HP Data Protector A.06.20

Integration Guide for HP Operations Manager for Windows

Part Number: n/a
First edition: March 2011

Legal and notice information

Contents

Figures

Tables

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 Windows.

Intended audience

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

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

Documentation set

Other documents and online Help provide related information.

Guides

Data Protector guides are available in 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 Business Support Center website:

http://www.hp.com/support/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 online 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. It is intended for backup administrators or operators. There are six guides:

  - *HP Data Protector Integration Guide for Microsoft Applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*

    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, and Lotus Notes/Domino Server.

  - *HP Data Protector Integration Guide for VMWare, Sybase, Network Node Manager, 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, Microsoft Hyper-V, and Citrix XEN Server.

- *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. The 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 StorageWorks P6000 EVA Disk Array Family, HP StorageWorks P9000 XP Disk Array Family, HP StorageWorks P4000 SAN Solution, 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 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 Virtualization Environment*

  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 A.06.11. 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 providing some basic command-line examples.

Online help

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

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

- ***Windows:*** Unzip `DP_help.zip` and open `DP_help.chm`.

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

Documentation map

Abbreviations

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

Abbreviation	Guide
CLI	Command Line Interface Reference
Concepts	Concepts Guide
DR	Disaster Recovery Guide
GS	Getting Started Guide
GRE-SPS	Granular Recovery Extension User Guide for Microsoft SharePoint Server
GRE-VMware	Granular Recovery Extension User Guide for VMware vSphere
Help	Online 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

Abbreviation	Guide
IG-VirtEnv	Integration Guide for Virtualization Environments: VMware, Microsoft Hyper-V, and Citrix XEN Server
IG-VSS	Integration Guide for Microsoft Volume Shadow Copy Service
Install	Installation and Licensing Guide
MO GS	Media Operations Getting Started Guide
MO RN	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.

	Help	GS	Concepts	Install	Trouble	DR	PA	Integration Guides: MS	O/S	IBM	Var	VSS	VirtEnv	OMU	OMW	ZDB: Concept	Admin	IG	GRE: SPS	VMware	MO: GS	User	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				
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		
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				
Supported configurations																X								
Troubleshooting	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 User
Microsoft Exchange Server	IG-MS, ZDB IG

Software application	Guides
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
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 StorageWorks P4000 SAN Solutions	ZDB Concept, ZDB Admin, IG-VSS
HP StorageWorks P6000 EVA Disk Array Family	all ZDB
HP StorageWorks P9000 XP Disk Array Family	all ZDB

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text: Table 1 on page 17	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

NOTE:

Provides additional information.

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/storage
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to DP.DocFeedback@hp.com. All submissions become the property of HP.

1 Introduction

In this chapter

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.

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 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 Operations Manager Server can monitor multiple Data Protector Cell Managers.
- The integration also depicts the functionality of Data Protector as a service tree.
- The ARM and DSI interfaces of the Performance Agent collect performance data and ARM transactions.
- Messages sent to Operations Manager Server are channeled according to user profiles. Operations Manager users see only messages they need.
- The Data Protector Cell Manager and the Operations Manager Server to be installed on different systems.

- You can run Data Protector functionality from the **Operations Manager tool group** window.
- Data Protector Integration messages sent to the Operations Manager Server includes 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.
- Complements the Data Protector Administration GUI.
- Collection and monitoring of performance data.
- A central data repository for storing event records and action records for all Data Protector managed nodes.
- Utilities for running Data Protector management tasks.
- Allowing Operations Manager users to start the Data Protector GUI and use Data Protector functionality from the Operations Manager Server.

Data Protector Integration architecture

The Data Protector Integration is installed on the Operations Manager Server system and is deployed to instrument 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 Manager Agent and should have the HP Performance Agent (PA) installed. The Data Protector Console must be installed on the Operations Manager Server.

Once installed, the Operations Manager user can start the Data Protector graphical user interface (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. This is facilitated by the Data Protector Console using the Data Protector communication protocol on port 5555 to exchange data.

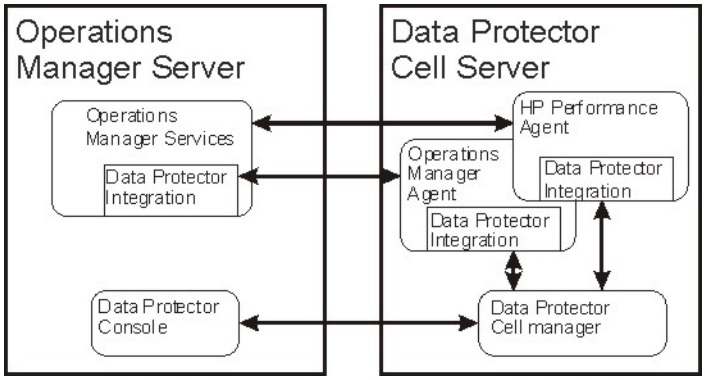


Figure 1 Operations Manager-Data Protector Integration architecture

The Operations Manager policies monitor:

- Data Protector vital Cell Manager processes
- Data Protector log files
- Data Protector events through SNMP traps

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

The integration policies, such as policies to monitor Data Protector logfiles, SNMP traps, database and processes, define the conditions on which the Operations Manager Agent will send messages to the Operations Manager Server for display in Operations Manager message browser.

2 Installing the Data Protector Integration

This chapter describes:

- Prerequisites for installing the Data Protector integration.
- Installing the Data Protector Integration on the 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 Operations Manager managed node (Data Protector Cell Manager) systems.
- Uninstalling the Data Protector Integration from the Operations Manager Server system.

Supported platforms and installation prerequisites

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

- One or more systems running Operations Manager Server
- The Operations Manager Server with Console (remote consoles are not supported) and the Data Protector Console installed on the same system.
- Operations Manager Agent running on systems with the Data Protector Cell Manager.

Before installing the Data Protector Integration, ensure that the requirements described in the sections below are met.

Data Protector supported versions

The Data Protector Integration is designed to work with the following HP Data Protector versions:

Table 2 HP Data Protector availability

HP Operations Manager for Windows	Data Protector Version
	6.0, 6.1, 6.11, 6.2
8.1 plus patches, if available 9.0 plus patches, if available	On all Data Protector cell server platforms where the OM Agent is also available

Operations Manager Server system

The supported platforms of HP Operations Manager Servers are documented in the associated product documents and product web-pages. The Operations Manager Server can run on a different system from the system on which the Data Protector Cell Manager is installed.

Operations Manager patches

Ensure up-to-date patches are installed, and that OM Agent patches after its installation on the OM Server 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 Windows*. The console is installed and configured on the Operations Manager Server system or other appropriate systems.
- The *HP Data Protector Console* is installed on the Operations Manager Server system.

Hardware prerequisites on the Operations Manager Server

Ensure the following hardware prerequisites are met on the Operations Manager Server system:

- 15 MB disk space on the Operations Manager Server system.

Managed node systems (Data Protector Cell Server)

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

Supported Operations Manager Agent versions

Ensure the Data Protector Cell Manager system runs on a platform for which the Operations Manager Agent is available. Go to http://www.hp.com/support/manuals to find out which platforms are supported.

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

The following software is required, but is not installed as part of the Operations Manager 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 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.

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 Server)

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

Disk-space requirements

The following table lists disk space requirements for both the installation of the Data Protector Integration and the Data Protector Integration's run-time files on the Operations Manager Server and the OM managed node.

Machine	Operations Manager Version	Operating System	Total
Operations Manager Server	8.1, 9.0	Windows	15 MB
Operations Manager Managed Node	8.1, 9.0	HP-UX, Solaris, Linux, Windows supported as managed node and Data Protector cell server	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 in the `HPOvSpiDp-6.20.000-WinNT4.0.msi` MSI package used to install the integration and console onto the Operations Manager Server. This installs all components required for the management server and the managed nodes on the management server system. Agent software and configuration data for these agents is then distributed by the Operations Manager administrator to the managed nodes using Operations Manager.

NOTE:

In the case of a cluster setup, install the integration on all cluster nodes that are designated to run Operations Manager. Install on first node, and after the installation finishes successfully, start it on the next node. Repeat this until all designated nodes are installed. The installation of the first cluster node differs from the installation of subsequent nodes.

Installation

To install the software on the management server, run the `HPOvSpiDp-6.20.000-WinNT4.0.msi` executable file.

The following directories are created on the Operations Manager Server system, where `INSTALLDIR` is the default installation directory:

OMW 8.1, 9.0: `system_drive\Program Files\HP\HP BTO Software`	
`INSTALLDIR\install\DPSPI\`	Installation directory with subdirectories for policies and Operations Manager configuration files
`INSTALLDIR\bin\`	Binary and script files

`INSTALLDIR\Instrumentation\Platform\Version\SPI for DataProtector\`	Monitor scripts, Service discovery scripts, and configuration files
`INSTALLDIR\NLS\1033\Manuals\`	Documentation containing this *Integration Guide* and the *Product Announcements, Software Notes, and References*

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

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

- `ob_spi_proc.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_Installed_Packages_Dir` should be:

Platform Agent Instrumentation directory

Windows HTTPS: `data_dir\bin\instrumentation`

`System Drive:\Program Files\HP OpenView\Installed Packages\{790C06B4-844E-11D2-972B-080009Ef8C2A}`

In `OM_Installed_Packages_Dir\bin\instrumentation`:

`obspi.conf`

- `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`
- `DPCmd.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`

NOTE:

You should delete these instrumentation files manually deleted from the Windows/UNIX Cell Manager nodes after the policies are un-installed from the nodes. The management server will *not* remove them automatically.

Installation verification

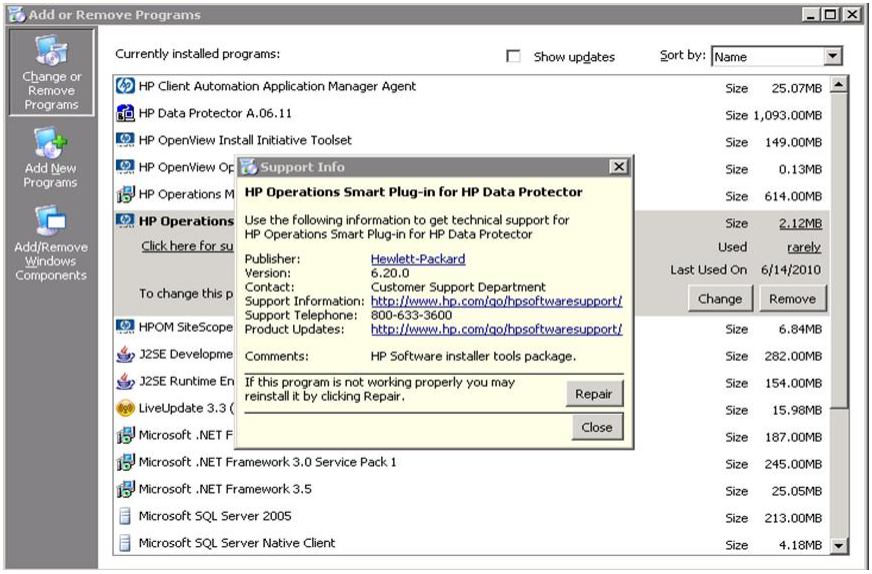
To verify the installation:

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

   Start -> Settings -> Control Panel -> Add/Remove Programs

2. Check `HP Operations Smart Plug-in for HP Data Protector` appears as an installed product.

Once the Data Protector integration is installed, you can find the integration components under Nodes, Tools and Policy on the OMW GUI.



NOTE:

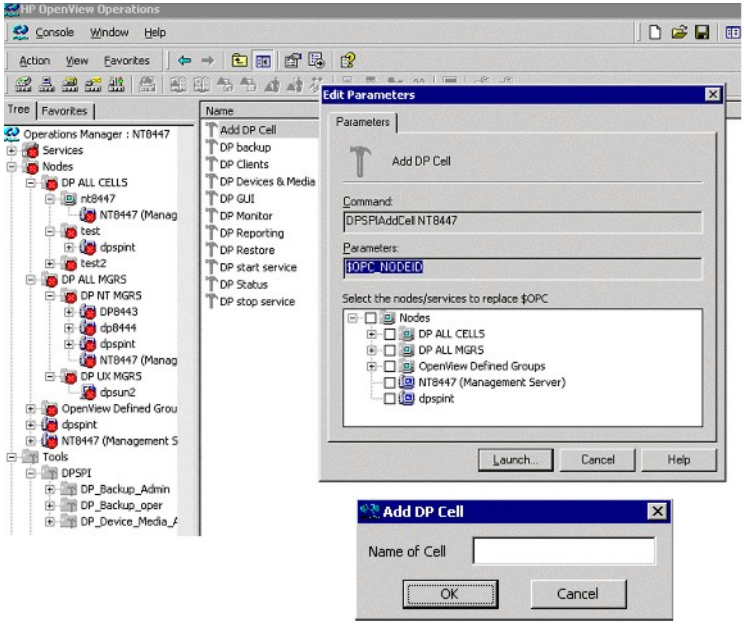
The ellipses highlight Data Protector integration components.

Running the Add Data Protector Cell application

To run the `Add Data Protector Cell` application:

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

   The **Edit Parameters** window is displayed:



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

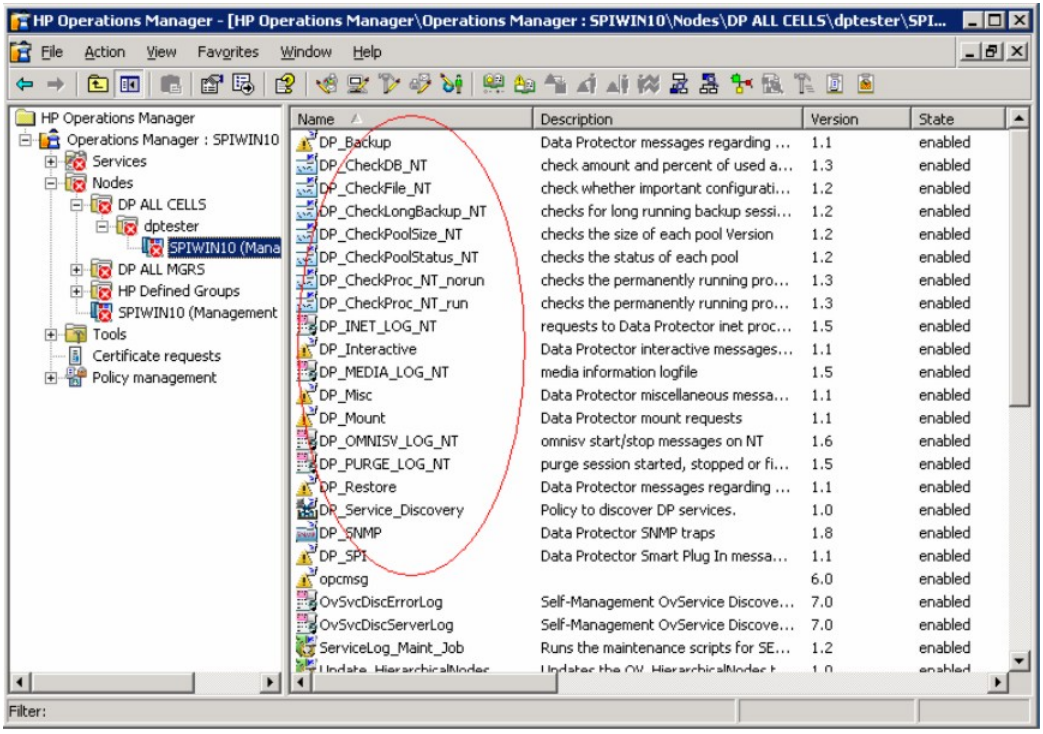
In the example in window above, the node name of the Cell Manager, `nt8447`, is also used for the name of the node folder created under `DP ALL CELLS`. This node group is provided to help you organize all systems managed by a Cell Manager, and including that Cell Manager, under the same folder in Operations Manager. You can use a different name if you wish. The resulting node configuration is displayed in the Operations Manager console.

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

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

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

View -> Policy inventory



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

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

3. Configure Data Protector to send SNMP traps to the Data Protector Cell Manager:

   a. Using the Data Protector GUI `Reporting` context, set up all Notification events to use:

      - SNMP as delivery method
      - Cell Manager system as the destination

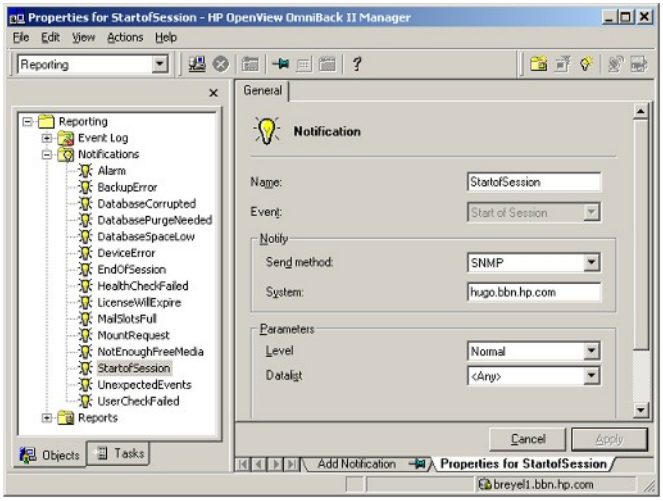


Figure 2 Data Protector GUI Reporting Context

   b. Add the Cell Manager hostname as trap destination to the `OVdests` file in `/etc/opt/omni/server/snmp` (Data Protector 6.0 and above).

   c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `/etc/opt/omni/server/snmp` (Data Protector 6.0 and above).

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, run 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 that Data Protector 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 CommunityREG_SZ:custom community name
   ```

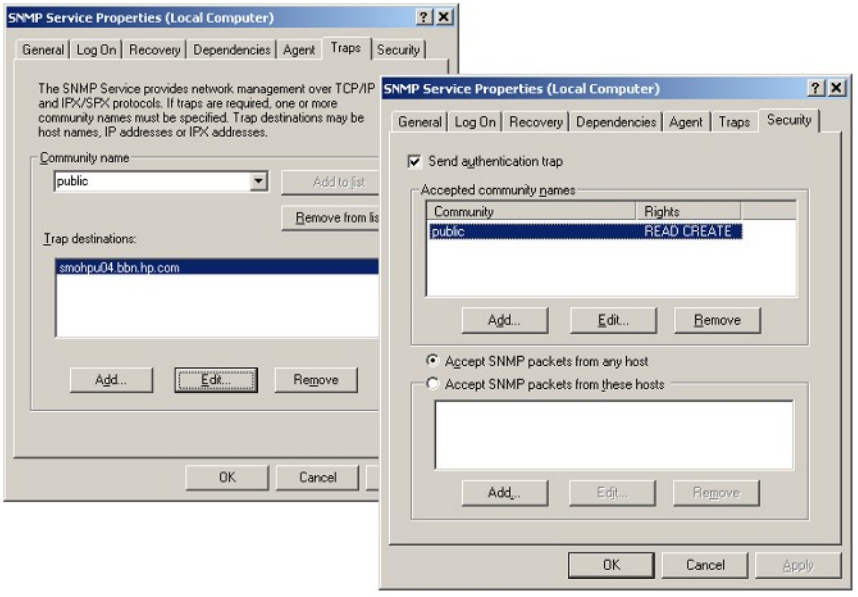


Figure 3 Configuring the SNMP service on Windows

4. Configure Data Protector to send SNMP traps to the Operations Manager Server system:

   a. Using the Data Protector GUI `Reporting` context, set up all notification events to use:

      - SNMP as delivery method
      - Operations Manager Server system as the destination

      See Figure 2 on page 33.

   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`.

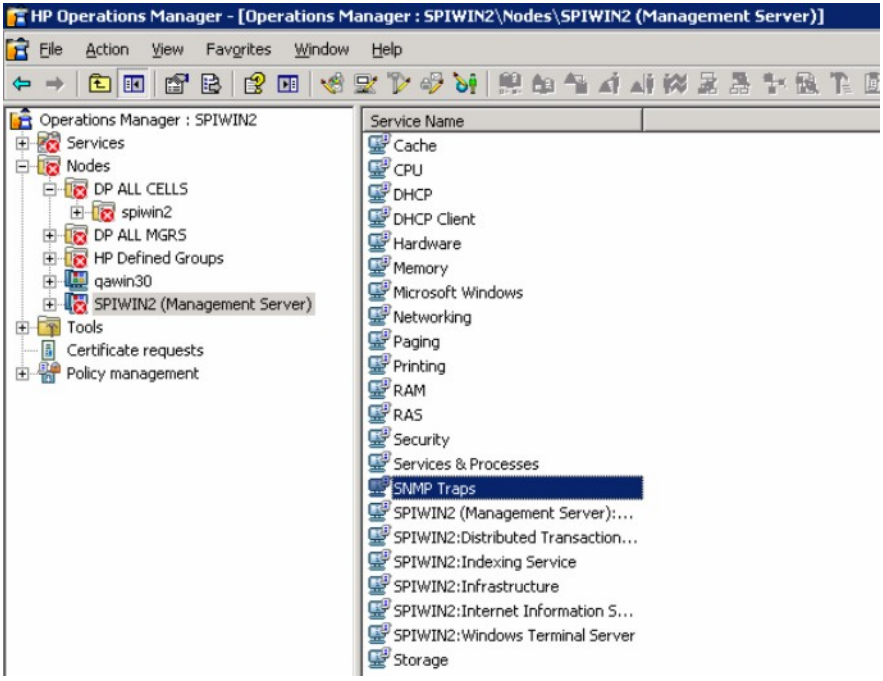
5. Configure the Operations Manager Server to intercept SNMP traps sent by the Windows Cell Manager. To do this, use the Operations Manager GUI to select and distribute the DP_SNMP policy to the Operations Manager Server.

   The DP_SNMP policy is located in:

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

NOTE:

To check whether SNMP is been configured or not , on the OMW server GUI, right-click on the node **Select View -> Hosting service list**. SNMP traps should be displayed in the list.



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

Uninstalling the Data Protector Integration

You need to remove components from:

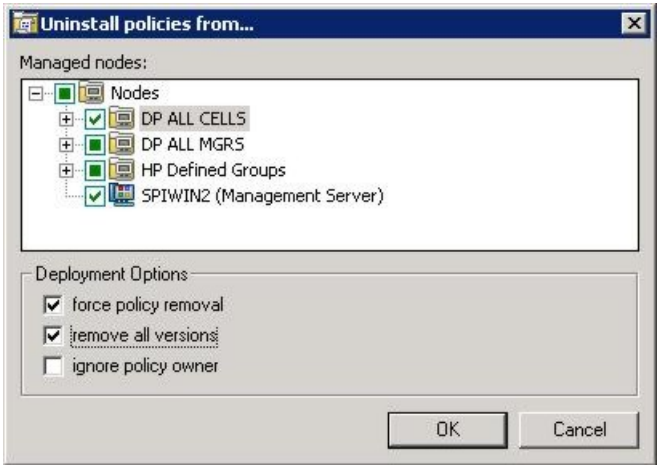
- Managed node systems (Data Protector Cell Manager)
- HP Operations Manager Server system

Uninstalling from managed nodes

Undeploying all Data Protector policies from managed nodes

1. Select `Policy management\Policy groups\SPI for DataProtector`, right-click and select **All Tasks -> Uninstall from ...** from the pop-up menu.

   The **Uninstall policies from ...** window is displayed.



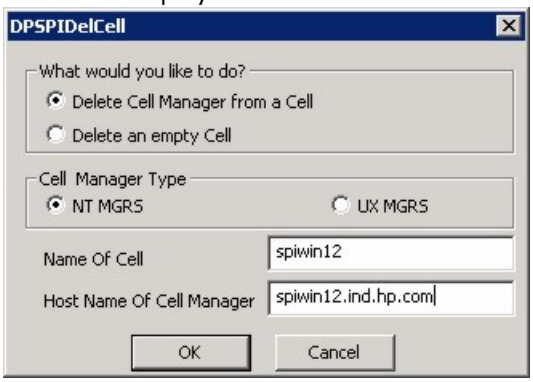
2. Mark the `DP ALL MGRS` node entry.
3. Click on **force policy removal** and **remove all versions** (in the case of OMW 8.1).
4. Click **OK**.

Uninstalling from HP Operations Manager Server

Removing the Data Protector Cell Manager node from the Operations Manager Server

You can use the Delete DP Cell tool to remove managed nodes from the Operations Manager Server managed environment:

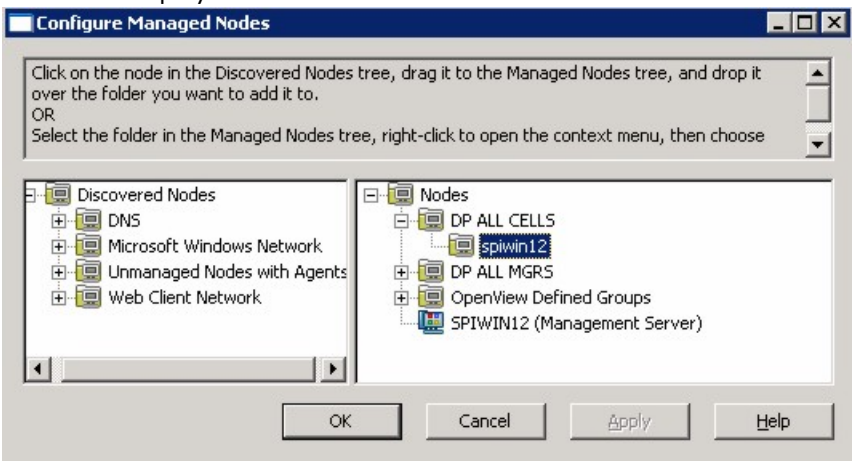
1. Select **Tools \ SPI for DataProtector \ DP_tools -> Del DP Cell**. The DPSPIDelDPCell window is displayed:



2. Enter the Data Protector Cell Manager name and select its OS type.
3. Click OK.

4. Remove the Cell Manager entry from DP ALL CELLS.

   Right-click on `Node`, select **Configure->Nodes**. The Configure Managed Nodes window is displayed:



   Under DP ALL CELLS, right-click on the `DP Cell Manager Node name` and select **Delete**. A Confirmation window pops up. Click OK.

NOTE:

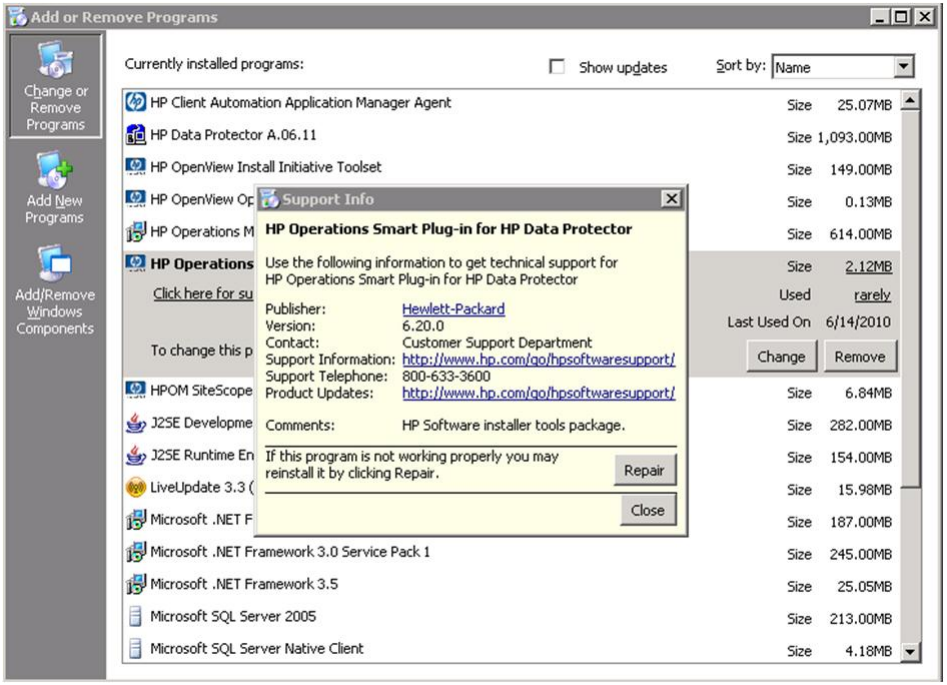
Before proceeding to the next step, make sure all the Data Protector Cell Manager Managed nodes are removed from the Operations Manager Server.

Removing the Data Protector integration

To remove the Data Protector Integration from the Operations Manager Server:

1. From the `Control Panel`, select **Add/Remove Programs**.

   The **Add/Remove Programs** window is displayed:



2. In the **Add/Remove Programs** window, scroll down until you find the `HP Operations Smart Plug-in for HP Data Protector` entry.
3. Click **Remove** to start the removal. This will take a short time.

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

NOTE:

When uninstalling Data Protector Integration from a cluster node, make sure that the first cluster node is uninstalled last. All other nodes can be uninstalled in any order.

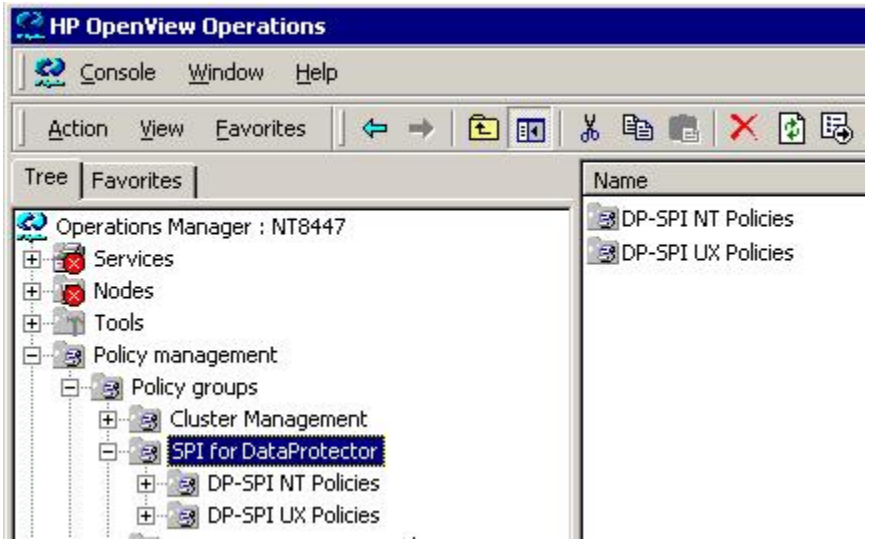
3 Using the Data Protector Integration

In this chapter

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

Data Protector SPI policies

The Data Protector Integration adds the `SPI for DataProtector` policy group to Operations Manager:



The `SPI for DataProtector` policy group contains:

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

Both are assigned by default to the `DP UX MGRS` node group for automatic deployment to any node added to this node group.

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

Message groups

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

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

Where appropriate, the integration assigns relevant messages to existing 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 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 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 log file set this parameter to the name of the log file. • 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 **Nodes** tab/context in the OM window. Open a node group to view all systems within it. A system may belong to more than one node group.

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

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

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

- The user responsibilities
- The messages the user sees in the message browser

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

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

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

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

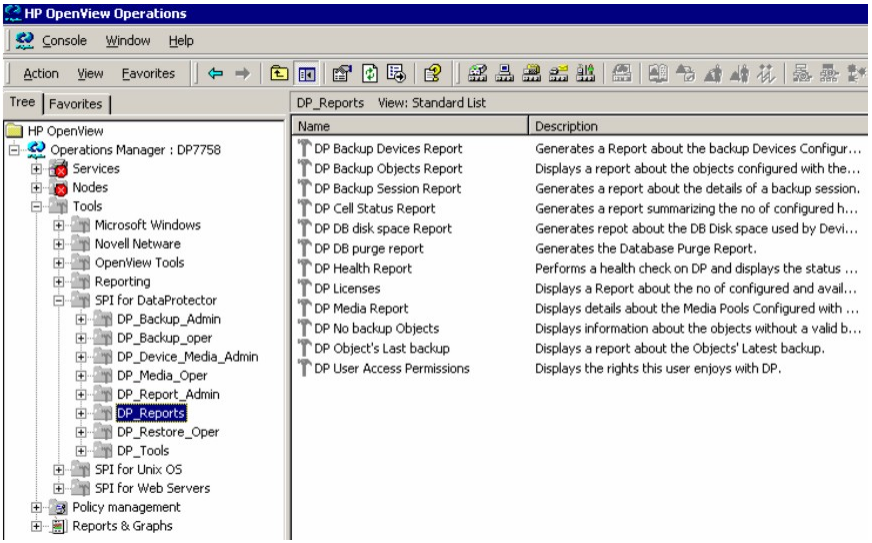
These can be used by any Operations Manager administrator to help assign and distribute policies and monitors to all nodes of a selected operating system. If the cell

administrator uses the `Add Data Protector Cell` application to create a new node, the node is automatically placed in the node group corresponding to its operating system.

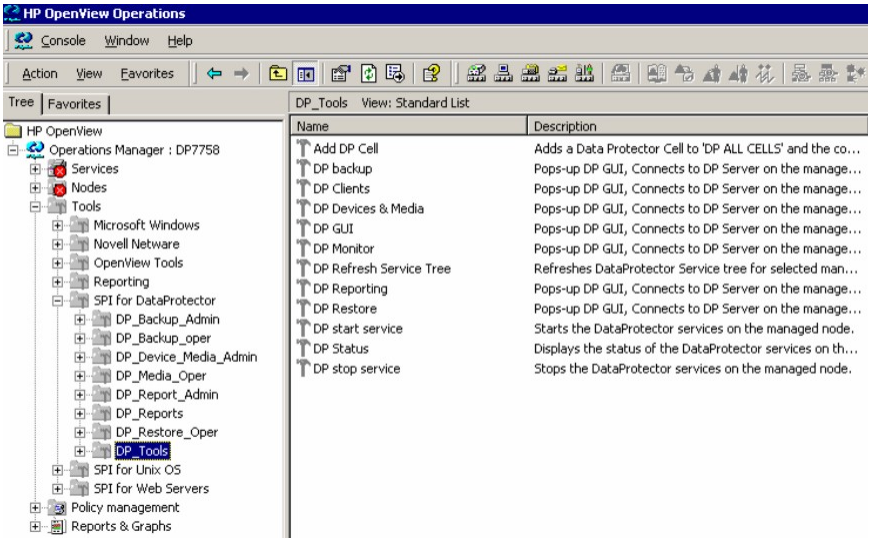
Tools groups

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

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



- `DPSPI`, containing applications used to manage the Data Protector environment:



Using tools and reports

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

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

Examples

DP GUI: Invokes the Data Protector GUI by starting the Data Protector Console on the Operations Manager Server. The Data Protector Console connects through port 5555 to the selected Data Protector Cell Manager.

DP Cell Status report: Starts `omnicellinfo` remotely on the Operations Manager Managed Node/Data Protector Cell Manager.

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

Data Protector service tree

Data Protector is represented as a service tree with each cell an icon. The tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from Data Protector Integration monitors. Figure 4 illustrates the `HP_Data Protector` service tree consisting of a sub-tree for the `Cell Manager:nt8446` Data Protector Cell Manager.

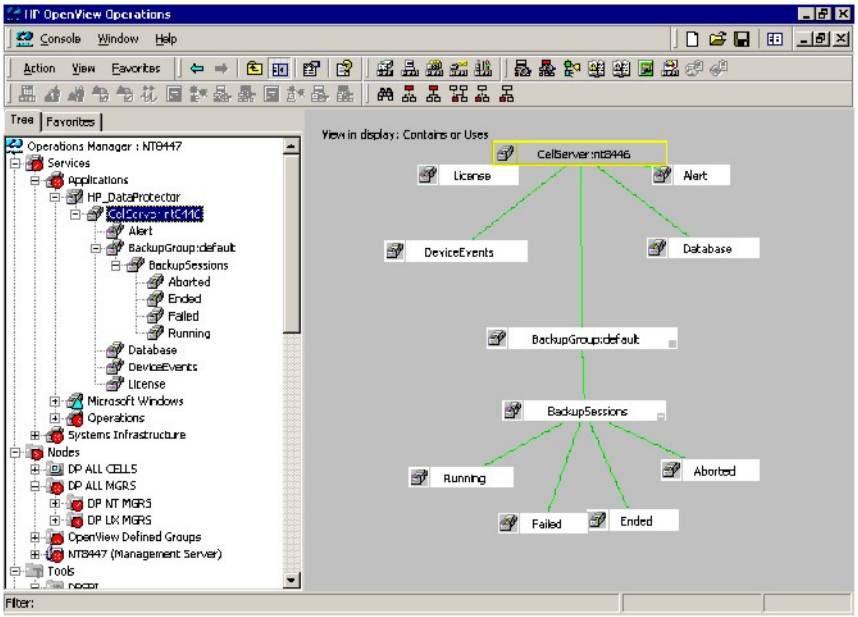
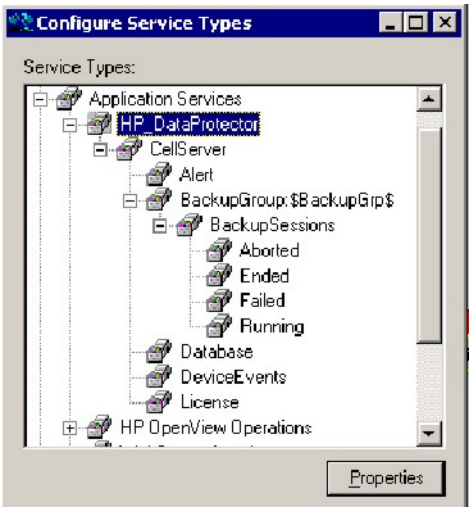


Figure 4 The Data Protector service tree

The service tree for Data Protector Cell Managers is automatically created after the `Add DP Cell` tool is run and the `DP_Service_Discovery` policy is automatically deployed to the Cell Manager.

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



The following service tree nodes are available for each cell:

Table 3 Cell service tree nodes

Node	Description
`backup group. Backup Sessions`	Contains `Running`, `Waiting`, `Aborted`, `Failed`, `Completed`, `Completed with Failures`, and `Completed with Errors`. Data Protector sends SNMP traps to trigger the update of these items.
`Running`	Updated by `Start of Session` SNMP trap issued by Data Protector notification.
`Waiting`	Updated by messages indicating that session is waiting because: • the device is occupied • the database is in use • all licenses are currently allocated • too many backup sessions are running in parallel
`Aborted`	Updated by Session Aborted trap.
`Failed`	Updated by Session Failed SNMP trap.

Node	Description
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 log file monitoring.
Device Events	Updated by Device Error-, Mount Request-, Mail Slots-, and Full- SNMP traps issued by Data Protector notification.
Alert	Updated by Alarm-, Health Check Failed-, User Check Failed-, Unexpected Events-, Not Enough Media- SNMP traps issued by Data Protector notification.
License	Updated by License trap

Users and user roles

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

Data Protector and operating system users

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

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

- **Data Protector User Group**

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

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

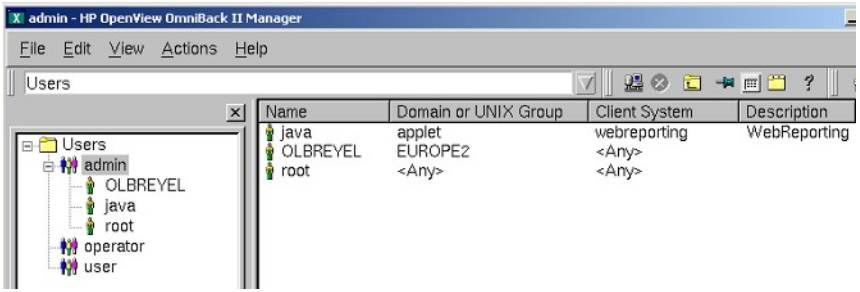


Figure 5 Windows users

Data Protector Integration users

The operating system user is required by the Data Protector Integration. The integration adds seven new user roles to the `OM User Roles` configuration. For details, see "Data Protector OVO user roles" on page 51. The role determines the layout of the Operations Manager GUI:

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

NOTE:

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

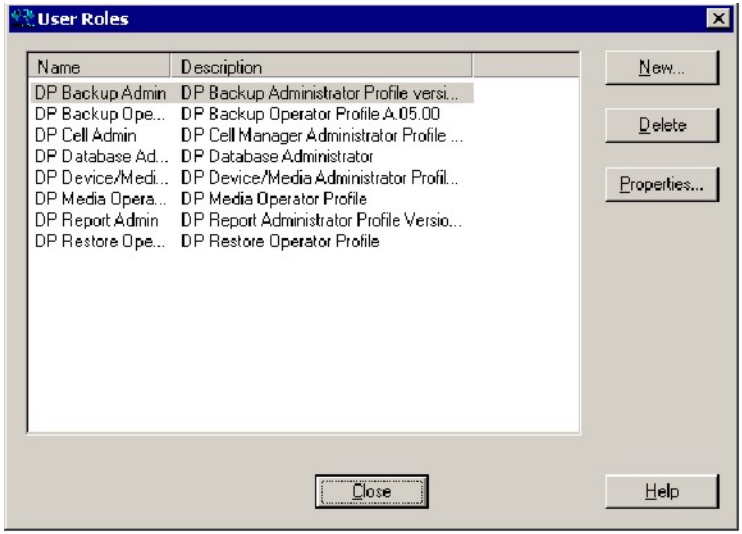
Operations Manager user roles

Operations Manager uses User Roles 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 roles suitable for use with different Operations Manager-Data Protector operator roles.

Data Protector Operations Manager user roles

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



Each of these roles defines a custom subset of tools and a unique combination of the `DP ALL MGRS` node group with `DP_*` message groups. This defines the responsibilities of a user and the tools available to him. The roles can be used to implement the Operations Manager user roles described in "Data Protector OVO operators" on page 53.

DP Backup Admin	Restricted to a Data Protector Cell. *Tool Groups:* • `DP_Backup_Admin` • `DP_Reports` Can access messages in the Operations Manager Message Browser, if the Operations Manager message policy for detailed messages `DP_Detailed` is enabled.
DP Backup Operator	Restricted to a Data Protector Cell. *Tool Groups:* `DP_Backup_Oper` *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. *Tool Groups:* `DP_Restore_Oper` *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. *Tool Groups:* `DP_Device_Media_Admin` Can access messages in the Operations Manager Message Browser, if the Operations Manager message policy for detailed messages `DP_Detailed` is enabled.
DP Media Operator	Restricted to a Data Protector Cell. *Tool Groups:* `DP_Media_Oper` *Messages:* Mount requests of backup and restore sessions (`DP_Mount`) messages.

DP Cell Administrator	Restricted to clients of Data Protector Cells. *Tool Groups:* • `DP_Reports` • `DP_Tools` *Message Groups:* • `DP_Misc` • `DP_SPI`
DP Report Administrator	Restricted to a Data Protector Cell. *Tool Groups:* `DP_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 4 defines roles for Data Protector Operations Manager operators and describes their access rights.

NOTE:

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

Operations Manager users are not created by the Data Protector integration. The roles described in Table 4 are examples of possible roles you may create and use to manage Data Protector.

Table 4 Data Protector Operations Manager operators and their roles

Role	Data Protector Privileges	Description
Backup Administrator	Create backup specifications (what to back up, from which system, to which device) and schedule the backup.	
	Save backup specification	You can create, schedule, modify and save personal backup specifications.

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

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

Role	Data Protector Privileges	Description
Cell Administrator	Instals and update Data Protector client systems, add, delete, or modify Data Protector users and groups, and administer the Data Protector database.	
	Client configuration	You can install and update client systems.
	User configuration	You can add, delete and modify users or user groups. *Note:* This is a powerful right.
	Monitor	You can view information about any active session in the cell, and access the Data Protector database to view past sessions. You can use the Data Protector database context.
	See private object	You can see private objects. Database administrators require this right.
Report Administrator	Create and modify Data Protector reports.	
	Reporting and notifications	You can create Data Protector reports. To use Web Reporting, you also need a Java user under applet domain in the admin user group.

Monitored objects

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 minutes

Message structure:

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

Databases

Checks amount and percentage of used available space.

Threshold: ≥95% for error, ≥80% for warning

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

Polling interval: 60 minutes

Message structure:

Message Group	`DP_Misc`

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

NOTE:

The usage of this monitor program is as follows:

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

UNIX: `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 - 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 minutes

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:* `DP_CheckPoolStatus_NT` *UNIX:* `DP_CheckPoolStatus_UX`
Operator Action in case of problem	Status of the Media Pool
Message Text when problem solved	Auto-acknowledge this message and the preceding problem message

Media pool size

Checks the amount of used space:

Threshold: ≥95% of total available space is Critical, ≥85% of total available space is Warning

Command: `omnimm -list_pool -detail`

Polling interval: 60 minutes

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:* `DP_CheckPoolSize_NT` *UNIX:* `DP_CheckPoolSize_UX`

Operator Action in case of problem	Status of the Media Pool
Message Text when problem solved	Auto-acknowledge this message and the preceding problem message

Monitor status of long running backup sessions

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

- 12 minutes (Critical)
- 8 minutes (Warning)

Polling interval: 60 minutes

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:* `DP_CheckLongBackup_NT` *UNIX:* `DP_CheckLongBackup_UX`
Automatic Action in case of problem	Session status
Operator Action in case of problem	Session report
Message Text when problem solved	Auto-acknowledge this message and the preceding problem message

Check important configuration files

Windows nodes: `OB_CheckFile_NT` starts `ob_spi_file.pl`

UNIX nodes: `OB_CheckFile_UX` starts `ob_spi_file.pl`

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 6.0 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`
- `Config\client\cell_server`
- `Client\omni_format`
- `Client\omni_info`

Polling interval: 15 minutes

The value for *`OBHOME`* is read by `ob_spi_file.pl` from the registry key:

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

UNIX systems

Checks if the following files exist:

For Data Protector 6.0 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_format
- /etc/opt/omni/client/omni_info

Polling interval: 15 minutes

Changing monitor parameters

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

The location of the file is:

Windows: `OvAgentDir\bin\instrumentation`

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

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

Windows:

```
[DP_CheckServerFile]
\Config\client\cell_info
\Config\client\installation_servers
\Config\server\users\userlist
\Config\server\users\classspec
\Config\server\users\webaccess
\Config\server\SNMP\OVdests
\Config\server\SNMP\OVfilter
\Config\server\Options\global
\Config\server\Options\trace
\Config\client\cell_server
[DP_CheckClientFile]
\Config\client\omni_format
\Config\client\omni_info

[DP_CheckProc]
rds.exe crs.exe
mmd.exe
```

```
uiproxy.exe

[DP_CheckProc_60]
rds
crs
mmd

[DP_CheckLongBackup
critical=12:00
warning=08:00
```

UNIX:

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

[DP_CheckClientFile]
/etc/opt/omni/client/omni_info
/etc/opt/omni/client/omni_format
[DP_CheckProc]
rds
crs
mmd
uiproxy

[DP_CheckProc_60]
rds
crs
mmd

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

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

Monitored log files

You can use Operations Manager to monitor applications by observing their log files. You can suppress log file 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 Operations Manager documentation (see http://www.hp.com/support/manuals) and online help.

Four Data Protector log files are monitored for warning and error patterns. Basic information is provided in the *HP Data Protector Troubleshooting Guide*.

Data Protector default log files

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

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

omnisv.log

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

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

Parameters for messages for the default log files are:

Message Group	`DP_Misc`
Applications	`Data Protector`
Note	`name_system`on which log file 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

```
2001-6-13 7:46:40 -STOP

HP Data Protector services successfully stopped.

2001-6-13 7:46:47 -START

HP Data Protector services successfully started.
```

inet.log

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

Examples

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

UNIX inet.log

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

Windows inet.log

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

OmniInet service was teminated.
```

Data Protector database log file

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

purge.log

Contains purge session messages. Purge sessions are used to clean up the database. The data/time format depends on the value of the language environment variable.

Examples

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

Parameters for messages in the default log files are:

Message Group	`DP_Misc`
Applications	`Data Protector`
Note	`name_system`on which log file 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`

Log files not monitored by Data Protector Integration

The following log files either do not provide information relevant to the correct operation of Data Protector or the information is extracted from other sources, such as SNMP traps.

`debug.log`	Exception messages that have not been handled.
`RDS.log`	Raima Database service messages.
`readascii.log`	Messages generated when the database is read from a file using `readascii`.
`writeascii.log`	Messages generated when the database is written to a file with `writeascii`.

`lic.log`	Unexpected licensing events.
`sm.log`	Detailed errors during backup or restore sessions, such as errors while parsing the backup specification. No message catalog is used. The time/date format depends on the language environment variable.

Managing cluster-aware applications

Clustered fail-over environments

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

When you configure the Data Protector 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, Data Protector 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 Data Protector SPI setup for a cluster environment requires that you do the following:

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

Modifying `dpspi.apm.xml`

The Data Protector 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. The purpose of the file is to list all the Data Protector 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 Data-Protector\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 Data Protector 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 Data Protector 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 Data Protector SPI, you would enter `dpspi`, as shown below). Enter the Instance Name to match the instance name entered in the Data Protector 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 Data Protector 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
```

Data Protector SPI policies will be enabled only on the active node.

4 Troubleshooting

Following are the issues in the HP Data Protector Integration:

- HP Data Protector events not arriving on the HPOM message browser
- HP Data Protector services not visible in the HPOM Console
- Auto-deployment of policies failing on HPOM 8.10

HP Data Protector events not arriving on the HPOM message browser

Symptom: No HP Data Protector events arriving in the HPOM message browser.

Action: To resolve the issue, complete the following steps:

1. Ensure that the connection between HPOM and the HP Data Protector CM is up and running.
2. Send a test message from the Data Protector CM and ensure that it can be received in the HPOM Message Browser. You can send a test message using the command `opcmsg` on the managed node.
3. Ensure that the HP Data Protector services are running on the HP Data Protector CM node. Use `omnisv -status` command.
4. Verify that the HPOM agent is correctly installed and configured on the HP Data Protector CM server and that HPOM agent processes (and in particular the control agent) are running.
5. Ensure that you have followed all the configuration steps in the order specified in Installing the Data Protector integration
6. Ensure that the HP Data Protector Integration policies are correctly deployed to the HP Data Protector CM Agent nodes.
7. Ensure that HP Data Protector CM Agent nodes are added to the appropriate node groups. For more information, see Node Groups.
8. Check the `dpspiInstall.log` created at the *`OM_INSTALL_DIR`* to make sure that there are no errors during installation and configuration.

9. Make sure the dpspi instrumentation binaries are deployed at the Data Protector CM at the *OM_AGENT_INSTRUMENTATION_DIR*.

HP Data Protector services not visible in the HPOM Console

Symptom: HP Data Protector services are not visible in the HPOM Console.

Action: Ensure that the Service Discovery policies in the policy groups from **Policy Management > Policy Groups > SPI for DataProtector > DPSPI NT POLICIES > DP_Service_Discovery** is deployed on the HP Data Protector CM node. To check that the policies are correctly deployed, right-click on the node and select **View > Policy Inventory** and ensure that the Service Discovery policy is present. You can also check the service discovery log at `OvAgentDir\log\javaagent.log` on the HP Data Protector CM node for error messages.

Auto-deployment of policies failing on HPOM 8.10

Symptom: Auto-deployment of policies failing on HPOM 8.10.

Action: Select **OVO Console Operations Manager Nodes Server Configuration Utility Name Space Policy Management and Deployment Disable autodeployment for all nodes and services** and set the value to **False**.

Index

P

R

S

T

U

V

W