Operations Manager administrator to the managed nodes using Operations Manager.

Limitations

Data Protector cluster installations are not supported.

Upgrading the DP SPI

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

Installation

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

- Monitoring and administration programs
- Operations Manager 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-OM
```

The following filesets are installed on an Operations Manager Server on UNIX systems:

`SPI-DP-AGT-HP`	Operations Manager agent files for the DP Cell Manager on HP-UX
`SPI-DP-AGT-NT`	Operations Manager agent files for the DP Cell Manager on Windows

`SPI-DP-AGT-SOL`	Operations Manager agent files for the DP Cell Manager on Solaris
`SPI-DP-CONF`	Operations Manager templates and configuration files for the Operations Manager Server
`SPI-DP-DOC`	Data Protector Integration's documentation in PDF format

The following fileset is installed on an Operations Manager Server on HP-UX systems:

`SPI-DP-SRV-HP`	Data Protector Integration's executables and scripts for the Operations Manager Server on HP-UX

The following fileset is installed on an Operations Manager Server on Solaris systems:

`SPI-DP-SRV-SOL`	Data Protector Integration's executables and scripts for the Operations Manager Server on Solaris

The following directories are created on the Operations Manager 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/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`	Operations Manager 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

To install software on the management server 9.x version, execute the following command on the server:

On HP-UX systems:

```
# swinstall -s depot_location DPSPI
```

The following filesets are installed on an Operations Manager Server 9.x on HP-UX systems:

`HPOVSPIDP`	Data Protector Integration's executables and scripts for the Operations Manager Server on HP-UX
	Operations Manager templates and configuration files for the Operations Manager Server
	Data Protector Integration's documentation in PDF format

On Solaris systems:

```
# pkgadd -d depot_location HPOvSpiDp
```

The following filesets are installed on an Operations Manager Server 9.x on Solaris systems:

`HPOvSpiDp`	Data Protector Integration's executables and scripts for the Operations Manager Server on HP-UX
	Operations Manager templates and configuration files for the Operations Manager Server
	Data Protector Integration's documentation in PDF format

On Linux systems:

```
# rpm –ivh depot_location
```

The following filesets are installed on an Operations Manager Server 9.x on Linux systems:

HPOvSpiDp	Data Protector Integration's executables and scripts for the Operations Manager Server on HP-UX Operations Manager templates and configuration files for the Operations Manager Server Data Protector Integration's documentation in PDF format

The following directories are created on the Operations Manager Server system 9.x:

/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/doc	Documentation
/var/opt/OV/log/obspi	Logfiles
/var/opt/OV/share/tmp/OpC_appl/DPSPI	Operations Manager files in uploadable format

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:

If the server is OMU 8.x:

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

If the server is OMU/OML 9.x:

In /var/opt/OV/bin/instrumentation/:

- ob_spi_proc.pl
- obspi.conf
- ob_spi_backup.pl
- ob_spi_db.pl
- ob_spi_file.pl
- ob_spi_poolsize.pl
- ob_spi_poolstatus.pl
- ob_spi_medialog.pl
- ob_spi_omnisvlog.pl
- ob_spi_purgelog.pl

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 *`OM_AGENT_INSTALLED_PACKAGE_DIR`* should be in:

For Windows HTTPS platform agent: *`OM_data_dir`*`\bin\instrumentation`

For Windows DCE platform agent: *`OM_install_dir`*`\Installed Packages\{790C06B4-844E-11D2-972B-080009Ef8C2A}\bin\Instrumentation`

If the server is OMU 8.x:

In *`OM_AGENT_INSTALLED_PACKAGE_DIR`*:

- `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`
- `DPPath.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`

If the server is OMU/OML 9.x:

In *`OM_AGENT_INSTALLED_PACKAGE_DIR`*:

- `obspi.conf`
- `ob_spi_backup.pl`
- `ob_spi_db.pl`
- `ob_spi_file.pl`
- `ob_spi_poolsize.pl`
- `ob_spi_poolstatus.pl`
- `ob_spi_proc.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 on Operations Manager 8.x

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-OM
```

You should get the following response.

```
# SPI-DATAPROTECTOR-OM SPI-DATAPROTECTOR-OM
```

HP Data Protector Integration into Operations Manager

```
SPI-DATAPROTECTOR-OM.SPI-DP-AGT-HP A.06.20 Configured
```

Data Protector Integration's files for the DP Cell Manager on HP-UX 11.x

```
SPI-DATAPROTECTOR-OM.SPI-DP-AGT-NT A.06.20 Configured
```

Data Protector Integration's files for the DP Cell Manager on Windows

```
SPI-DATAPROTECTOR-OM.SPI-DP-AGT-SOL A.06.20 Configured
```

Data Protector Integration's files for the DP Cell Manager on Solaris 7, 8, 9 and 10

```
SPI-DATAPROTECTOR-OM.SPI-DP-CONF     A.06.20 Configured
```

Data Protector Integration's templates for the Mgmt. Server

```
SPI-DATAPROTECTOR-OM.SPI-DP-DOC       A.06.20 Configured
```

Data Protector Integration's documentation

On HP-UX Operations Manager Server:

```
SPI-DATAPROTECTOR-OM.SPI-DP-SRV-HP A.06.20 Configured
```

Data Protector Integration's executables and scripts for the Management Server

On Solaris Operations Manager Server:

```
SPI-DATAPROTECTOR-OM.SPI-DP-SRV-SOL A.06.20 Configured
```

Data Protector Integration's executables and scripts for the Management Server

Installation verification on Operations Manager 9.x

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 on HP-UX, enter the following:

```
# swlist -a revision -a state -a title -l fileset

  DPSPI
```

You should get the following response:

```
# DPSPI 6.20.000 HP Operations SPI for DataProtector
  DPSPI.HPOVSPIDP 6.20.000  HP Operations Smart Plug-in for HP Data Protector configured
```

To check the Software Distributor installation on Linux, enter the following:

```
# rpm -qa HPOvSpiDp
```

You should get the following response:

```
HPOvSpiDp-6.20.000-1
```

To check the Software Distributor installation on Solaris, enter the following:

`#pkginfo HPOvSpiDp  application HPOvSpiDp` HP Operations Smart Plug-in for HP Data Protector

Agent installation

Distribute agent software to managed nodes in three stages:

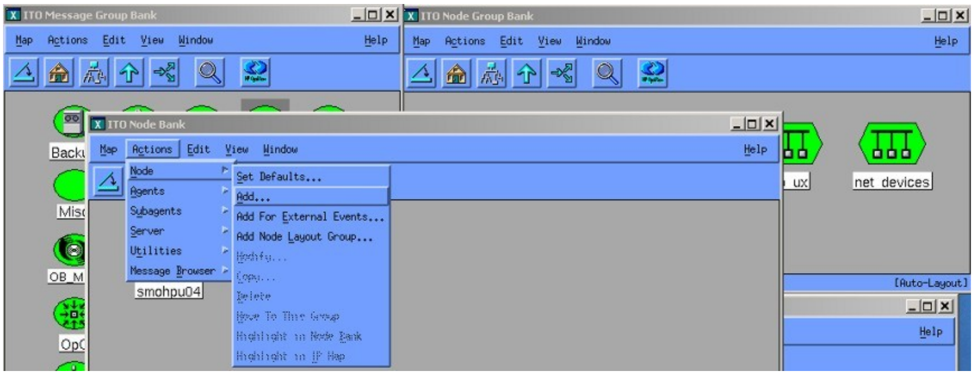
1. Add the Data Protector Cell Manager host system to the Operations Manager managed environment as a managed node.
2. Run the `Add Data Protector Cell` application for each Data Protector Cell Manager node.
3. Distribute software, actions, commands, monitors and templates to the Data Protector Cell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

Adding the Data Protector Cell Manager system as an Operations Manager node

On OMU 8.x:

To add the DP Cell Manager host system to the Operations Manager managed environment as a managed node:

1. Log in to Operations Manager as user `opc_adm`.
2. Open the `Node Bank`.
3. Select **Actions > Node > Add...**

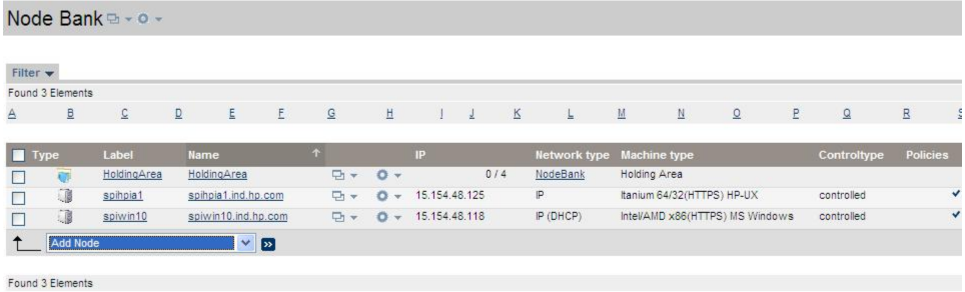


4. Add the label and hostname of the new node in the **Add Node** window.

On OMU/OML 9.x:

To add the DP Cell Manager host system to the Operations Manager managed environment as a managed node:

1. Log in to Operations Manager Admin UI as user `opc_adm`.
2. Open the **Node Bank**:
3. Select **Add Node**.



Node Bank

Filter

Found 3 Elements

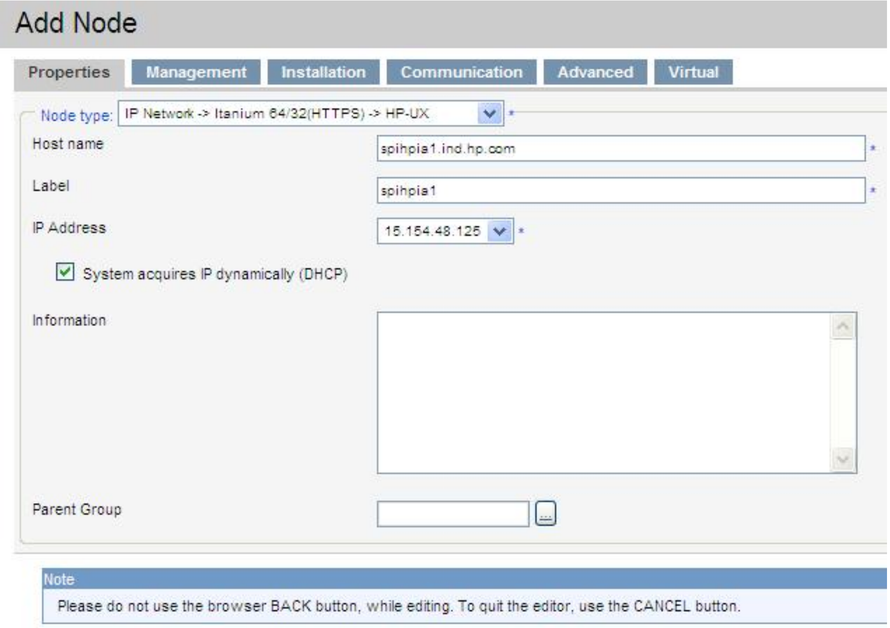
A B C D E F G H I J K L M N O P Q R S

☐	Type	Label	Name		IP	Network type	Machine type	Controltype	Policies
☐		HoldingArea	HoldingArea		0 / 4	NodeBank	Holding Area		
☐		spihpia1	spihpia1.ind.hp.com		15.154.48.125	IP	Itanium 64/32(HTTPS) HP-UX	controlled	✓
☐		spiwin10	spiwin10.ind.hp.com		15.154.48.118	IP (DHCP)	Intel/AMD x86(HTTPS) MS Windows	controlled	✓

Add Node »

Found 3 Elements

4. In the **Add Node** window select the **Node Type** and then enter the label and hostname of the new node.



Add Node

Node type: IP Network -> Itanium 64/32(HTTPS) -> HP-UX *

Host name: spihpia1.ind.hp.com *

Label: spihpia1 *

IP Address: 15.154.48.125 *

☑ System acquires IP dynamically (DHCP)

Information:

Parent Group:

Note

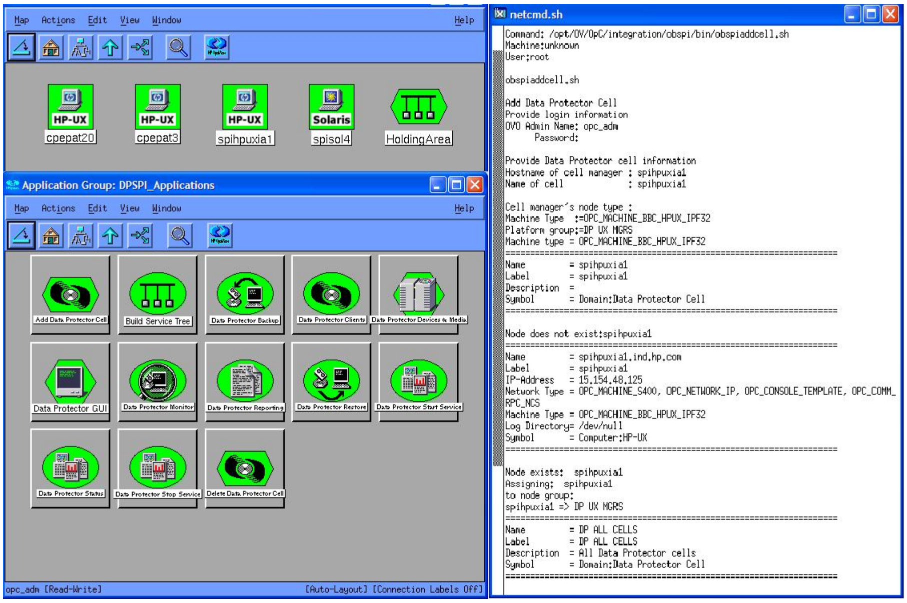
Please do not use the browser BACK button, while editing. To quit the editor, use the CANCEL button.

Running the Add Data Protector Cell application

On OMU 8.x:

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:

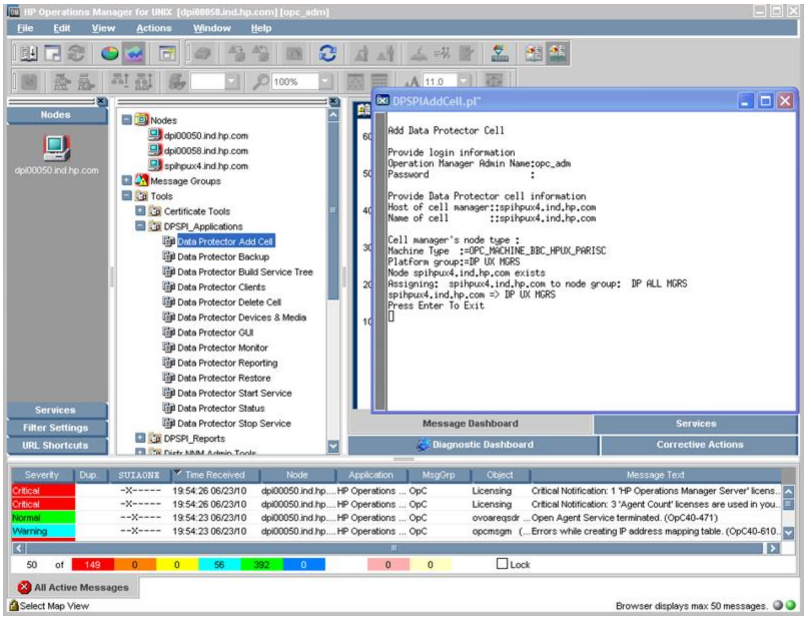


```
Command: /opt/OV/OpC/integration/obspi/bin/obspiaddcell.sh
Machine:unknown
User:root

obspiaddcell.sh

Add Data Protector Cell
Provide login information
OVO Admin Name: opc_adm
      Password:

Provide Data Protector cell information
Hostname of cell manager : spihpuxia1
Name of cell             : spihpuxia1

Cell manager's node type :
Machine Type  :=OPC_MACHINE_BBC_HPUX_IPF32
Platform group:=DP UX MGRS
Machine type = OPC_MACHINE_BBC_HPUX_IPF32
=====================================================================
Name         = spihpuxia1
Label        = spihpuxia1
Description  =
Symbol       = Domain:Data Protector Cell
=====================================================================

Node does not exist:spihpuxia1
=====================================================================
Name         = spihpuxia1.ind.hp.com
Label        = spihpuxia1
IP-Address   = 15.154.48.125
Network Type = OPC_MACHINE_S400, OPC_NETWORK_IP, OPC_CONSOLE_TEMPLATE, OPC_COMM_
RPC_NCS
Machine Type = OPC_MACHINE_BBC_HPUX_IPF32
Log Directory= /dev/null
Symbol       = Computer:HP-UX
=====================================================================

Node exists:  spihpuxia1
Assigning:  spihpuxia1
to node group:
spihpuxia1 => DP UX MGRS
=====================================================================
Name         = DP ALL CELLS
Label        = DP ALL CELLS
Description  = All Data Protector cells
Symbol       = Domain:Data Protector Cell
=====================================================================
```

   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.

On OMU/OML 9.x:

1. Log in to Java Console as user `opc_adm`.
2. Go to **Tools > DPSPI Applications**. Start the tool **Data Protector Add Cell**. This opens a terminal window where you are asked to input some information:



```
Add Data Protector Cell

Provide login information
Operation Manager Admin Name:opc_adm
Password                    :

Provide Data Protector cell information
Host of cell manager::spihpux4.ind.hp.com
Name of cell        ::spihpux4.ind.hp.com

Cell manager's node type :
Machine Type  :=OPC_MACHINE_BBC_HPUX_PARISC
Platform group:=DP UX MGRS
Node spihpux4.ind.hp.com exists
Assigning:  spihpux4.ind.hp.com to node group:  DP ALL MGRS
spihpux4.ind.hp.com => DP UX MGRS
Press Enter To Exit
```

Severity	Dup.	SUIAONE	Time Received	Node	Application	MsgGrp	Object	Message Text
Critical		-X-----	19:54:26 06/23/10	dpi00050.ind.hp....	HP Operations ...	OpC	Licensing	Critical Notification: 1 'HP Operations Manager Server' licens...
Critical		-X-----	19:54:26 06/23/10	dpi00050.ind.hp....	HP Operations ...	OpC	Licensing	Critical Notification: 3 'Agent Count' licenses are used in you...
Normal		--X----	19:54:23 06/23/10	dpi00050.ind.hp....	HP Operations ...	OpC	ovoareqsdr ...	Open Agent Service terminated. (OpC40-471)
Warning		--X----	19:54:23 06/23/10	dpi00050.ind.hp....	HP Operations ...	OpC	opcmsgm (...	Errors while creating IP address mapping table. (OpC40-610...

50 of 149 0 0 56 392 0 0 0 □ Lock

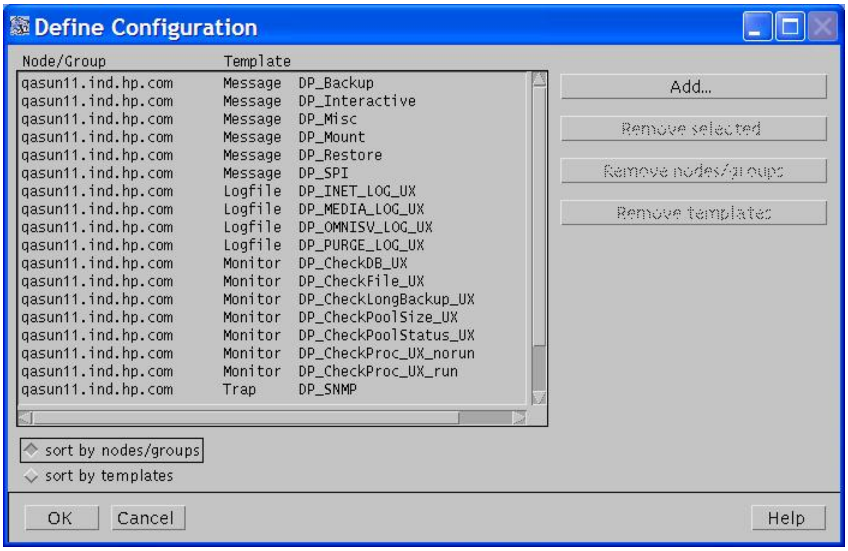
As a result, a new node group is added to the `Node Group Bank` and a new layout group is added to the `DP ALL MGRS` node hierarchy.

Distributing software, actions, commands, monitors and templates to the Data Protector Cell Manager

On OMU 8.x:

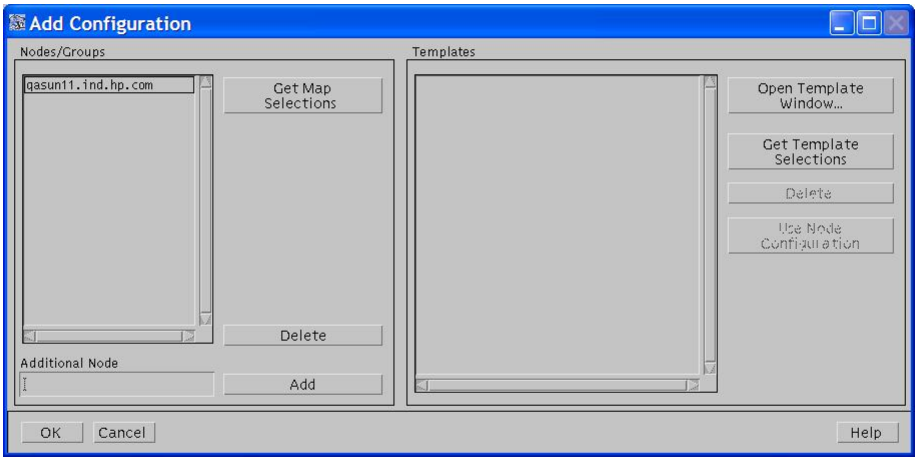
To distribute items to the DP Cell Manager Managed Node (appropriate assignments should have been made during installation):

1. Log in as user `opc_adm`.
2. Select the appropriate node group from the `Node Group Bank`.
3. From the `Node Group Bank`, assign templates as follows:
   a. Select **Actions > Agents > Assign Templates > Add**.



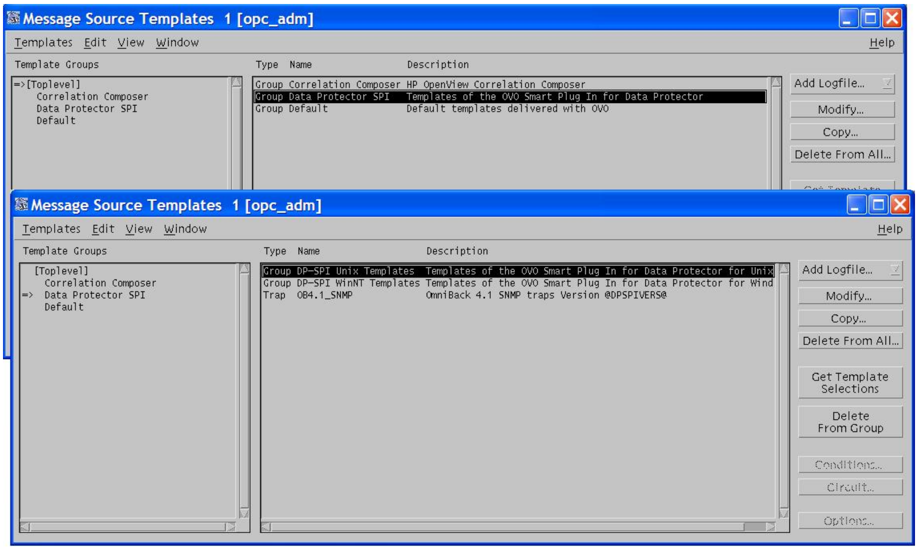
```
Node/Group          Template
qasun11.ind.hp.com  Message  DP_Backup
qasun11.ind.hp.com  Message  DP_Interactive
qasun11.ind.hp.com  Message  DP_Misc
qasun11.ind.hp.com  Message  DP_Mount
qasun11.ind.hp.com  Message  DP_Restore
qasun11.ind.hp.com  Message  DP_SPI
qasun11.ind.hp.com  Logfile  DP_INET_LOG_UX
qasun11.ind.hp.com  Logfile  DP_MEDIA_LOG_UX
qasun11.ind.hp.com  Logfile  DP_OMNISV_LOG_UX
qasun11.ind.hp.com  Logfile  DP_PURGE_LOG_UX
qasun11.ind.hp.com  Monitor  DP_CheckDB_UX
qasun11.ind.hp.com  Monitor  DP_CheckFile_UX
qasun11.ind.hp.com  Monitor  DP_CheckLongBackup_UX
qasun11.ind.hp.com  Monitor  DP_CheckPoolSize_UX
qasun11.ind.hp.com  Monitor  DP_CheckPoolStatus_UX
qasun11.ind.hp.com  Monitor  DP_CheckProc_UX_norun
qasun11.ind.hp.com  Monitor  DP_CheckProc_UX_run
qasun11.ind.hp.com  Trap     DP_SNMP
```

b. In the **Add Configuration** window click **Open Template Window…**. This opens a **Message Source Templates** window.



```
qasun11.ind.hp.com
```

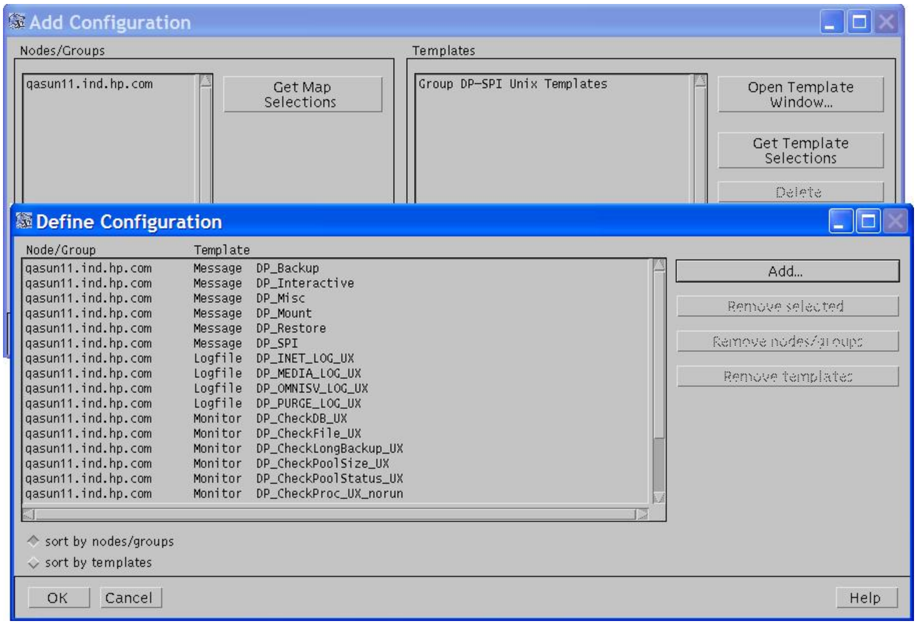
c. Select `Data Protector SPI` templates.



```
Template Groups          Type  Name                 Description
=>[Toplevel]             Group Correlation Composer HP OpenView Correlation Composer
    Correlation Composer Group Data Protector SPI   Templates of the OVO Smart Plug In for Data Protector
    Data Protector SPI   Group Default              Default templates delivered with OVO
    Default
```

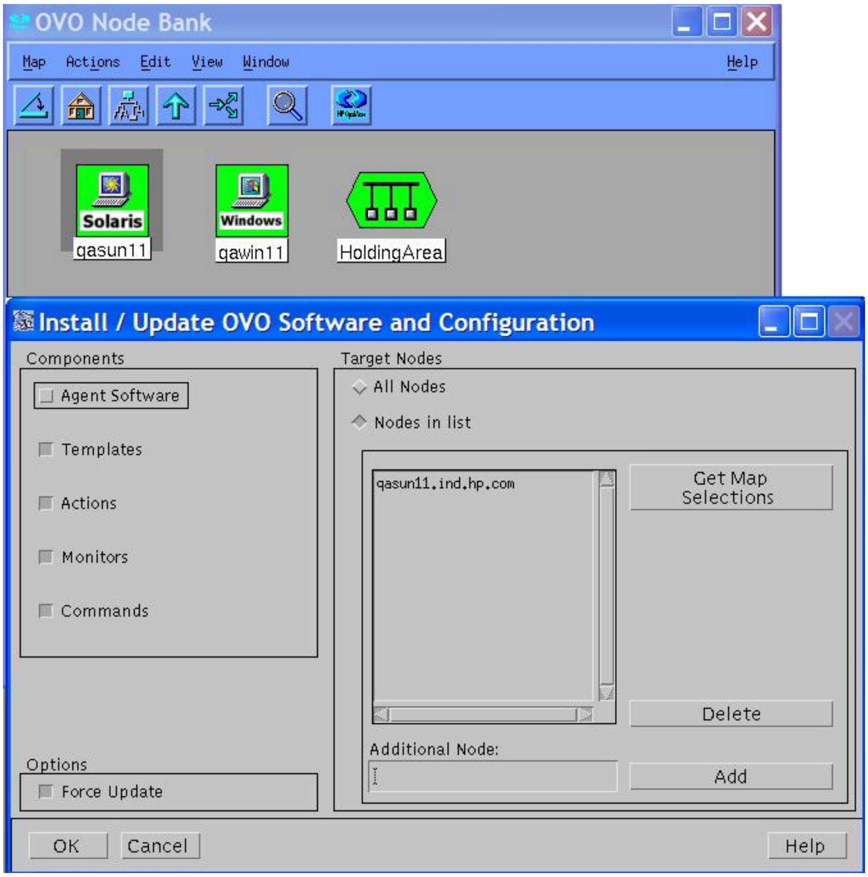
```
Template Groups          Type  Name                 Description
  [Toplevel]             Group DP-SPI Unix Templates  Templates of the OVO Smart Plug In for Data Protector for Unix
    Correlation Composer Group DP-SPI WinNT Templates Templates of the OVO Smart Plug In for Data Protector for Wind
=>  Data Protector SPI   Trap  OB4.1_SNMP             OmniBack 4.1 SNMP traps Version @DPSPIVERS@
    Default
```

d. In the **Add Configuration** window, click **Get Template Selections** to get the selected templates.



```
Node/Group            Template
qasun11.ind.hp.com    Message  DP_Backup
qasun11.ind.hp.com    Message  DP_Interactive
qasun11.ind.hp.com    Message  DP_Misc
qasun11.ind.hp.com    Message  DP_Mount
qasun11.ind.hp.com    Message  DP_Restore
qasun11.ind.hp.com    Message  DP_SPI
qasun11.ind.hp.com    Logfile  DP_INET_LOG_UX
qasun11.ind.hp.com    Logfile  DP_MEDIA_LOG_UX
qasun11.ind.hp.com    Logfile  DP_OMNISV_LOG_UX
qasun11.ind.hp.com    Logfile  DP_PURGE_LOG_UX
qasun11.ind.hp.com    Monitor  DP_CheckDB_UX
qasun11.ind.hp.com    Monitor  DP_CheckFile_UX
qasun11.ind.hp.com    Monitor  DP_CheckLongBackup_UX
qasun11.ind.hp.com    Monitor  DP_CheckPoolSize_UX
qasun11.ind.hp.com    Monitor  DP_CheckPoolStatus_UX
qasun11.ind.hp.com    Monitor  DP_CheckProc_UX_norun
```

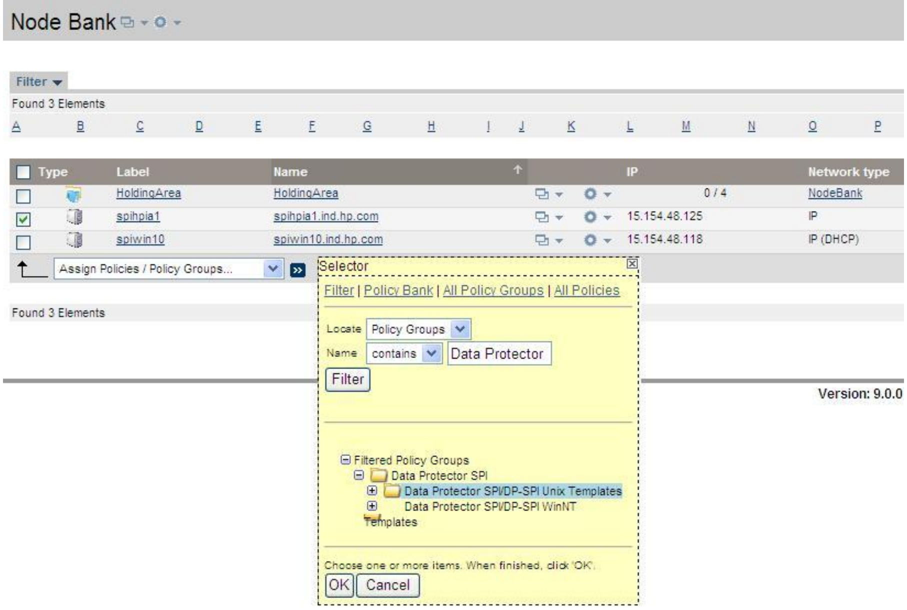
4. Deploy the templates by selecting **Actions > Agents > Install/Update SW & Config**. Follow any instructions displayed in the terminal window.



On OMU/OML 9.x:

To distribute items to the DP Cell Manager Managed Node:

1. Log in to Operations Manager Admin UI as user `opc_adm`.
2. Open the Node Bank. Select the node and click **Assign Policies/Policy Groups...**. Select the policy and click **OK**.


Node Bank
Filter
Found 3 Elements
A B C D E F G H I J K L M N O P

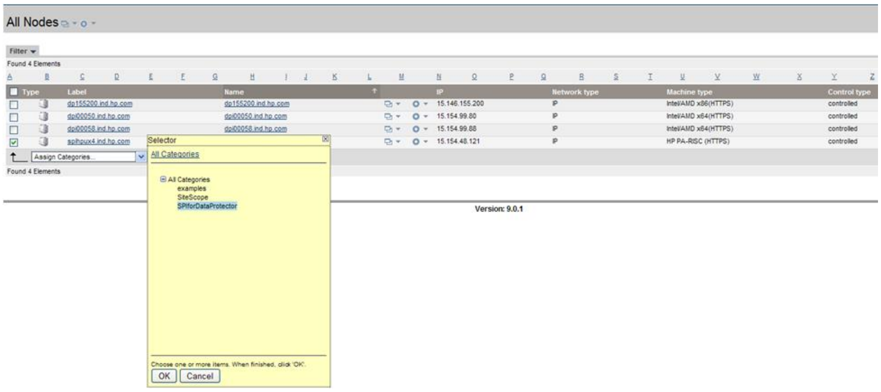
☐ Type	Label	Name	IP	Network type
☐	HoldingArea	HoldingArea	0 / 4	NodeBank
☑	spihpia1	spihpia1.ind.hp.com	15.154.48.125	IP
☐	spiwin10	spiwin10.ind.hp.com	15.154.48.118	IP (DHCP)

Assign Policies / Policy Groups...
Found 3 Elements
Version: 9.0.0
Selector
Filter | Policy Bank | All Policy Groups | All Policies

Locate: Policy Groups
Name: contains Data Protector

Filter
Filtered Policy Groups
Data Protector SPI
Data Protector SPI/DP-SPI Unix Templates
Data Protector SPI/DP-SPI WinNT Templates
Choose one or more items. When finished, click 'OK'.
OK
Cancel

3. Open the Node Bank. Select the node and click **Assign Categories…**. Select **SPIforDataProtector** and click **OK**.



☐ Type	Label	Name	IP	Network type	Machine type	Control type
☐	dp155200.ind.hp.com	dp155200.ind.hp.com	15.146.155.200	IP	Intel/AMD x86(HTTPS)	controlled
☐	dpi00050.ind.hp.com	dpi00050.ind.hp.com	15.154.99.80	IP	Intel/AMD x64(HTTPS)	controlled
☐	dpi00058.ind.hp.com	dpi00058.ind.hp.com	15.154.99.88	IP	Intel/AMD x64(HTTPS)	controlled
☑	spihpux4.ind.hp.com		15.154.48.121	IP	HP PA-RISC (HTTPS)	controlled

4. Deploy the policy by selecting **Deploy Configuration** option.

Agent configuration

SNMP configuration on UNIX

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

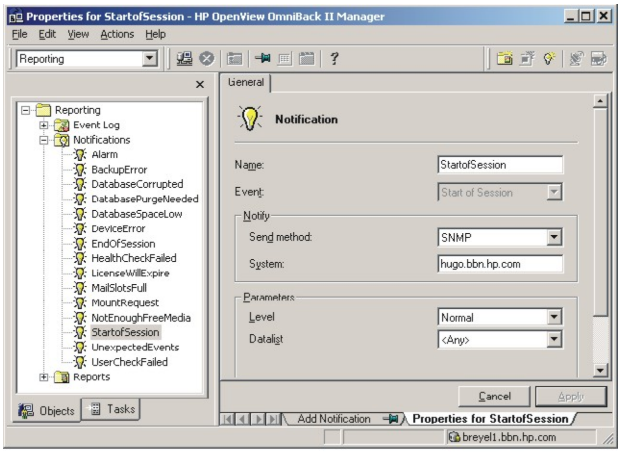
1. Execute one of the following commands to set the SNMP mode:
   - If an `ovtrapd` process is running, add:

     ```
     ovconfchg -ns eaagt -set SNMP_SESSION_MODE TRY_BOTH
     ```

   - If no `ovtrapd` process is running, add:

     ```
     ovconfchg -ns eaagt -set SNMP_SESSION_MODE NO_TRAPD
     ```

2. Configure the SNMP Emanate Agent to send SNMP traps to the local Operations Manager Agent by adding the following lines to the `snmpd.conf` file:
   - ***HP-UX systems:*** `/etc/SnmpAgent.d/snmpd.conf trap-dest: 127.0.0.1`
   - ***Solaris systems:*** `/etc/snmp/conf/snmpd.conf trap localhost trap-community public`
   - ***Linux systems:*** `/etc/snmp/snmp.conf com2sec local localhost public`
3. Configure Data Protector to send SNMP traps to the DP Cell Manager host:
   a. Using the Data Protector GUI's **Reporting** context window, set up all Notification events to use:
      - SNMP as delivery method
      - Cell Manager host system as the destination



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/server/snmp` (Data Protector A.06.00 and later).
   c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `/etc/opt/omni/server/snmp` (Data Protector A.06.00 and later).

SNMP configuration on Windows

Configure the Windows system to forward its SNMP traps to the Operations Manager Server as follows:

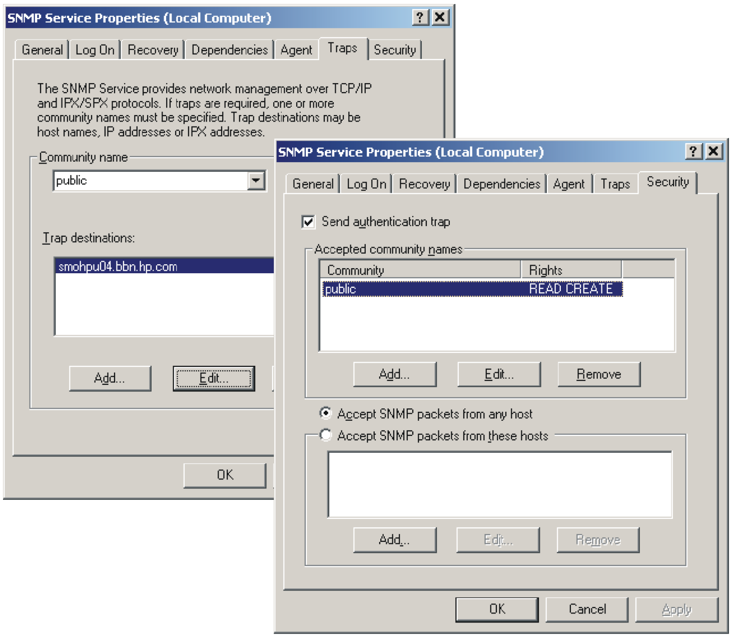
1. To enable Data Protector to send SNMP traps, execute the command: `omnisnmp`
2. To set the SNMP mode, execute the following command:

   ```
   ovconfchg -ns eaagt -set SNMP_SESSION_MODE NO_TRAPD
   ```

3. Configure the SNMP Service on a Windows system to send traps to the Operations Manager 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 Operations Manager 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 will then use this 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
Add... | Edit... | OK
SNMP Service Properties (Local Computer)
General | Log On | Recovery | Dependencies | Agent | Traps | Security
Add... | Edit... | Remove
Add... | Edit... | Remove
OK | Cancel | Apply

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

☑ Send authentication trap

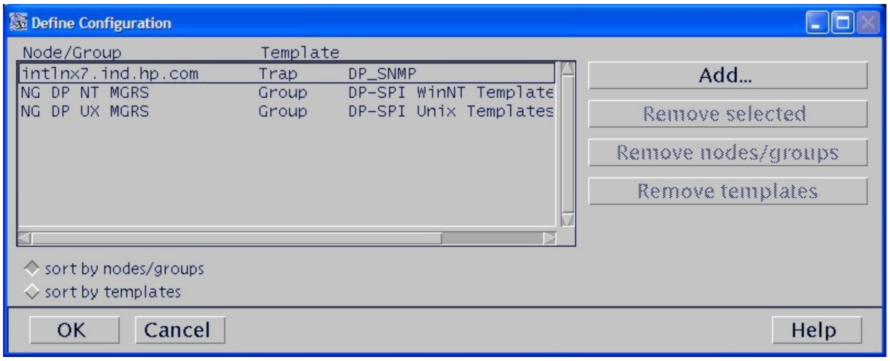
Accepted community names

Community	Rights
public	READ CREATE

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

4. Configure Data Protector to send SNMP traps to the Operations Manager Server system:
   a. Using the Data Protector GUI's **Reporting** context window, set up all Notification events to use:
      - SNMP as delivery method
      - Operations Manager Server system as the destination
   b. Add the Operations Manager Server hostname as trap destination to the `OVdests` file in *`Data Protector Root`*`/Config/server/SNMP`.
   c. Disable filtering of SNMP traps by emptying the `OVfilter` file in *`Data Protector Root`*`/Config/server/SNMP`.
5. Configure the Operations Manager sever to intercept SNMP traps sent by Windows Cell Manager. To do this, use the Operations Manager GUI to assign and distribute the template “DP_SNMP” to the Operations Manager Server.



Node/Group		Template
intlnx7.ind.hp.com	Trap	DP_SNMP
NG DP NT MGRS	Group	DP-SPI WinNT Template
NG DP UX MGRS	Group	DP-SPI Unix Templates

Data Protector user configuration

NOTE: DP SPI tools and applications do not support non-root agent nodes.

UNIX nodes: Check the local root user is in Data Protector's `admin` user group.

Windows systems: Add the local `HP ITO account` user to Data Protector's `admin` user group.

Program identification

NOTE: This applies to Operations Manager 8.x only.

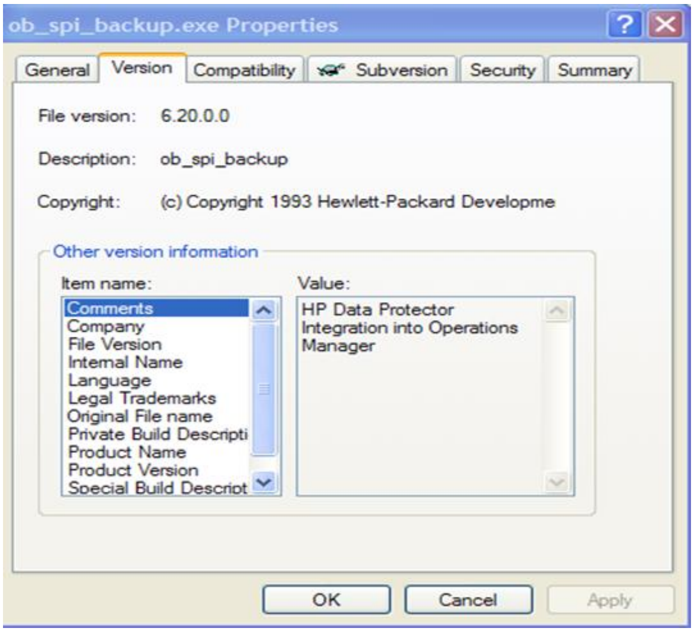
UNIX managed nodes: All Data Protector Integration programs and configuration files contain an identification string that can be displayed using the UNIX command “`what(1):`”.

The output is of the form:

```
Data Protector Integration into Operations Manager Unix A.06.20
(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.



File version: 6.20.0.0

Description: ob_spi_backup

Copyright: (c) Copyright 1993 Hewlett-Packard Developme

Other version information

Item name:
Comments
Company
File Version
Internal Name
Language
Legal Trademarks
Original File name
Private Build Descripti
Product Name
Product Version
Special Build Descript

Value:
HP Data Protector Integration into Operations Manager

Uninstalling the Data Protector Integration

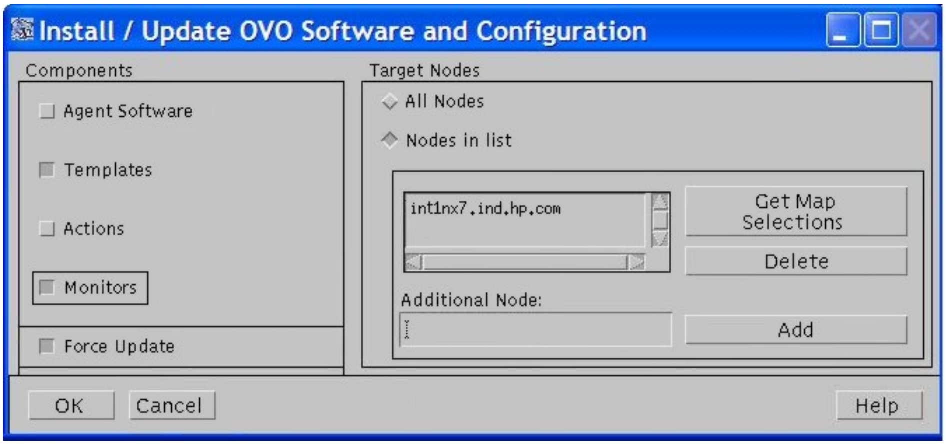
You need to remove components from:

- Managed node systems (Data Protector Cell Manager)
- HP Operations Manager Server system

Uninstalling from managed nodes

On OMU 8.x:

1. Unassign the Data Protector Integration‘s Operations Manager templates and monitors from the Data Protector Cell Manager system (Operations Manager 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.



Install / Update OVO Software and Configuration

Components

□ Agent Software

□ Templates

□ Actions

□ Monitors

□ Force Update

Target Nodes

◇ All Nodes

◆ Nodes in list

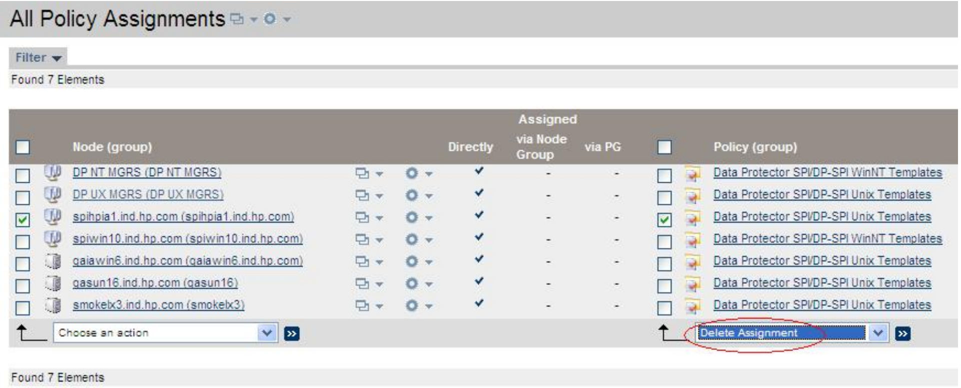
intlnx7.ind.hp.com

Additional Node:

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

On OMU/OML 9.x:

1. Log in to the Operations Manager Admin UI as user `opc_adm`.
2. Select **Browse > All Policy Assignments**.
3. Select the Node and the Policy. Click **Delete Assignment**:



All Policy Assignments

Filter

Found 7 Elements

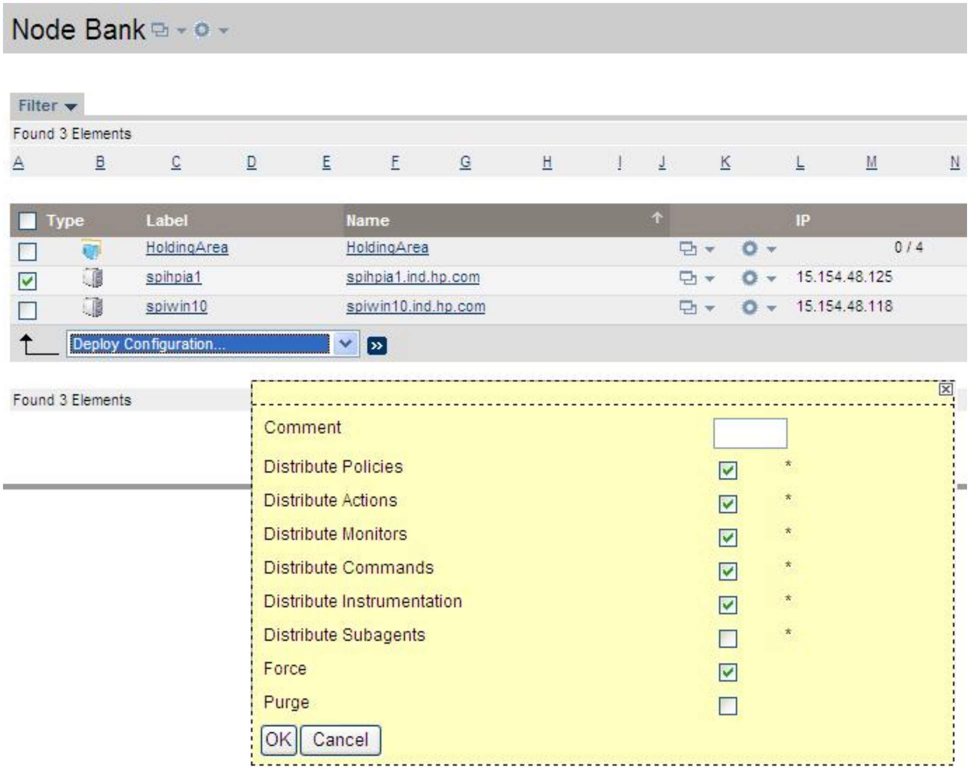
		Assigned				
□	Node (group)	Directly	via Node Group	via PG	□	Policy (group)
□	DP NT MGRS (DP NT MGRS)	✓	-	-	□	Data Protector SPI/DP-SPI WinNT Templates
□	DP UX MGRS (DP UX MGRS)	✓	-	-	□	Data Protector SPI/DP-SPI Unix Templates
☑	spihpia1.ind.hp.com (spihpia1.ind.hp.com)	✓	-	-	☑	Data Protector SPI/DP-SPI Unix Templates
□	spiwin10.ind.hp.com (spiwin10.ind.hp.com)	✓	-	-	□	Data Protector SPI/DP-SPI WinNT Templates
□	gaiawin6.ind.hp.com (gaiawin6.ind.hp.com)	✓	-	-	□	Data Protector SPI/DP-SPI Unix Templates
□	gasun16.ind.hp.com (gasun16)	✓	-	-	□	Data Protector SPI/DP-SPI Unix Templates
□	smokelx3.ind.hp.com (smokelx3)	✓	-	-	□	Data Protector SPI/DP-SPI Unix Templates

Choose an action

Delete Assignment

Found 7 Elements

4. 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.



Node Bank

Filter

Found 3 Elements

A B C D E F G H I J K L M N

☐ Type	Label	Name		IP
☐	HoldingArea	HoldingArea		0 / 4
☑	spihpia1	spihpia1.ind.hp.com		15.154.48.125
☐	spiwin10	spiwin10.ind.hp.com		15.154.48.118

Deploy Configuration...

Found 3 Elements

Comment		
Distribute Policies	☑	*
Distribute Actions	☑	*
Distribute Monitors	☑	*
Distribute Commands	☑	*
Distribute Instrumentation	☑	*
Distribute Subagents	☐	*
Force	☑	
Purge	☐	

OK Cancel

5. Remove the Data Protector Cell Manager from the Operations Manager managed environment by using the tool **Tools > DPSPI Applications > Delete Data Protector Cell**.

Uninstalling from the management server system 8.x

If the Operations Manager Server is using the default Administrator login name and password, uninstall with the command: `swremove SPI-DATAPROTECTOR-OM`

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

1. Use the command: `swask SPI-DATAPROTECTOR-OM`.
2. Enter the Operations Manager Server administrator login name and password.
3. Uninstall: `swremove SPI-DATAPROTECTOR-OM`

Once the DP integration is uninstalled, integration components will be removed from the Nodes, Tools, Policy and User Roles on the OMU GUI.

Uninstalling from the management server system 9.x

On HP-UX systems:

If the Operations Manager Server is using the default Administrator login name and password, uninstall with the command:`swremove DPSPI`

On Solaris systems:

If the Operations Manager Server is using the default Administrator login name and password, uninstall with the command:`pkgrm HPOvSpiDp`

On Linux systems:

If the Operations Manager Server is using the default Administrator login name and password, uninstall with the command:`rpm -e HPOvSpiDp`

3 Integration into HP Service Navigator

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

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

What is HP Service Navigator?

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

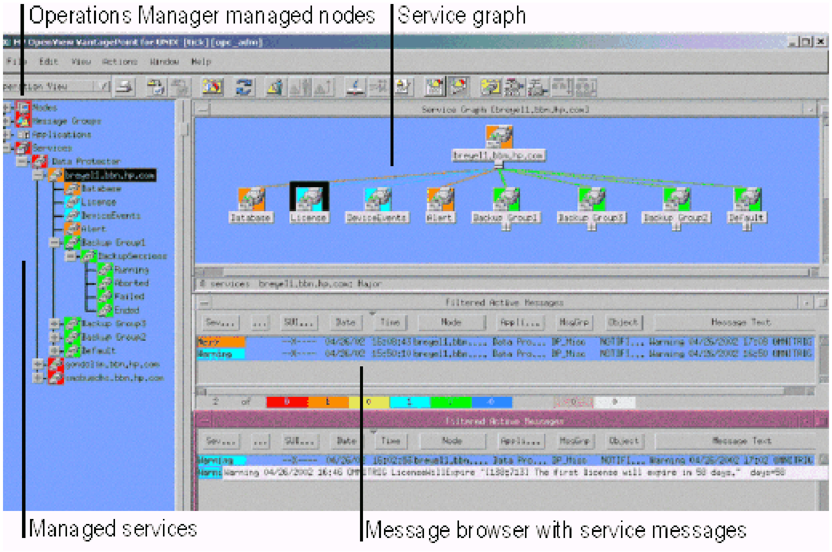
With Operations Manager, if a problem occurs on one of the objects, a message is sent to the user responsible for the area concerned. With Service Navigator, the message is mapped to the service impacted by the problem, and sent to the user responsible for that service.

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, Operations Manager'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 2 shows the Service Navigator main window. In addition to the customary Operations Manager 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 Operations Manager message browser configured to display only messages relevant to your service.

Figure 2 The Service Navigator GUI


Operations Manager managed nodes
Service graph
Managed services
Message browser with service messages

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.

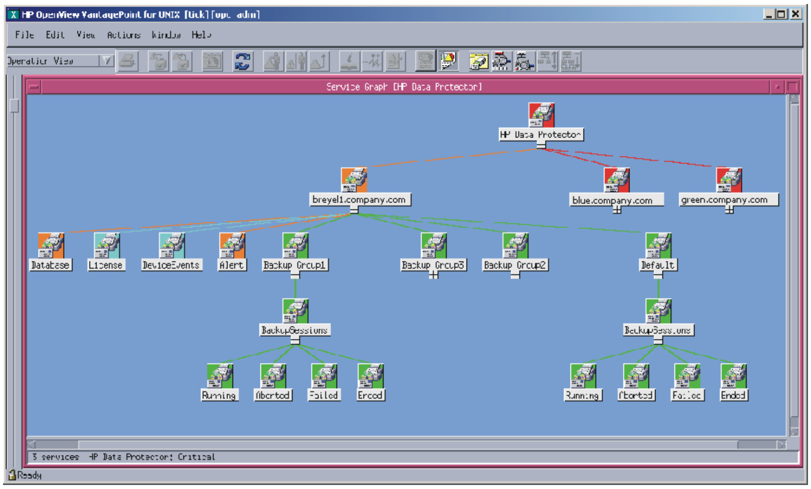
Service Navigator supports up to 256 hierarchical levels.

Figure 3 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.

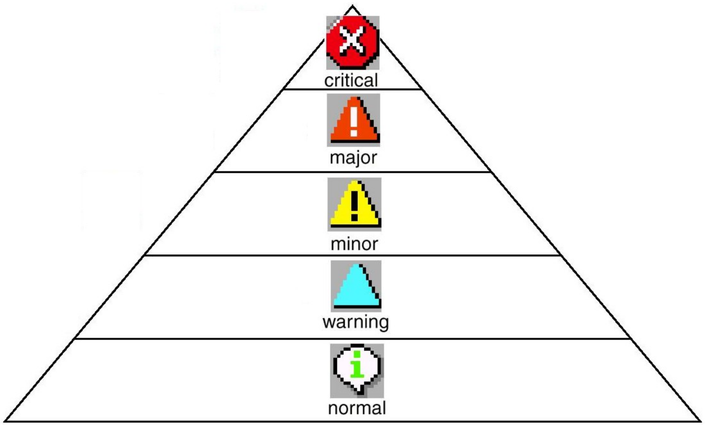
Figure 3 Example: Data Protector service hierarchy



Because Operations Manager 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.

Operations Manager severity pyramid

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



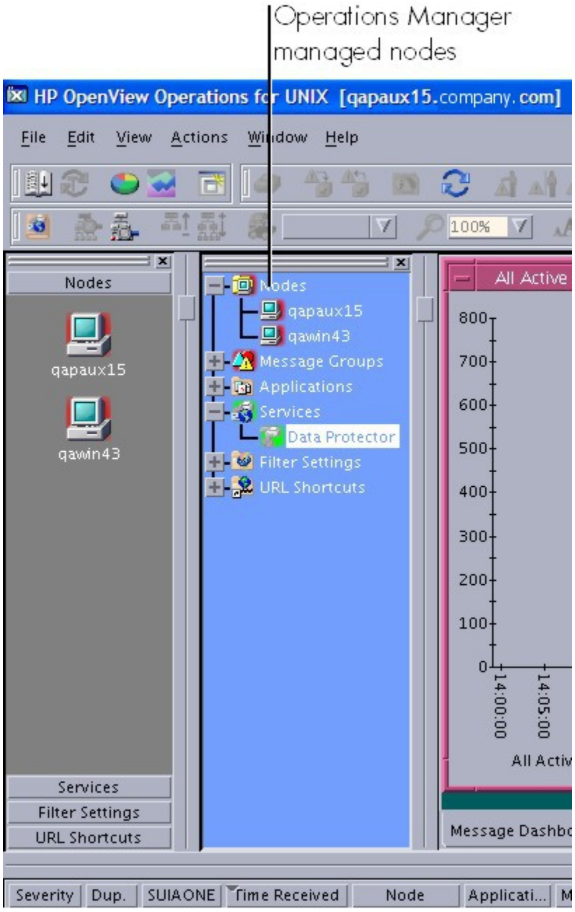
The severity status of the service is determined from the severity status of its subservices according to a set of rules. These are defined in the service configuration file; see the *HP Operations Service Navigator Concepts and Configuration Guide* for more information.

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 4 illustrates the Data Protector service tree with three Data Protector Cell Managers.

Figure 4 Data Protector service tree



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.

Node	Description
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 Data Protector Integration, `SPI-DATAPROTECTOR-OM` 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"
```

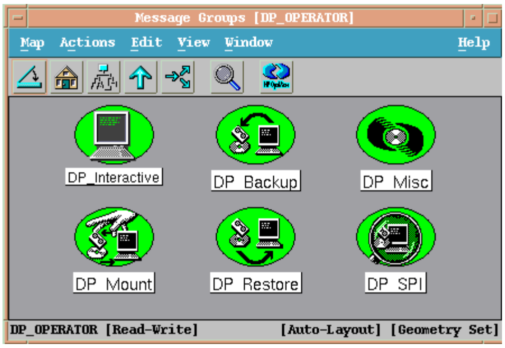
4 Using the Data Protector Integration

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

- “Message groups” (page 40)
- “Node groups” (page 41)
- “Application groups” (page 43)
- “Users and user profiles” (page 45)
- “Monitored objects” (page 50)
- “Monitored logfiles” (page 54)

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 Operations Manager 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 Operations Manager 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 Cell Manager system on which the event occurred.

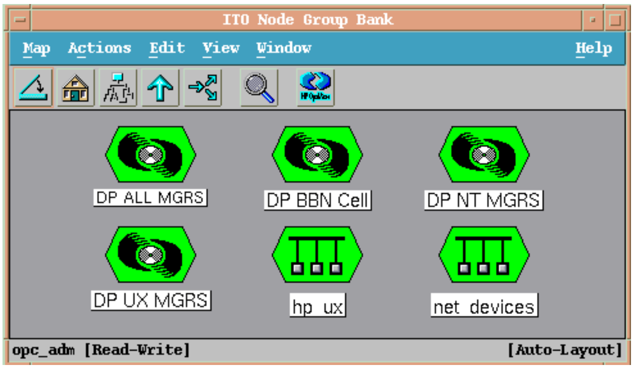
Severity	Reflection of the impact that the event has on Data Protector. For SNMP trap derived messages, the severity value of the SNMP trap is used as the severity level of the message.
Service Name	Depends on the impact the event has on a service. The value must map with a node in Data Protector's service 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:

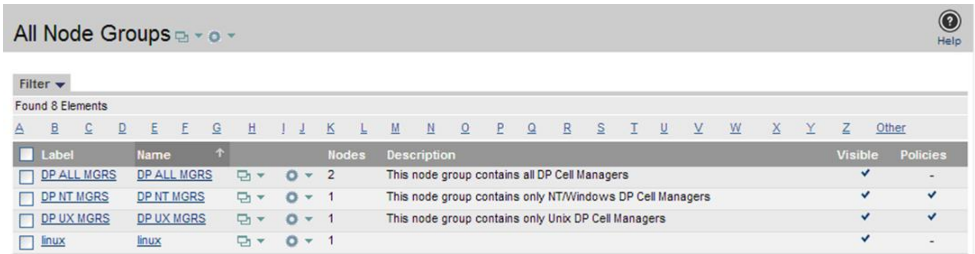
Figure 5 Data Protector Integration node groups for opc_adm for Operations Manager 8.x



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

Figure 6 Data Protector Integration node groups for opc_adm for Operations Manager 9.x

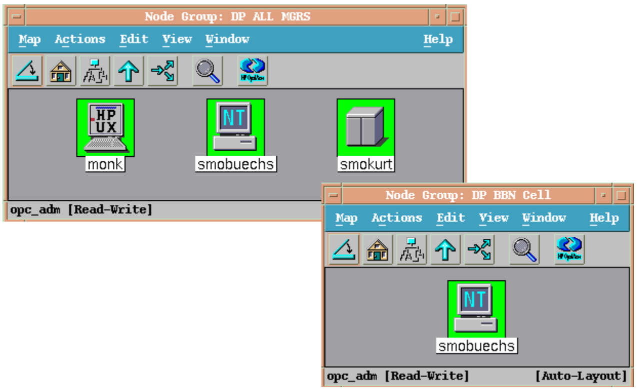


Found 8 Elements

Label	Name		Nodes	Description	Visible	Policies
DP ALL MGRS	DP ALL MGRS		2	This node group contains all DP Cell Managers	✓	-
DP NT MGRS	DP NT MGRS		1	This node group contains only NT/Windows DP Cell Managers	✓	✓
DP UX MGRS	DP UX MGRS		1	This node group contains only Unix DP Cell Managers	✓	✓
linux	linux		1		✓	-

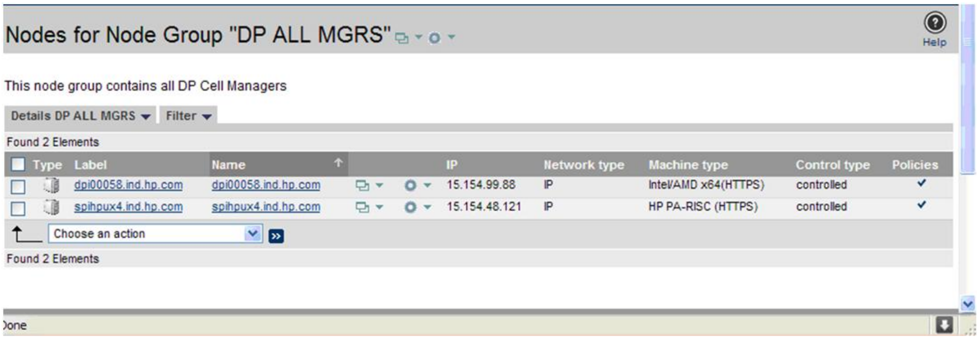
The content of `DP ALL MGRS` Node Group in Operations Manager 8.x and of the `DP BBN Cell` Node Group are illustrated in Figure 7.

Figure 7 DP ALL MGRS node group and DP BBN cell node groups in OM 8



The content of DP ALL MGRS node group in Operations Manager 9.x are illustrated in the following screen:

Figure 8 DP ALL MGRS node group in OM 9



Nodes for Node Group "DP ALL MGRS"

This node group contains all DP Cell Managers

Found 2 Elements

☐	Type	Label	Name		IP	Network type	Machine type	Control type	Policies
☐		dpi00058.ind.hp.com	dpi00058.ind.hp.com		15.154.99.88	IP	Intel/AMD x64(HTTPS)	controlled	✓
☐		spihpux4.ind.hp.com	spihpux4.ind.hp.com		15.154.48.121	IP	HP PA-RISC (HTTPS)	controlled	✓

Found 2 Elements

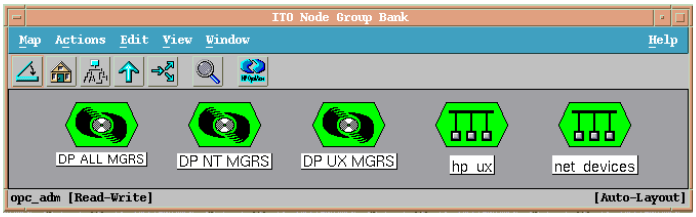
The predefined user profiles of the Data Protector Integration use message groups and node groups. Two further node groups are created during installation of the Data Protector Integration:

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

These can be used by any Operations Manager 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 9.

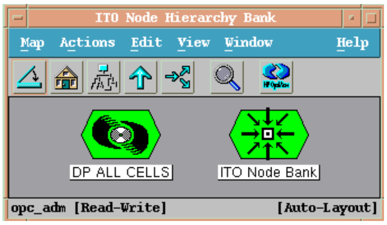
Figure 9 DP node groups created during installation


ITO Node Group Bank
Map Actions Edit View Window Help
DP ALL MGRS
DP NT MGRS
DP UX MGRS
hp_ux
net_devices
opc_adm [Read-Write] [Auto-Layout]

Node hierarchies

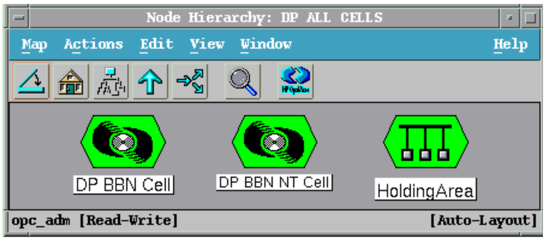
Node hierarchies are used to organize each operator's **Managed Node** window and are directly assigned to Operations Manager users (rather than to profiles). Each hierarchy is represented by an icon in the **Node Hierarchy Bank** window. It represents an organization of nodes and node layout groups.

Figure 10 Data Protector Integration node hierarchy bank for opc_adm



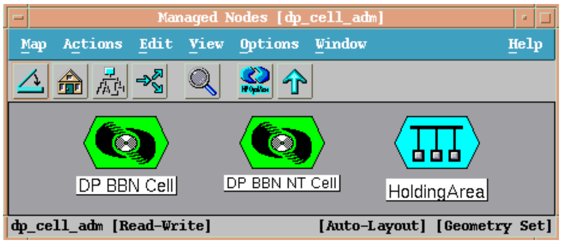
The `Add Data Protector Cell` action adds a node layout group for a Data Protector cell below the `DP ALL CELLS` node hierarchy, which is automatically created during installation.

Figure 11 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` is illustrated in Figure 12.

Figure 12 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]

NOTE: `DP ALL CELLS` is present only in Operations Manager 8.x.

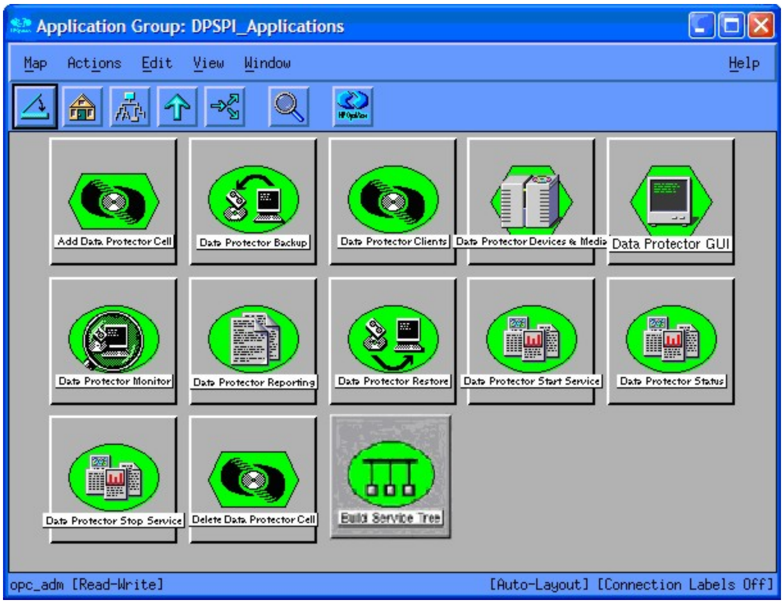
Application groups

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

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

DPSPI_Reports application group

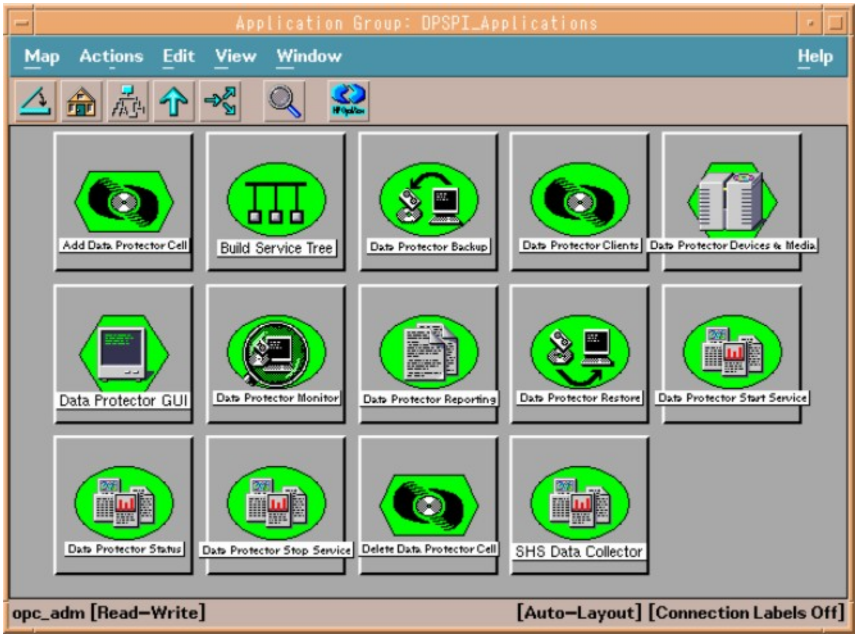
`DPSPI_Reports` contains applications for monitoring the health and performance of the Data Protector environment:



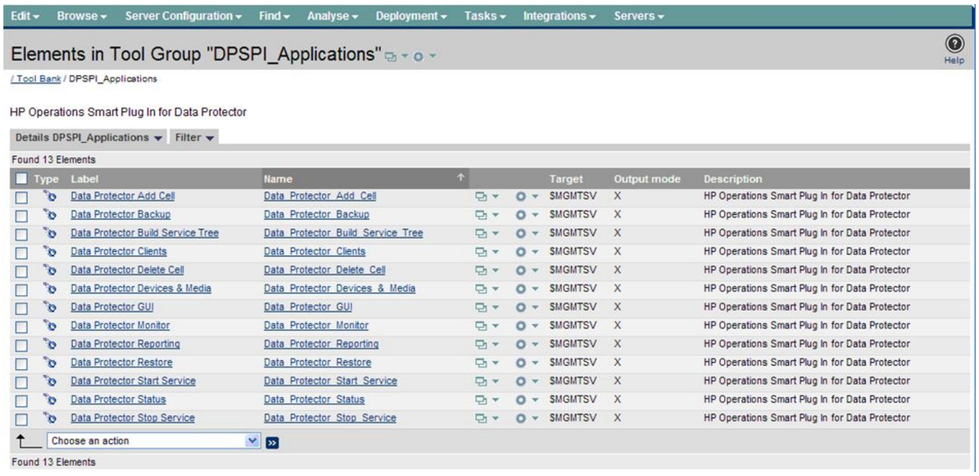
DPSPI_Applications application group

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

On OMU 8.x:



On OMU/OML 9.x:



Elements in Tool Group "DPSPI_Applications"

/ Tool Bank / DPSPI_Applications

HP Operations Smart Plug In for Data Protector

Found 13 Elements

□	Type	Label	Name	Target	Output mode	Description
□		Data Protector Add Cell	Data_Protector_Add_Cell	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Backup	Data_Protector_Backup	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Build Service Tree	Data_Protector_Build_Service_Tree	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Clients	Data_Protector_Clients	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Delete Cell	Data_Protector_Delete_Cell	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Devices & Media	Data_Protector_Devices_&_Media	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector GUI	Data_Protector_GUI	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Monitor	Data_Protector_Monitor	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Reporting	Data_Protector_Reporting	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Restore	Data_Protector_Restore	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Start Service	Data_Protector_Start_Service	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Status	Data_Protector_Status	$MGMTSV	X	HP Operations Smart Plug In for Data Protector
□		Data Protector Stop Service	Data_Protector_Stop_Service	$MGMTSV	X	HP Operations Smart Plug In for Data Protector

Found 13 Elements

Users and user profiles

This section describes the types of user in Operations Manager, 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, Operations Manager, and operating system users

Data Protector and Operations Manager 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 Operations Manager.

  Examples: Windows user in the EUROPE domain: `EUROPE\janesmith`

  UNIX user whose primary UNIX group is marketing:

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

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

  Example: `opc_adm` and `opc_op` are the default Operations Manager users.

  The Data Protector Integration generally does not set up any Operations Manager 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 Operations Manager, it does not matter who the operating system user is. The Operations Manager user used to log in to Operations Manager 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 Operations Manager user are required by the Data Protector Integration. The Operations Manager user determines the layout of the Operations Manager 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 Operations Manager 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 Operations Manager, not by the Operations Manager user itself.

Operations Manager user profiles

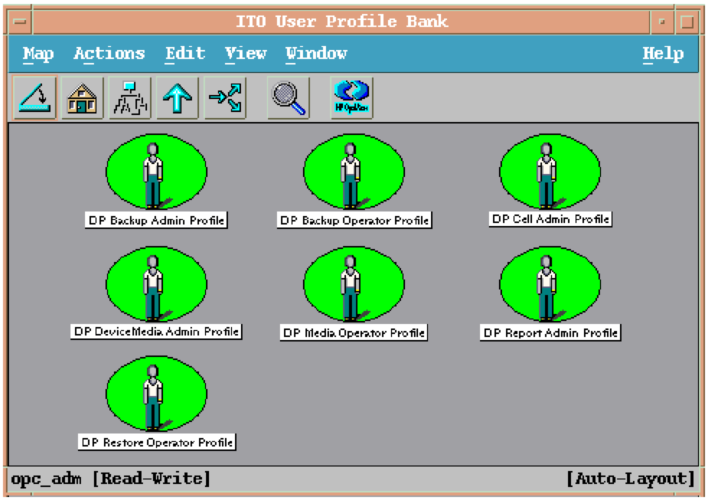
Operations Manager uses **user profiles** to describe the configuration of abstract users. They are useful in large, dynamic environments with many Operations Manager users and allow the rapid setting up of Operations Manager users with default configuration. An Operations Manager user may have multiple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

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

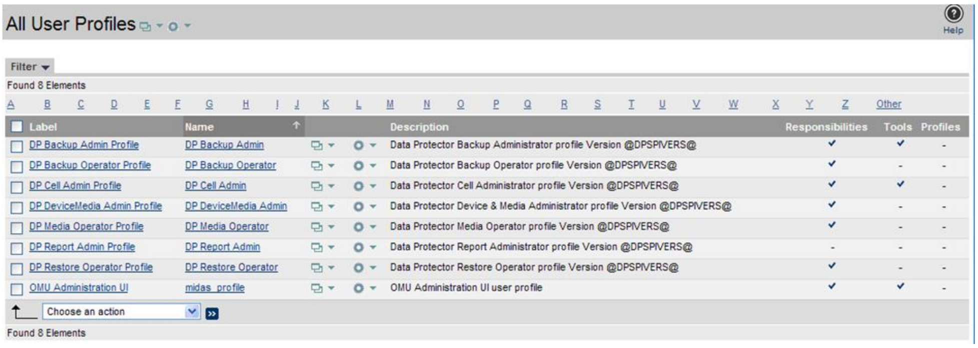
Data Protector Operations Manager user profiles

During installation, Data Protector Integration adds seven new user profiles to the Operations Manager **User Profile Bank** window—four administrators and three operators.

On OMU 8.x:



On OMU/OML 9.x:



Found 8 Elements

Label	Name	Description	Responsibilities	Tools	Profiles
DP Backup Admin Profile	DP Backup Admin	Data Protector Backup Administrator profile Version @DPSPIVERS@	✓	✓	-
DP Backup Operator Profile	DP Backup Operator	Data Protector Backup Operator profile Version @DPSPIVERS@	✓	-	-
DP Cell Admin Profile	DP Cell Admin	Data Protector Cell Administrator profile Version @DPSPIVERS@	✓	✓	-
DP DeviceMedia Admin Profile	DP DeviceMedia Admin	Data Protector Device & Media Administrator profile Version @DPSPIVERS@	✓	-	-
DP Media Operator Profile	DP Media Operator	Data Protector Media Operator profile Version @DPSPIVERS@	✓	-	-
DP Report Admin Profile	DP Report Admin	Data Protector Report Administrator profile Version @DPSPIVERS@	-	-	-
DP Restore Operator Profile	DP Restore Operator	Data Protector Restore Operator profile Version @DPSPIVERS@	✓	-	-
OMU Administration UI	midas_profile	OMU Administration UI user profile	✓	✓	-

Choose an action

Found 8 Elements

The following table lists for each user, applications available through icons on the **Application** window and message groups through the Operations Manager Message Browser. Roles for each user are listed in "Data Protector Operations Manager operators and their roles" (page 48).

Table 5 Data Protector Operations Manager user profiles

Admin/operator profile	Description
DP Backup Administrator	Restricted to a Data Protector Cell. *Applications:* Data Protector Backup *Messages:* Enable the Operations Manager message template for detailed messages, `DP_Detailed`.
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 Operations Manager 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.
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 Operations Manager operators

The Data Protector Operations Manager Operators use Operations Manager to maintain, manage, monitor, and control multiple Data Protector cells from a single console. Table 6 (page 48) defines the roles a Data Protector Operations Manager Operator might have and describes the appropriate access rights of an equivalent Data Protector user.

NOTE: Operations Manager users and Data Protector users are different and have to be set up in Operations Manager and Data Protector separately.

Operations Manager users are not created by the Data Protector Integration. The roles described in Table 6 (page 48) are examples of possible roles you may create and use to manage Data Protector.

Table 6 Data Protector Operations Manager 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.
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.
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.

Table 6 Data Protector Operations Manager operators and their roles *(continued)*

Role	DP privileges	Description
	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.
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 Operations Manager 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.pl` 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 Operations Manager 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 Operations Manager.

Operations Manager administrator

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

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

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

Monitored objects

Operations Manager 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 Operations Manager 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`
Node	*`name_cell_manager`*
Severity	Critical
Service Name	`Services.Data Protector.`*`cell name`*
Object	*Windows systems:* `DP_CheckProc_NT` *UNIX systems:* `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`
Node	*`name_database_server`*
Severity	Critical
Service Name	`Services.Data Protector.`*`cell name`*`.Database`
Object	*Windows systems:* `DP_CheckDB_NT` *UNIX systems:* `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:

On OMU 8.x:

Windows systems: `ob_spi_db.exe DP_CheckDB_NT` *`days`* `obspi.conf`

UNIX systems: `ob_spi_db.sh DP_CheckDB_UX obspi.conf` *`days`*

On OMU/OML 9.x:

Windows systems: `ob_spi_db.pl DP_CheckDB_NT` *`days`* `obspi.conf`

UNIX systems: `ob_spi_db.pl DP_CheckDB_UX` *`days`* `obspi.conf`

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:

- Bad (Critical)
- Poor (Critical)
- Fair (Warning)

Polling interval: 60 min.

Message structure:

Message Group	`DP_Misc`
Applications	`Data Protector`
Node	*`name_cell_manager`*
Severity	Critical or Warning
Service Name	`Services.Data Protector.`*`cell name`*
Object	*Windows systems:* `DP_CheckPoolStatus_NT` *UNIX systems:* `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`
Node	*`name_cell_manager`*
Severity	Critical or Warning
Service Name	`Services.Data Protector.`*`cell name`*
Object	*Windows systems:* `DP_CheckPoolSize_NT` *UNIX systems:* `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`
Node	*`name_database_server`*
Severity	Critical or Warning
Service Name	`Services.Data Protector.`*`cell name`*`.`*`backup group`*`.Backup Sessions.`*`session status`*
Object	*Windows systems:* `DP_CheckLongBackup_NT` *UNIX systems:* `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 A.06.00 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`
- `/etc/opt/omni/client/omni_info`
- `/etc/opt/omni/client/omni_format`

Polling interval: 15 min.

Windows systems

Checks if the following files exist in subdirectories of the Data Protector configuration directory (*default:* *`system_drive`*`\Program Files\OmniBack\Config\`):

For Data Protector A.06.00 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`
- `Client\omni_info`
- `Client\omni_format`

Polling interval: 15 min.

Monitored logfiles

You can use Operations Manager to monitor applications by observing their logfiles. You can suppress logfile entries or forward them to Operations Manager as messages. You can also restructure these messages or configure them with Operations Manager-specific attributes. For details, see the **Message Source Templates** window of the Operations Manager administrator's GUI.

Four Data Protector logfiles are monitored for warning and error patterns. For basic information, see the *HP 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`
Node	*`name_system`* on which logfile resides
Severity	`omnisv.log` (Normal) `inet.log` (Warning)
Service Name	`Services.Data Protector.`*`cell name`*
Object	*`logfile name`*
Automatic Action	Get status of Cell Manager processes

Examples:

```
2012-6-13 7:46:40 -STOP
HP Data Protector services successfully stopped.
```

```
2012-6-13 7:46:47 -START
HP 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:

```
06/14/12 09:42:30 INET.12236.0 ["inet/allow_deny.c /main/7":524] A.06.20
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 2012 [root.root@jowet.mycom.com] : .util

06/14/12 09:43:24 INET.12552.0 ["inet/allow_deny.c /main/7":524] A.06.20
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 2012 [root.sys@jowet.mycom.com] : .util

6/14/12 10:17:53 AM CRS.411.413 ["cs/mcrs/daemon.c /main/145":1380]
A.06.20 b364

User LARS.R@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:

```
06/17/12 15:42:15 ASM.1999 5.0 ["sm/asm/asm_purge.c /main/16":435]
A.06.20 b364

Purge session started.

06/17/12 15:42:15 ASM.1999 5.0 ["sm/asm/asm_purge.c /main/16":445]
A.06.20 b364

Filename purge session started.

06/17/12 15:42:16 ASM.1999 6.0 ["sm/asm/asm_purge.c /main/16":205]
A.06.20 b364

Purge session finished.

06/17/12 15:42:16 ASM.1999 5.0 ["sm/asm/asm_msg.c /main/12":91] A.06.20
b364

Filename purge session ended.
```

Parameters for messages for the default logfiles are:

Message Group	`DP_Misc`
Applications	`Data Protector`

Node	*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.

Managing cluster-aware applications

Clustered fail-over environments

The DP SPI can be configured to accommodate cluster environments with fail-over configuration.

When you configure the DP SPI to be synchronized with a cluster environment, you can choose for monitoring to switch off for a failed node and switch on for an active node. To recognize clustered instances, DP SPI relies on two XML configuration files. These files allow the Operations Manager agent to automatically enable instance monitoring on the currently active node after disabling instance monitoring on the inactive node.

The DP SPI setup for a cluster environment requires that you do the following:

- *(if needed)* Modify the file `dpspi.apm.xml` included with the DP SPI.
- Create `apminfo.xml` that associates DP SPI-monitored instances with the cluster packages.

Modifying dpspi.apm.xml

The DP SPI includes the XML file `dpspi.apm.xml`. This file works in conjunction with the file `apminfo.xml`, which you need to create (see “Creating apminfo.xml” (page 57). The purpose of the file is to list all the DP SPI policies on the managed node so that these policies can be disabled or enabled as appropriate for inactive or active managed nodes.

On the HP Operations Manager management server, `dpspi.apm.xml` is located in the following directories:

- *On an Operations Manager UNIX/Linux server using HTTPS agents:*

  ```
  /var/opt/OV/share/databases/OpC/mgd_node/instrumentation/
  SPIforDataProtector/Windows
  ```

- *On an Operations Manager Windows server using HTTPS agents:*

  ```
  OVAgentDir\shared\Instrumentation\Categories\SPI for
  DataProtector\Windows
  ```

Example of dpspi.apm.xml (using Data Protector configuration)

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
  <Application>
    <Name>dpspi</Name>
      <Template>DP_INET_LOG_NT</Template>
      <Template>DP_MEDIA_LOG_NT</Template>
      <Template>DP_OMNISV_LOG_NT</Template>
      <Template>DP_PURGE_LOG_NT</Template>
      <Template>DP_CheckFile_NT</Template>
      <Template>DP_CheckLongBackup_NT</Template>
      <Template>DP_CheckPoolSize_NT</Template>
      <Template>DP_CheckPoolStatus_NT</Template>
      <Template>DP_CheckProc_norun_NT</Template>
      <Template>DP_CheckDB_NT</Template>
      <Template>DP_Backup</Template>
      <Template>DP_CheckProc_run_NT</Template>
      <Template>DP_Interactive</Template>
      <Template>DP_Misc</Template>
      <Template>DP_Mount</Template>
      <Template>DP_Restore</Template>
      <Template>DP_SPI</Template>
      <Template>DP_SNMP_NT</Template>
      <Template>DP_Service_Discovery</Template>
  </Application>
</APMApplicationConfiguration>
```

Creating apminfo.xml

The second XML file is one you create and save as `apminfo.xml`. This file, working in conjunction with `dpspi.apm.xml`, allows you to associate DP SPI monitored instances with cluster packages. As a result, when a package is moved from one node in a cluster to another node in the same cluster, monitoring stops on the failed node and starts on the new node.

To create the file for DP SPI:

NOTE:

You *must* name the file `apminfo.xml`.

1. Using a text editor, create a file with entries as specified below. In the file, enter the Application Name to match the prefix of the `apm.xml` file (for example, for DP SPI, you would enter `dpspi`, as shown below). Enter the Instance Name to match the instance name entered in the DP SPI configuration file:

   ```
   <?xml version="1.0" ?>
   <APMClusterConfiguration xmlns="http://www.hp.com/OV/opcapm/cluster">
    <Application>
     <Name>dpspi</Name>
     <Instance>
      <Name>TESTCLUS</Name>
      <Package>Cluster Group</Package>
   ```

```
  </Instance>
      </Application>
</APMClusterConfiguration>
```

The instance `<Name>` is the Cluster Virtual Name and `<Package>` is the Group Name.

2. Save the completed `apminfo.xml` file on each node in the cluster in the following directory:
   - *HP-UX or Solaris or Linux using HTTPS agents:* `/var/opt/OV/conf/conf`
   - *Windows nodes using HTTPS agents:* `<installation_directory>\data\conf\conf\`

   If the directory does not already exist on the managed node, you need to create it.

3. On each node, stop and restart the agent:

   ```
   opcagt -kill
   opcagt -start
   ```

4. Add `CLUSTER_LOCAL_NODENAME` to the `conf.cluster` namespace:

   For example, on “Node1” execute:

   ```
   ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME Node1
   ```

   On “Node2”:

   ```
   ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME Node2
   ```

Once this is done, you will notice all DP SPI policies being disabled on passive nodes and enabled only on the active node.

NOTE: To verify if this configuration is successful, execute the command on all the physical nodes in a cluster:

```
#opctemplate -l
```

DP SPI policies will be enabled only on the active node.

5 Troubleshooting

Error: No message appearing on the Operations Manager browser for illegal command usage in DP/deny host.

Action: Ensure messages are written into `inet.log` file.

Error: Monitor messages are not appearing on the message browser. For example, Data Protector Backup is running for over 12 hours (greater than the critical time mentioned in the `obspi.conf` file). A LongBackup message does not appear on the Message browser.

Action: Ensure:

1. Monitor scripts are present in the directory *`OM_Installed_Packages_Dir`*`\bin\instrumentation` (Windows) or `/var/opt/OV/bin/instrumentation` (UNIX).
2. SPI templates are enabled on the managed node:

   ```
   OM_Installed_dir/bin/OpC/opctemplate
      Type     Name                         Status   Version
      ----------------------------------------------------
      MONITOR  "DP_CheckDB_UX"              enabled  1
      MONITOR  "DP_CheckFile_UX"            enabled  1
      MONITOR  "DP_CheckLongBackup_UX"      enabled  1
   ```

3. The proper agent is deployed on to the managed node and all agent processes are running.
   - On the node: `opcagt -status`
   - From the Operations Manager server: `opcragt -status` *`node name`*

Error: Not getting any SNMP traps.

Action:

1. On the Data Protector managed node check whether the SNMP Emanate Agent is installed.
2. Ensure the SNMP template is enabled on the node

   ```
   OM_Installed_dir/bin/OpC/opctemplate
      Type       Name           Status    Version
   ---------------------------------------------
      SNMPTRAP   "DP_SNMP"      enabled   1
      SNMPTRAP   "OB4.1_SNMP"   enabled   1
   ```

3. Ensure all the steps listed in “SNMP configuration on UNIX” (page 29) or “SNMP configuration on Windows” (page 30) are followed.
4. On a Linux machine check if the SNMP service is enabled as follows:

   ```
   # chkconfig --list | grep -i snmpd
     snmpd   0:off  1:off  2:off  3:off  4:off  5:off  6:off
   ```

   If it is off, use the following command to switch it on:

   ```
   # chkconfig --level 0123456 snmpd on

   # chkconfig --list | grep -i snmpd
     snmpd   0:on  1:on  2:on  3:on  4:on  5:on  6:on
   ```

Error: For on itanium managed node, Data Protector SPI applications are not able to open Data Protector's Java GUI.

Action: Ensure the `java1.5/jre/bin` directory is included in the PATH environment variable.

Error: The Data Protector Health Report in not being produced for the Windows node-DP SPI.

Action: Ensure the `remsh` daemon is running on the Windows node.

Error: `obusergrp.pl` is failing while adding the Operations Manager user profile to the Data Protector (installed on Windows) user list.

Action: Ensure FTP is installed on the windows node and OBCONFIG (virtual directory) is set to `C:\Program Files\OmniBack\Config` directory (or equivalent, if you have chosen a custom path).

Index