HP OpenView Storage Data Protector

Integration Guide for HP OpenView Operations for UNIX

Version: A.05.01

HP-UX, Solaris and Windows

Manufacturing Part Number: B6960-90089

April 2003

Legal Notices

Warranty.

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

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20, HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Contents

Contents

Contents

Contents

Contents

Contents

Printing History

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

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

Table 1 **Edition History**

Part Number	Manual Edition	Product
N.A.	November 2001	HP OpenView Omniback II A.04.10
B6960-90068	July 2002	HP OpenView Storage Data Protector A.05.00
B6960-90089	April 2003	HP OpenView Storage Data Protector A.05.10

Conventions

The following typographical conventions are used in this manual.

Table 2 **Typographical Conventions**

Convention	Meaning	Example
Italic	Book or manual titles, and manual page names	Refer to the *HP OpenView Storage Data Protector Integration Guide* for more information.
	Provides emphasis	You *must* follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: `rlogin` *`your_name`* where you supply your login name.
Bold	New terms	The Data Protector **Cell Manager** is the main ...
`Computer`	Text and items on the computer screen	The system replies: `Press Enter`
	Command names	Use the `grep` command ...
	File and directory names	`/usr/bin/X11`
	Process names	Check to see if `Data Protector Inet` is running.
	Window/dialog box names	In the `Backup Options` dialog box...
`Computer Bold`	Text that you must enter	At the prompt, type: **`ls -l`**

Table 2 **Typographical Conventions (Continued)**

Convention	Meaning	Example
Keycap	Keyboard keys and Buttons on the user interface.	Press **Return** Click **Operator** Click the **Apply** button
Menu Items	A menu name followed by a colon (:) means select the menu, then the item. When the item is followed by an arrow (→), a cascading menu follows.	Select **Actions:**→**Utilities**→ **Reports**…

1 Introduction

This chapter provides an overview of:

- HP OpenView Storage Data Protector
- HP OpenView Operations
- HP OpenView Storage Data Protector Integration

If you are familiar with HP OpenView Storage Data Protector and HP OpenView Operations you may chose to skip these sections.

The section entitled “What is the Data Protector Integration?” on page 44 provides a short overview of this product, its key features and its architecture.

About Data Protector

HP OpenView Storage Data Protector is a backup solution that provides reliable data protection and high accessibility for your fast growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. The following list describes major Data Protector features:

- **Scalable and Highly Flexible Architecture**

  Data Protector can be used in environments ranging from a single system to thousands of systems on several sites. Due to the network component concept of Data Protector, elements of the backup infrastructure can be placed in the topology according to user requirements. The numerous backup options and alternatives to setting up a backup infrastructure allow the implementation of virtually any configuration you want.

- **Easy Central Administration**

  Through its easy-to-use graphical user interface (GUI), Data Protector allows you to administer your complete backup environment from a single system. To ease operation, the GUI can be installed on various systems to allow multiple administrators to access Data Protector via their locally installed consoles. Even multiple backup environments can be managed from a single system. The Data Protector command-line interface allows you to manage Data Protector using scripts.

- **High Performance Backup**

  Data Protector allows you to back up to several hundred backup devices simultaneously. It supports high-end devices in very large libraries. Various types of backups, such as local, network, full, differential, leveled incremental, online, disk image, and built-in support of parallel data streams, allow you to tune your backups to best fit your requirements.

- **Supporting Mixed Environments**

  As Data Protector supports heterogeneous environments, most features are common to the UNIX and Windows platforms. The HP-UX, Solaris and Windows Cell Managers can control all

supported client platforms (UNIX, Windows NT, Windows 2000, Windows XP Professional, Windows Server 2003, and Novell NetWare). The Data Protector user interface can access the entire Data Protector functionality on all supported platforms.

- **Easy Installation for Mixed Environments**

  The Installation Server concept simplifies the installation and upgrade procedures. To remotely install UNIX clients, you need an Installation Server running HP-UX or Solaris. To remotely install Windows clients, you need an Installation Server running Windows NT, Windows 2000, Windows XP Professional, or Windows .Net. The remote installation can be performed from any client with an installed Data Protector GUI.

- **High Availability Support**

  Data Protector enables you to meet the needs for continued business operations around the clock. In today's globally distributed business environment, company-wide information resources and customer service applications must always be available. Data Protector enables you to meet high availability needs by:

  - ❏ Integrating with clusters (HP-MC/ServiceGuard and Microsoft Cluster Server) to ensure fail-safe operation with the ability to back up virtual nodes.
  - ❏ Enabling the Data Protector Cell Manager itself to run on a cluster.
  - ❏ Supporting all popular online database Application Programming Interfaces.
  - ❏ Integrating with advanced high availability solutions like HP StorageWorks Disk Array XP, HP StorageWorks Virtual Array or EMC Symmetrix.
  - ❏ Providing various disaster recovery methods for supported Windows and UNIX platforms.

- **Easy Restore**

  Data Protector includes an internal database that keeps track of data such as which files from which system are kept on a particular medium. In order to restore any part of a system, browse the files and directories. This provides fast and convenient access to the data to be restored.

- **Automated or Unattended Operation**

  With the internal database, Data Protector keeps information about each Data Protector medium and the data on it. Data Protector provides sophisticated media management functionality. For example, it keeps track of how long a particular backup needs to remain available for restoring, and which media can be (re)used for backups.

  The support of very large libraries complements this, allowing for unattended operation over several days or weeks (automated media rotation).

  Additionally, when new disks are connected to systems, Data Protector can automatically detect (or discover) the disks and back them up. This eliminates the need to adjust backup configurations manually.

- **Service Management**

  Data Protector is the first backup and restore management solution to support service management. The integration with Application Response Management (ARM) and Data Source Integration (DSI) enables powerful support of Service Level Management (SLM) and Service Level Agreements (SLA) concepts by providing relevant data to management and planning systems.

  The DSI integration provides a set of scripts and configuration files from which users are able to see how to add their own queries using Data Protector reporting capabilities.

- **Monitoring, Reporting and Notification**

  Superior web reporting and notification capabilities allow you to easily view the backup status, monitor active backup operations, and customize reports. Reports can be generated using the GUI, or using the `omnirpt` command on systems running UNIX, Windows NT, Windows 2000, Windows XP Professional, or Microsoft Windows Server 2003 as well as using Java-based online generated web reports.

  You can schedule reports to be issued at a specific time or to be attached to a predefined set of events, such as the end of a backup session or a mount request.

- **Integration with Online Database Applications**

  Data Protector provides online backup of Microsoft Exchange Server 5.5, Microsoft Exchange Server 2000, Microsoft SQL Server 7, Microsoft SQL Server 2000, Oracle7, Oracle8, Informix, SAP R/3, Lotus Domino R5 Server, and Sybase database objects.

- **Integration with Other Products**

  Additionally, Data Protector integrates with EMC SRDF and TimeFinder, HP OpenView Operations for UNIX, Microsoft Cluster Server, MC/ServiceGuard, HP OpenView OmniStorage, and other products.

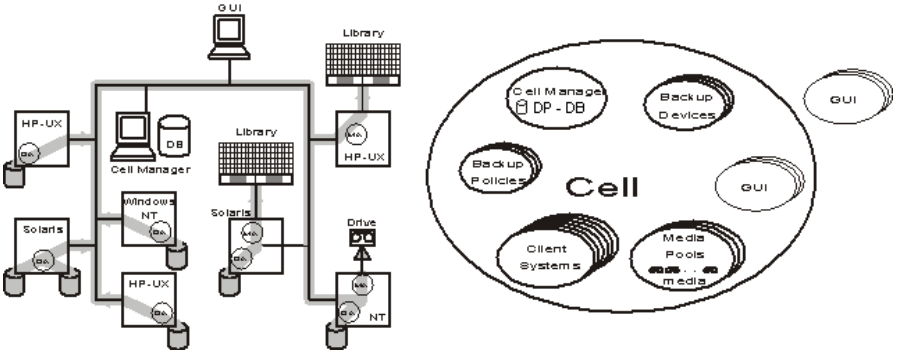
Data Protector Architecture

The Data Protector **cell,** shown in Figure 1-1, is a network environment that has a **Cell Manager**, **client systems**, and **devices**. The Cell Manager is the central control point where Data Protector software is installed. After installing Data Protector software, you can add systems to be backed up. These systems become Data Protector client systems that are part of the cell. When Data Protector backs up files, it saves them to media in backup devices.

The **Data Protector Internal Database (IDB)** keeps track of the files you back up so that you can browse and easily recover the entire system or single files.

Data Protector facilitates backup and restore jobs. You can do an immediate (or interactive) backup using the Data Protector user interface. You can also schedule your backups to run unattended.

Figure 1-1 **The Data Protector Cell (Physical View and Logical View)**



NOTE The GUI and the Cell Manager systems can run on HP-UX, Solaris Windows NT, Windows 2000, Windows XP Professional, or Microsoft Windows Server 2003 operating systems; they do not have to run the same operating system.

Cell Manager

The Cell Manager is the main system in the cell. The Cell Manager:

- Manages the cell from a central point.
- Contains the IDB.

  The IDB contains information about backup details such as, backup durations, media IDs, and session IDs.
- Runs core Data Protector software.
- Runs Session Managers that start and stop backup and restore sessions and write session information to the IDB.

Systems to Be Backed Up

Client systems you want to back up must have the Data Protector **Disk Agent** ((DA) also called Backup Agent) installed. To back up online database integrations, install the **Application Agent**. In the rest of the manual, the term Disk Agent will be used for both agents. The Disk Agent reads or writes data from a disk on the system and sends or receives data from the Media Agent. The Disk Agent is also installed on the Cell Manager, thus allowing you to back up data on the Cell Manager, the Data Protector configuration, and the IDB.

Systems with Backup Devices

Client systems with connected backup devices must have the Data Protector Media Agent (MA) installed. Such client systems are also called **Drive Servers**. A backup device can be connected to any system and not only to the Cell Manager. The Media Agent reads or writes data from media in the device and sends or receives data from the Disk Agent.

Systems with a User Interface

You can manage Data Protector from any system on the network on which the Data Protector graphical user interface (GUI) is installed. Therefore, you can have the Cell Manager system in a computer room while managing Data Protector from your desktop system.

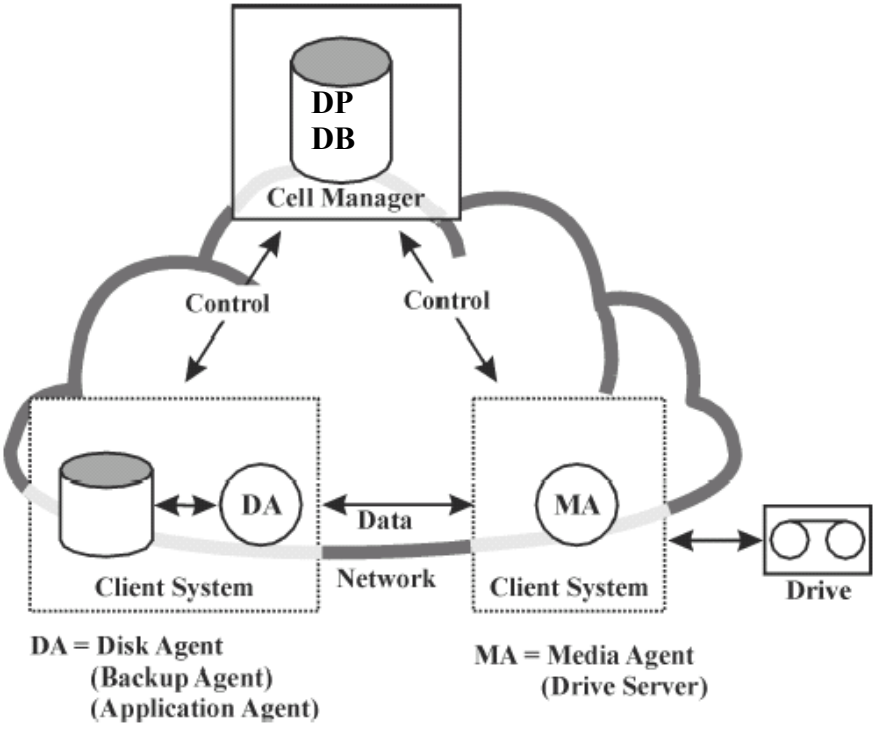
Installation Server

The **Installation Server** holds a repository of the Data Protector software packages for a specific architecture. The Cell Manager is by default also an Installation Server. At least two Installation Servers are needed for mixed environments: one for UNIX systems and one for the Windows systems.

Operations in the Cell

The Data Protector Cell Manager controls backup and restore sessions, which perform all the required actions for a backup or restore, respectively, as shown in Figure 1-2.

Figure 1-2 Backup or Restore Operation



Backup Sessions

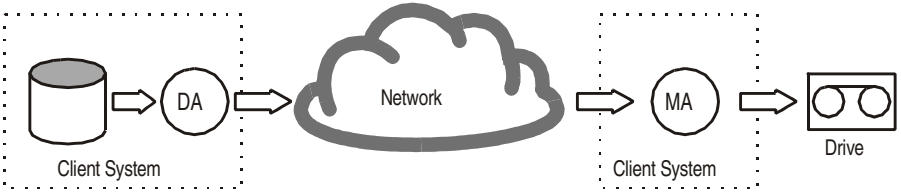
What Is a Backup Session?

A backup session, shown in Figure 1-3, is a process that creates a copy of data on storage media. It is started either interactively by an operator using the Data Protector user interface, or unattended using the Data Protector Scheduler.

How Does It Work?

The Backup Session Manager process starts Media Agent(s) and Disk Agent(s), controls the session, and stores generated messages to the IDB. Data is read by the Disk Agent and sent to the Media Agent, which saves it to media.

Figure 1-3 Backup Session



A typical backup session is more complex than the one shown in Figure 1-3. A number of Disk Agents read data from multiple disks in parallel and send data to one or more Media Agents. For more information on complex backup sessions, refer to the *HP OpenView Storage* Data Protector *Administrator's Guide*.

Restore Sessions

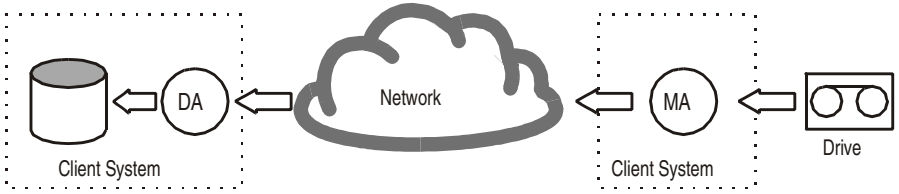
What Is a Restore Session?

A restore session, shown in Figure 1-4, is a process that restores data from previous backups to a disk. The restore session is interactively started by an operator using the Data Protector user interface.

How Does It Work?

After you have selected the files to be restored from a previous backup, you invoke the actual restore. The Restore Session Manager process starts the needed Media Agent(s) and Disk Agent(s), controls the session, and stores messages in the IDB. Data is read by the Media Agent and sent to the Disk Agent, which writes it to disks.

Figure 1-4 Restore Session



A restore session may be more complex than the one shown in Figure 1-4. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* for more information on restore sessions.

Data Protector Enterprise Environments

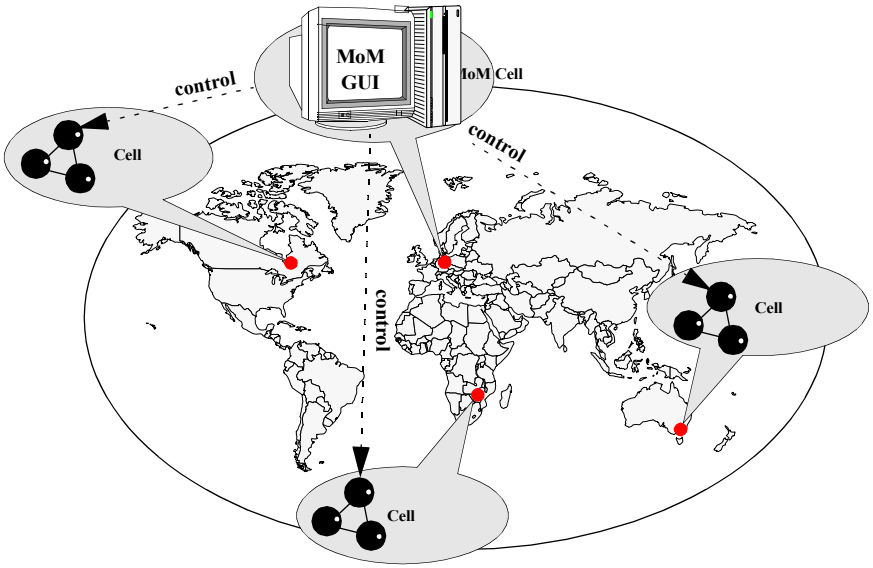
What Is an Enterprise Environment?

A typical enterprise network environment, shown in Figure 1-8, consists of a number of systems from different vendors with different operating systems. The systems may be located in different geographical areas and time zones. All the systems are connected with LAN or WAN networks operating at various communication speeds.

When to Use an Enterprise Environment?

This solution can be used when several geographically separated sites require common backup policies to be used. It can also be used when all departments at the same site want to share the same set of backup devices.

Figure 1-5 **Large Data Protector Enterprise Environment**



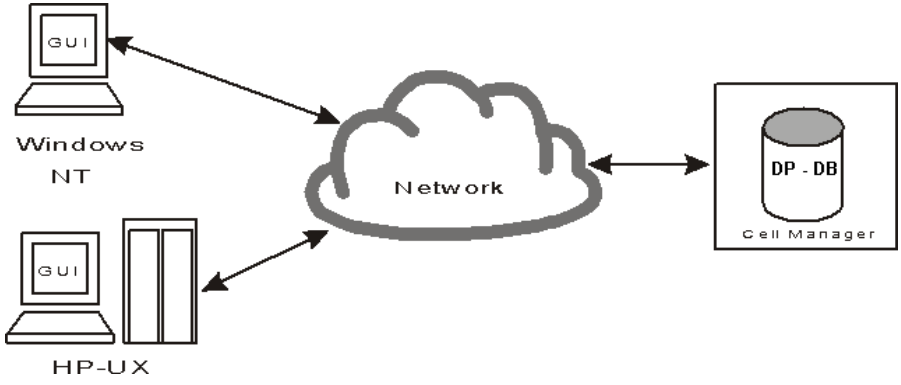
Configuring and managing backups of such a heterogeneous environment is challenging. Data Protector functionality has been designed to highly simplify this task.

User Interfaces

Data Protector provides easy access to all configuration and administration tasks using the Data Protector GUI provided to run under X11/Motif on UNIX platforms and on the Windows platforms. Additionally, a command-line interface is available on UNIX and Windows platforms.

The Data Protector architecture allows you to flexibly install and use the Data Protector user interface. The user interface does not have to be used from the Cell Manager system; you can install it on your desktop system. As depicted in Figure 1-12, the user interface also allows you to transparently manage Data Protector cells with HP-UX, Solaris or Windows Cell Managers.

Figure 1-6 **Using the Data Protector User Interface**



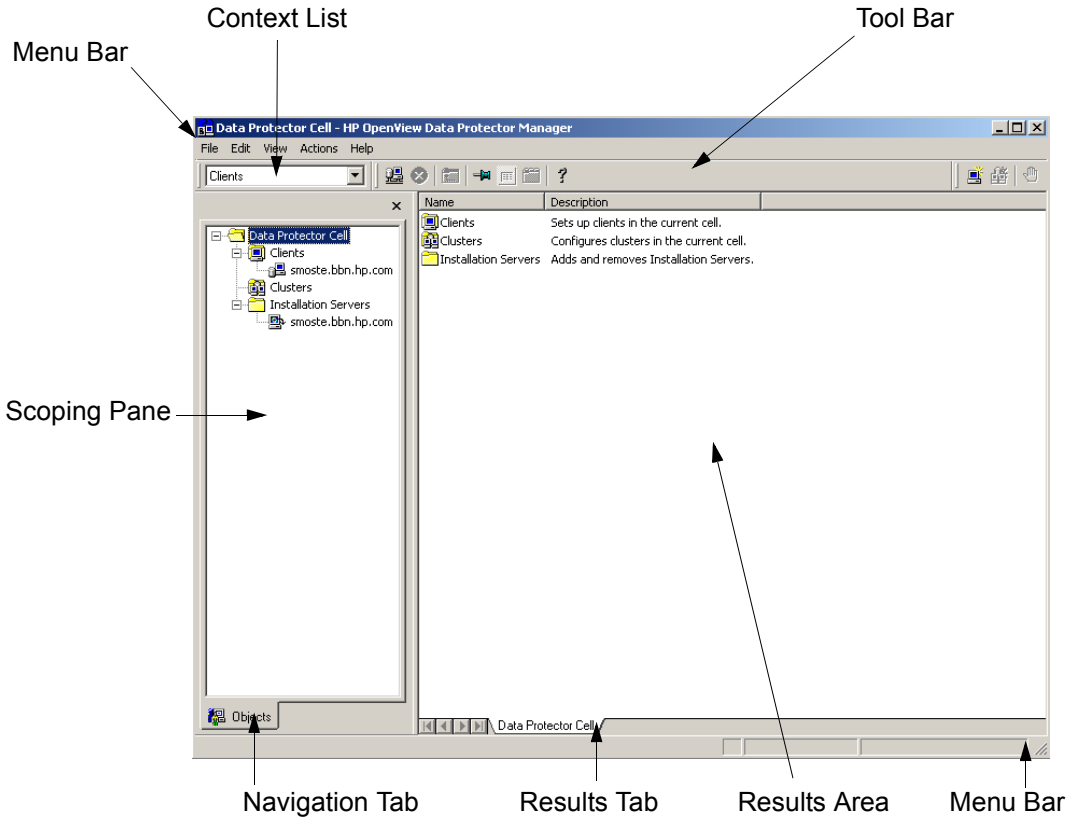
TIP In a typical mixed environment, install the Data Protector user interface on several systems in the environment, thus providing access to Data Protector from several systems.

Data Protector GUI

The Data Protector User Interface is an easy-to-use, powerful graphical user interface. It provides the following main functionality:

- A Results Tab with all the configuration wizards, properties and lists.
- Easy configuration and management of the backup of online database applications that run in Windows environments, such as Microsoft SQL 7, Microsoft Exchange 2000, SAP R/3, and Oracle8 or that run in the UNIX environments, such as SAP R/3, Oracle8, and Informix.
- A context-sensitive online Help system called the Help Navigator

Figure 1-7 Graphical User Interface



About HP OpenView Operations

The following sections introduce the main concepts behind HP OpenView Operations (OVO), and answers the questions:

- What Is OVO?
- What Is a Management Server?
- What Is a Managed Node?
- What Does OVO Do?
- How Does OVO Work?
- OVO User Concept

What Is OVO?

OVO is a distributed client/server software solution designed to help system administrators detect, solve, and prevent problems occuring in networks, systems, and applications in any enterprise. It is a scalable and flexible solution that can be configured to meet the requirements of any IT organization and its users. In addition, you can expand the applications of OVO by integrating management applications from HP OpenView partners or other vendors.

OVO helps you to:

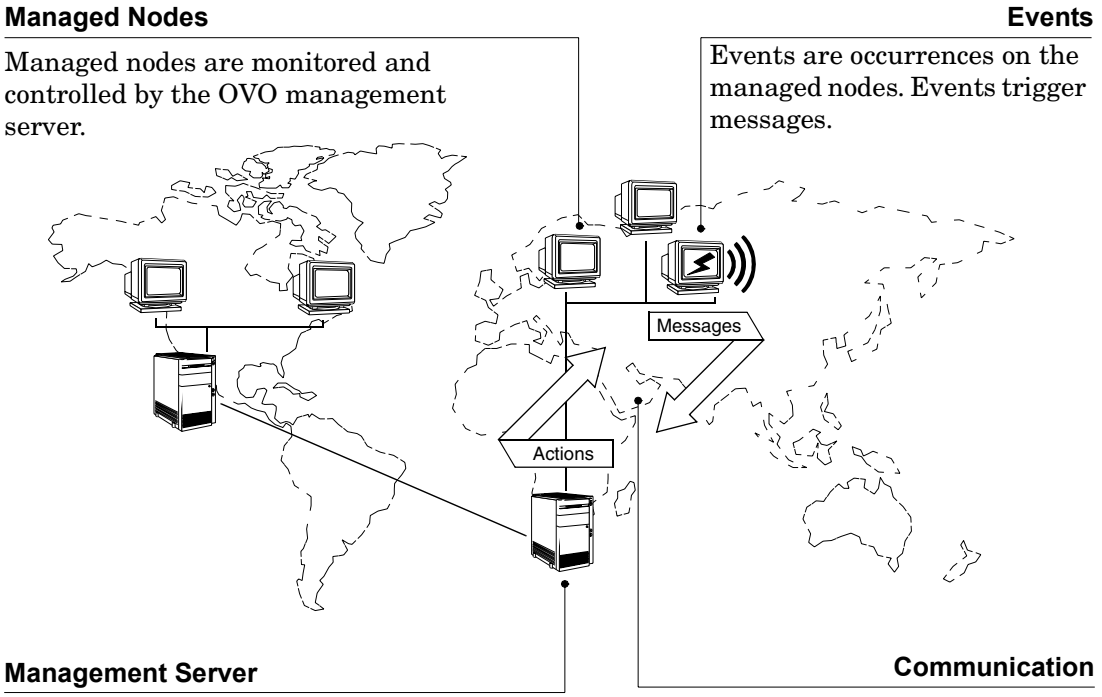
- Maximize the availability of network components.
- Reduce the time lost by end-users as a result of system down-time.
- Reduce user interactions by automatically solving problems.
- Reduce the amount of problems through preventive actions.
- Decrease the time needed to resolve problems.
- Reduce the cost of managing the client-server environment.

The OVO management concept is based on communication between a management server and managed nodes. Management server processes running on the central management server communicate with OVO agent processes running on managed nodes throughout the environment. The OVO agent processes collect and process events on the managed

nodes, and then forward relevant information in the form of OVO messages to the management server. The management server responds with actions to prevent or correct problems on the managed nodes.

Figure 1-8 on page 30 illustrates the management concept of OVO.

Figure 1-8 OVO Client-Server Concept



The agent on the management server also serves as the local managed node. A database serves as the central data repository for all messages and configuration data. You can use this runtime and historical data to generate reports. Historical data can also be helpful when creating

instruction text to help an operator solve problems caused by similar events, and to automate certain problem resolution processes. The database processes run on the management server.

What Is a Management Server?

The management server performs the central processing functions of OVO. It is on the management server that the entire software is stored, including the complete current configuration. The functions of a management server include:

- Collecting data from managed nodes.
- Managing and grouping messages.
- Calling the appropriate agent to:
  - ❏ start actions (local automatic actions started on a managed node).
  - ❏ initiate sessions on managed nodes (for example, open a virtual console).
- Controlling the history database for messages and performed actions.
- Forwarding messages: either to other management servers or to systems where OVO is running.
- Installing OVO agent software on managed nodes.

The management server also notifies the managed nodes about configuration changes and initiates any updates.

What Is a Managed Node?

Managed nodes are computers which are controlled and monitored by OVO via agent processes installed and running on them. The OVO agent software reads:

- Logfiles
- Console messages (MPE/iX)
- SNMP traps

The OVO message interceptor can intercept messages from any application running locally on the managed node.

Performance values are monitored at configurable intervals, and messages can be generated when performance varies from limits.

The agent compares all messages with conditions in preconfigured templates, then forwards unexpected or important messages to the management server. It can suppress duplicate or similar events. You determine your message filtering policy either by modifying existing templates, or configuring your own set of templates and conditions.

Corrective actions can be started locally on the managed node in response to a message, and can be restarted or stopped if necessary.

OVO can also monitor its own processes.

What Does OVO Do?

OVO helps you to solve problems occurring anywhere in your computing environment, including network elements, systems, and applications. OVO notifies you that a problem has occurred is likely to occur, and then provides the resources required to resolve or avoid it.

When a problem occurs at a managed node, it is registered in one of the following ways:

- A new entry in a logfile.
- An SNMP trap is sent.
- The node communicates directly with the management server via an application programming interface (API).

OVO examines error data and uses preconfigured conditions to decide whether to generate a message. If a message is required, OVO uses the error data to create a meaningful message text, attaches attributes to the message to provide additional information, and sends the complete message to the management server where it is displayed in the message browser.

The attributes of the message indicate to the user how severe the event is, on which managed node the event happened, and what triggered the message.

Depending on the type of action response configured for the event, the arrival of the message can trigger an automatic action executed immediately on the managed node, or might prompt a user to start an operator-initiated action.

How Does OVO Work?

The primary objectives of OVO are to monitor, control, and maintain systems in distributed heterogeneous environments. OVO performs these tasks by:

- Noting an occurrence (an event) in your environment.
- Generating a meaningful report (a message) about this event.
- Reacting with an appropriate response (an action) to this event.

OVO communicates changes in status, an event or a problem on a managed node via messages. If the event triggering the message represents a problem, an action can be started to correct it. The original message, the result of the corrective action, and other associated information for example user annotations, are stored in the database.

Events

An event is a fault or incident within the computing environment that occurs on an object. Typically, an event represents either a change in status or a threshold violation. For example, the status of a printer changes when the paper tray empties, and a threshold is violated when the available disk space on a system falls below a certain level. Each of these occurrences is an event, and for each event a message can be created.

Messages

A message is a structured, readable piece of information about a status, an event, or a problem related to a managed node.

OVO uses messages to:

- Communicate information about events.
- Highlight status changes within the environment.
- Initiate corrective actions.

OVO creates messages using information from OVO a variety of sources, including:

- **Logfiles**—the logfile encapsulator encapsulates application and system logfiles, for example NT Event Logs, to extract message information.
- **SNMP Events**—the SNMP event interceptor captures events on the management server and on selected agent platforms; see the *HP OpenView Operations Administrator's Reference Volume I* for more information.
- **MPE/iX Consoles**—the MPE/iX console message interceptor intercepts messages sent to the MPE/iX console.
- **OVO Message Interface**—these messages are generated by an OVO command or API (opcmsg(1|3)).
- **Monitored Objects**—you can set up threshold levels for monitored objects. When measured values of monitored objects exceed configured threshold levels, OVO will generate messages.
- **Your Applications**—all applications which write messages to logfiles, to an MPE/iX console, use the OVO APIs, or send SNMP traps can provide information to OVO.

OVO generates messages so that the information is presented to the user in the clearest form.

Managing Messages OVO can direct messages to logically related groups. A message group brings together messages from many related sources, providing status information about a class of managed objects or services. For example, the message group BACKUP can be used to gather all backup related messages, from sources such as backup applications and tape drives.

All messages forwarded to the management server use the same format in the message browser and are color coded to highlight message severity. The system can also be configured to activate external notification services such as pagers or automatic calling systems.

The message browser is the focal point for reviewing and solving problems. It contains message related information, including the availability and status of all preconfigured corrective actions. A service for documenting these or any other actions is also available.

Actions

An action is a response to a message. If the event creating the message represents a problem, OVO can start an action to correct it. However, actions are also used to perform daily tasks, such as starting an application every day on the same node(s). An action can be a shell script, program, command, application start, or any other response required. OVO offers the following types of actions:

- Automatic actions.
- Operator-initiated actions.
- Applications.

Automatic Actions Automatic actions are message-linked, preconfigured responses to problems. Automatic actions do not require operator interaction, and OVO starts them as soon as an appropriate message is received. The operator can manually restart or stop them if necessary.

Operator-Initiated Actions Operator-initiated actions are also message-linked, preconfigured responses to problems. These actions must be started and stopped by an operator. Administrators might choose to configure an operator-initiated action for a message instead of an automatic action because:

- The operator might have to perform manual operations in conjunction with the action.
- The starting of the action might be contingent upon conditions within the environment which must first be checked by the operator.

Applications Applications are scripts or programs which have been integrated into OVO. Whereas operator-initiated and automatic actions are directly associated with a message and can be started or stopped from the browser windows, applications are tools that are available in the operator's Application Desktops.

OVO User Concept

The OVO user concept distinguishes between real users, such as the OVO administrator and the OVO operators, and user profiles.

The primary user roles of OVO are:

- Administrator.
- Template administrator.
- Operator.

User profiles describe the configuration of abstract users and can be used to configure real users.

Operators and administrators must provide the correct login name and password before gaining access to their customized OVO user interface. These OVO passwords are not related to the operator's system login name and password.

User Profiles

User profiles are useful in large and dynamic environments with many OVO users. You can configure profiles of virtual users and assign these predefined profiles to real OVO users. This allows you to quickly set up users with a default configuration. You can create as many profiles as you need and arrange them in a user profile hierarchy.

OVO Administrator

The OVO administrator is primarily responsible for installing and configuring the OVO software, and establishing the initial operating policies and procedures.

The OVO administrator's tasks and responsibilities within the OVO working environment can be summarized as follows:

- Defines a custom environment for each user by managing all installation, configuration, and customization adaptations to add or change operators, template administrators, nodes, retrieved messages.
- Extends operator efficiency by matching corrective actions to specific events, and providing individual instructions for other events.
- Defines responsibility and capability sets, and decides which tools the operator needs to maintain the assigned nodes and perform the required tasks.
- Develops guidelines which template administrators use to implement a message policy and determines each template administrator's responsibility for templates or template groups.
- Maintains and reviews OVO's history data to modify or develop automatic and operator-initiated actions, provide specific event instructions, and track recurring-problems. For example, reviewing history data would reveal which nodes have permanently high utilization of disk-space.
- Acts as any operator to verify their configuration and help them resolve any current problem.
- Extends the scope of OVO by integrating additional applications and monitored objects and ensures consistent presentation and invocation of services by registering new applications in the Application Desktop.

Additionally, the administrator maintains the software, and defines management processes and security policies.

Template Administrator

OVO uses templates to intercept messages from different message sources, and to monitor areas where specified values, or preconfigured limits, are met or exceeded. Template administrators use configuration tools to set up message collection and monitoring services, and define filters and suppression criteria to refine and reduce information sent to operators.

Template administrators have administrative responsibilities limited to creating, modifying, or deleting templates and monitors which can be summarized as follows:

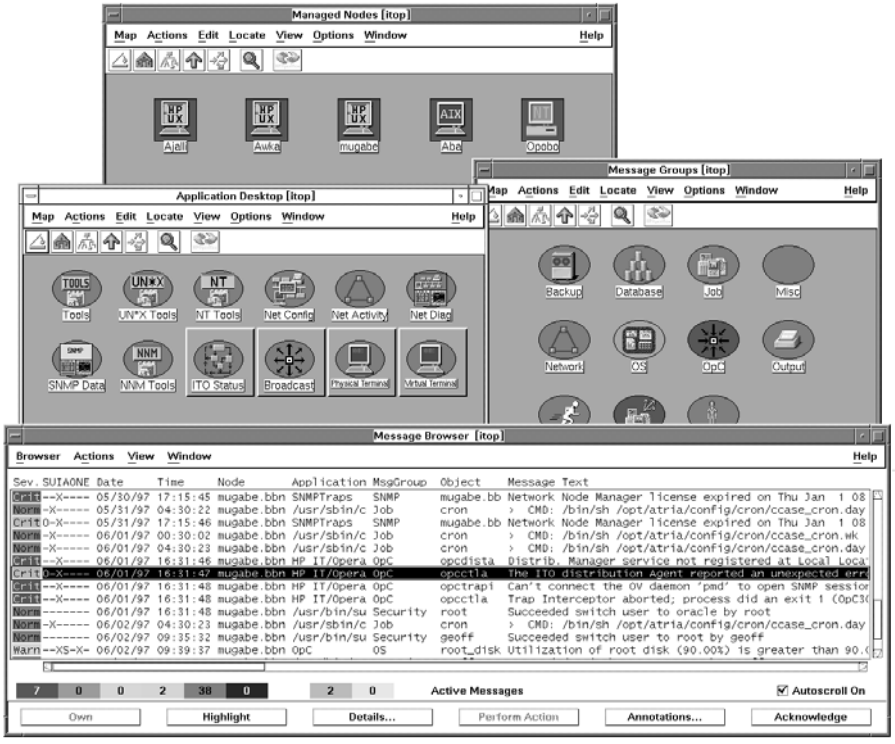
- Determining the message source or monitoring area and setting up the appropriate template or monitor.
- Providing instruction text to help the operator solve a problem.
- Defining advanced options for suppressing duplicate messages or diverting messages into, for example, an event correlation engine.
- Setting up filters to forward or suppress messages matching a specified pattern.
- Determining how matched and unmatched messages are handled by OVO.

Operators

Every operator's environment consists of a set of managed nodes. These nodes provide information which the operators use to solve problems and are the basis for daily tasks, such as application startups. Each OVO operator has a customized view of their managed environment. For example, one operator might be responsible for all nodes at a facility, and another responsible for a subset of nodes at another facility. By creating task-orientated environments, OVO operators see only the information from systems and objects under their control.

Figure 1-9 shows OVO's main operator windows. See Figure 1-10 on page 40 for an example of the Java-based operator GUI.

Figure 1-9 Main OVO Operator Windows



The following types of operators are available by default in OVO. For more detailed information on the default OVO operators, see "Setting Up Users and User Profiles" in the *HP OpenView Operations Concepts Guide*. The following list gives the names of the default operators and provides a brief description of their default role:

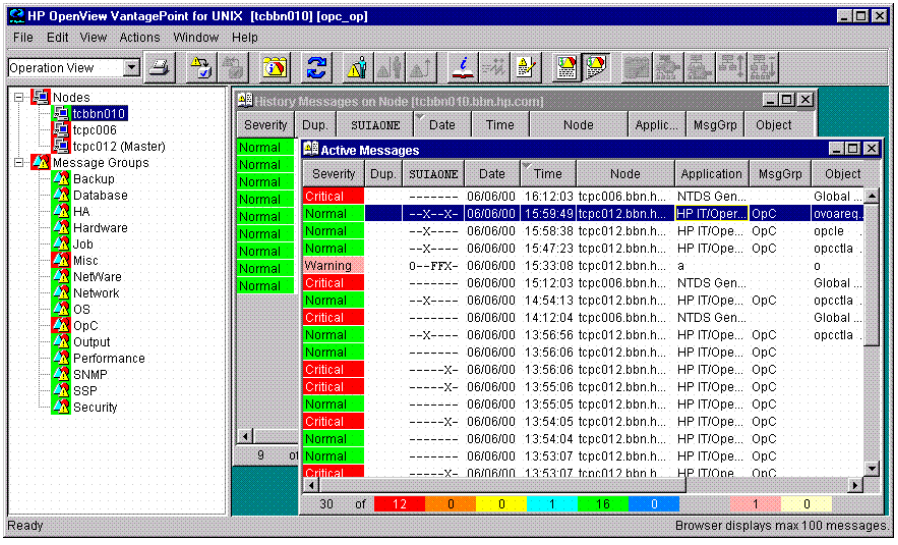
opc_op The opc_op operator controls system management functions only and is not concerned with the management of network activities such as applications for configuring OVO's network functions or network diagnostics tools.

netop The `netop` operator's environment combines OVO configuration capabilities with all the network-monitoring capabilities of a typical Network Node Manager operator.

itop The `itop` operator's role represents a combination of both the system and network-management roles. The itop operator has access to the full range of OVO software functionality.

Figure 1-10 shows the main windows that make up the working environment of an operator. Each window presents customized information matching the operator's responsibilities and capabilities and provides tools for performing management activities.

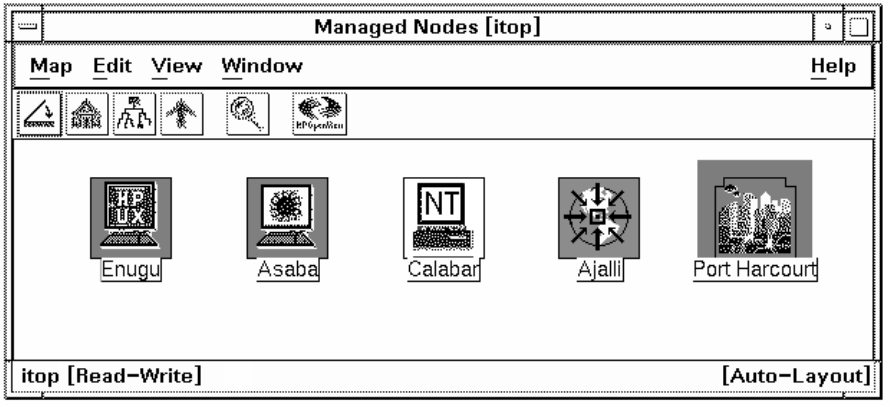
Figure 1-10 Java-based Operator GUI



The main windows are:

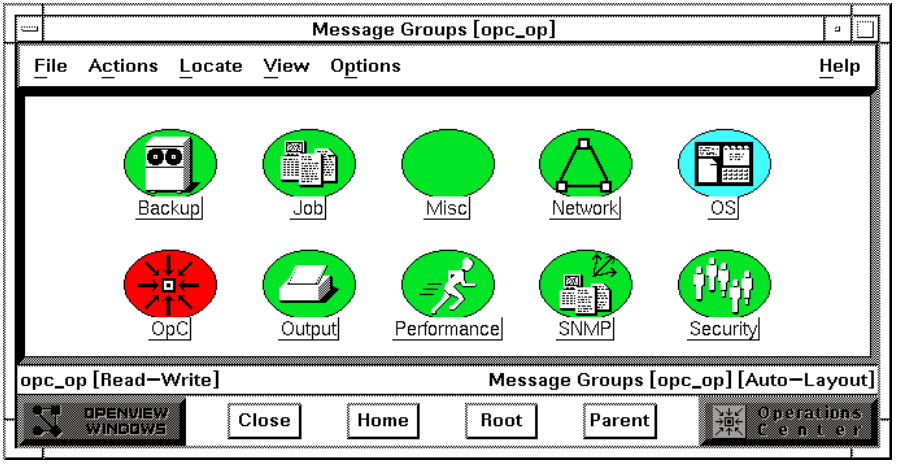
Managed Nodes The Managed Nodes window displays the operator's managed environment. Each node (or group of nodes) is represented by an icon. OVO changes the color of these icons to reflect the node's current status.

Figure 1-11 Managed Node Window



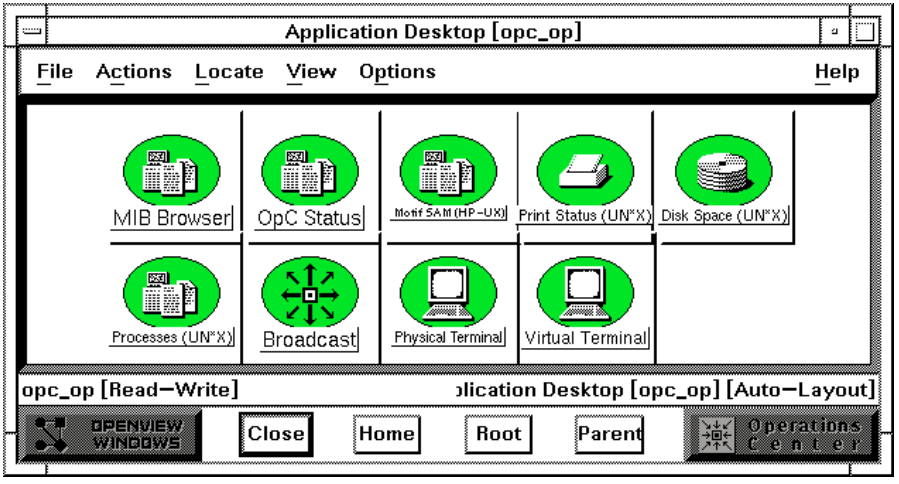
Message Groups The Message Groups window displays the operator's message groups. Messages are grouped by function, location, application, or any other logical classification. OVO changes the color of these icons to reflect the message group's current status.

Figure 1-12 Message Groups Window



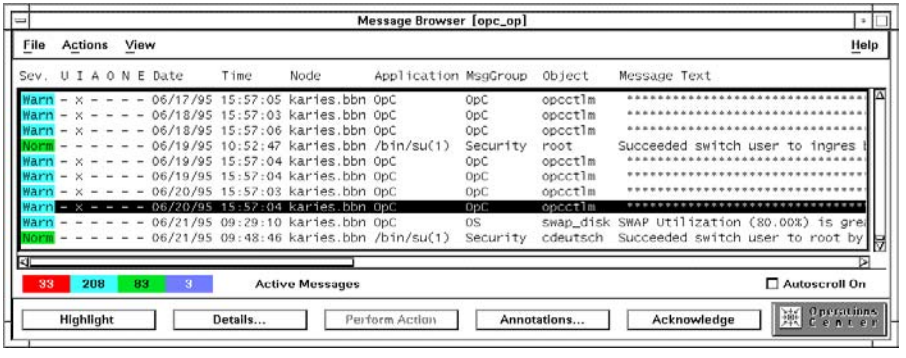
Application Desktop The Application Desktop window displays icons for each management application the operator can start. The OVO operator starts these tasks by double-clicking on a symbol or by selecting a node icon from the Managed Node Window and dragging and dropping it on an application icon.

Figure 1-13 Application Desktop Window



Message Browser The Message Browser window displays all incoming messages from the OVO operator's managed environment. The Severity column is colored to reflect the current status of the message.

Figure 1-14 Message Browser Window



From the Message Browser the operator can:

- access in-depth information about messages to be reviewed and managed.
- find instructions needed to help resolve problems.
- start and stop operator-initiated actions, which can be applications, scripts or programs.
- review the status of automatic actions, and restart or stop them if necessary.
- review or write annotations.
- highlight the location of problems.

The Message Browser window is a powerful source of information for performing system and problem management tasks. In addition, OVO supports the concept of marking or owning a message. Only the owner of a message may perform operations that need to be carried out in connection with a given message.

In addition to these main windows, operators may require or be assigned other windows according to the scope of their responsibility and their environment. For example, the itop operator has the IP Map window as part of the default environment.

What is the Data Protector Integration?

The Data Protector Integration is a software package that enables you to monitor and manage the health and performance of your Data Protector environment with HP OpenView Operations (OVO), HP OpenView Service Navigator, and the HP OpenView Performance (OVPA) Agent.

The union offers a complementary and consolidated view of Data Protector performance information and overall resource characteristics. The integration allows correlation of Data Protector performance data with the performance data of the operating system, the database, and the network - all from one common tool and in one central management system. Integration of Data Protector performance data into the OVPA helps to detect and eliminate bottlenecks in a distributed environment. In addition, the integration allows for system optimizations well as service level monitoring.

The Data Protector Integration offers the following key features:

- Instrumentation and configurations for the HP OpenView Operations agents on a Data Protector Cell Manager system to monitor the health and performance of Data Protector.
- Monitoring of multiple Data Protector Cell Managers with a single OVO Management Server.
- The Data Protector Integration integrates into HP OpenView Service Navigator and depicts the functionality of Data Protector as a service tree.
- The Data Protector Integration uses the ARM and DSI interfaces of the Performance Agent to collect performance data and ARM transactions.
- The Data Protector Integration channels messages sent to OVO Management Server based on a user's profile. Each OVO user sees only the messages he needs.
- The Data Protector Integration allows the Data Protector Cell Manager and the OVO Management Server to be installed on different systems.
- The Data Protector Integration enables you to run Data Protector functionality from the OVO Application Bank window.

- Data Protector Integration messages sent to the OVO management server includes instructions that help you correct the problem.

The Data Protector Integration offers the following key benefits:

- Centralized problem management using OVO agents at the Data Protector managed nodes. The use of a central management server avoids duplicated administrative effort.
- Real-time event and configuration information - including on-line 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 of any performance bottlenecks.
- Complements the Data Protector Administration GUI.
- Performance data collection and monitoring.
- Central data repository for storing event records and action records for all Data Protector managed nodes.
- Utilities for running Data Protector management tasks.

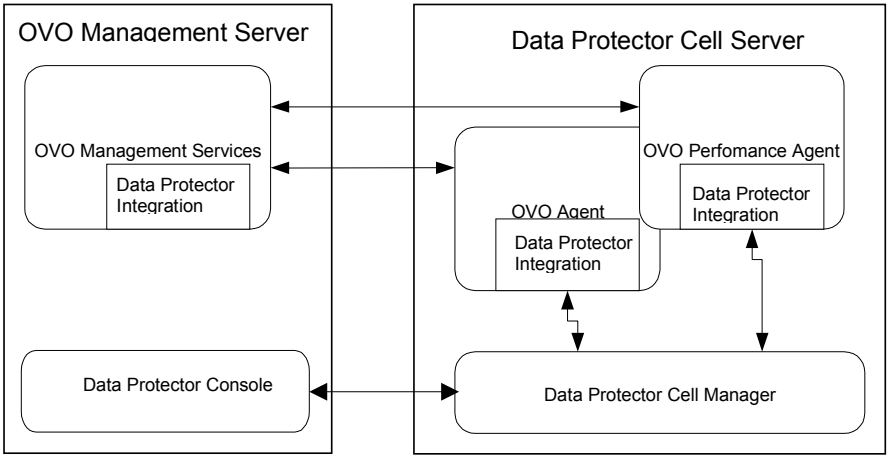
Data Protector Integration Architecture

The Data Protector Integration resides on the HP OpenView Operations (OVO) management server system and its OVO agent instrumentation on the Data Protector Cell Manager system, which is an OVO managed node. The Data Protector Cell Manager system must have the OVO agent and OVPA installed.

The Data Protector Console is installed on the OVO management server. Thus, the OVO user can start the Data Protector graphical user interface (GUI) as an OVO application and connect to any available Data Protector Cell Manager. Both Windows and UNIX Data Protector Cell Manager

are accessible from the same OVO Application Bank. This is facilitated by the Data Protector Console using Data Protector's communication protocol on port 5555 to exchange data.

Figure 1-15 Data Protector Integration Architecture



All the Data Protector OVO templates, which monitor:

- Data Protector logfiles
- Data Protector SNMP traps

configures the OVO agent on a Data Protector Cell Manager. The OVO agent on a Data Protector Cell Manager sends messages to the OVO management server for display in the message browser only if appropriate conditions match. This minimizes network traffic between a Data Protector Cell Manager and the OVO management 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 system where the HP OpenView Operations management server software is installed.
- Installing the Data Protector Integration components on OVO managed node (Data Protector Cell Manager) system.
- Deinstalling the Data Protector Integration components from OVO managed node (Data Protector Cell Manager) systems.
- Deinstalling the Data Protector Integration from the system where the HP OpenView Operations management server software is installed.

Supported Platforms and Installation Prerequisites

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

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

It is only guaranteed to work in these environments.

Before starting the Data Protector Integration installation process, make sure that the following requirements are met:

Data Protector Supported Versions

The Data Protector Integration is designed to work with HP OpenView Storage Data Protector, version 5.1 on the following platforms:

Table 2-1 HP OpenView Storage Data Protector Availability

Operating System	Data Protector Version	
	5.0	5.1
HP-UX 11.00	✔	✔
HP-UX 11.11	✔	✔
HP-UX 11.20		✔
Solaris 7	✔	✔
Solaris 8	✔	✔
Solaris 9 (OVO A.07.10 English Agent only)		✔
Microsoft Windows NT 4.0 with SP6A (Workstation, Server and Enterprise Edition)	✔	✔

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

Operating System	Data Protector Version	
	5.0	5.1
Microsoft Windows 2000 with SP3 (Professional, Server, Advanced Server, Data Center)	✔	✔
Microsoft Windows XP Professional (32 bit). Microsoft Windows Server 2003 (32 bit).		✔

OVO Management Server System

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

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

Table 2-2 OVO Management Server Supported Versions

OVO version[a] Operating System	OVO 6.x and Service Navigator 6.x	OVO 7.1 including Service Navigator
HP-UX 11.00	✔	✔
HP-UX 11.11	✔	✔
Solaris 7	✔	✔
Solaris 8	✔	✔

a. English, and Japanese.

OVO Patches

Please ensure that the following minimum patches are installed.

Table 2-3 Patches for OVO and Service Navigator (version A.06.00)[a]

Operating System	Patch Number	Description
HP-UX 11.x	PHSS_27342	Consolidated OVO Service Navigator patch A.06.13
	PHSS_28063	Intermediate OVO Server patch A.06.14
	PHSS_28177	HP-UX 11.00/11.11 OVO Agent A.06.12
	PHSS_28076	Java GUI client A.06.14.1
	PHSS_27298	Solaris OVO Agent A.06.11
	PHSS_27067	MS Windows OVO Agent A.06.11
	PHSS_27067	Windows XP Professional (32-bit) Agent
	PHSS_27298	Solaris 9 Agent
Solaris 7, 8[b]	ITOSOL_00117	OVO Service Navigator A.06.09
	ITOSOL_00101	Consolidated OVO Server patch A.06.08
	ITOSOL_00108	Intermediate OVO Server patch A.06.09
	ITOSOL_00104	HP-UX 11.x Agent A.06.08
	ITOSOL_00106	Solaris Agent A.06.08
	ITOSOL_00113	NT Agent A.06.08
	ITOSOL_00152	Windows XP Professional (32-bit) Agent
	ITOSOL_00158	Solaris 9 Agent

a. English, Japanese
b. Most of these patches are OS patches, so you may have them already installed if you use the latest “recommended & security patches” for Solaris from the Sun Webpage.

Table 2-4 Patches for OVO and Service Navigator (version A.07.10)[a]

Operating System	Patch Number	Description
HP-UX 11.x	PHSS_27387	HP-UX 11.0/11.11 OVO Msg/Act Agent A.07.12
	PHSS_28071	HP-UX 11.0/11.11 Coda Subagent A.07.10
	PHSS_27914	Consolidated OVO Java GUI A.07.x patch A.07.11
	PHSS_28501	Windows XP Professional (32-bit) Agent
Solaris 7, 8	ITOSOL_00192	Windows XP Professional (32-bit) Agent

a. English, Japanese

Software Prerequisites on the OVO Management Server

Please ensure that the following software is installed on the OVO management server system:

- HP OpenView Operations, version A.06.xx or A.07.xx. The console is installed and configured on the HP OpenView Operations management server system or other appropriate systems.
- *The HP OpenView Storage Data Protector Console is installed on the HP OpenView Operations management server system.*

  The **`swlist DATA-PROTECTOR`** command returns:

```
DATA-PROTECTOR           A.05.10  HP OpenView Storage Data Protector
DATA-PROTECTOR.OMNI-CC   A.05.10  HP OpenView Storage Data Protector Cell
Console
DATA-PROTECTOR.OMNI-CORE A.05.10  HP OpenView Storage Data Protector Core
```

Hardware Prerequisites on the OVO Management Server

Please ensure that the following hardware prerequisites are met on the OVO management server system:

- 5 MB disk space on the HP OpenView Operations management server system to install components necessary for the Data Protector Integration.

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 required components that must be installed on the managed node system hosting the Data Protector Cell Manager are:

- HP OpenView Operations Agent
- HP OpenView Performance Agent

NOTE The OVO and OVPA patches must be installed on the OVO management server and must be distributed by the OVO administrator to the manage node systems prior to the distribution of the Data Protector Integration.

Supported OVO Agent Versions

The Data Protector Cell Manager installation must be made on a platform for which the OVO Agent is available. Please refer to Table 2-5 for details of the available agent versions and ensure that the appropriate version is installed:

Table 2-5 HP OpenView Operations Agent Availability

Operating System	OVO Agent Version	
	OVO 6.0	OVO 7.1
HP-UX 11.00	A.06.08 or higher	A.07.10
HP-UX 11.11		
Solaris 7, 8		
Microsoft Windows		

Supported HP OpenView Performance Agent Versions

If the OVPA is to be installed, the Data Protector installation must be made on a platform for which the OVPA is available. Please refer to Table 2-6 for details of the available agent versions.

Table 2-6 HP OpenView Performance Agent Availability

Operating System	OVPA Version
HP-UX 11.00	C.03.70 or higher
HP-UX 11.11	
Solaris 7	C.03.75 or higher
Solaris 8	
Microsoft Windows NT 4.0 and 2000	C.03.65 or higher
Microsoft Windows XP Professional	
Microsoft Windows Server 2003	

Additional Software for HP-UX Managed Nodes

The following software is not installed as part of the OVO management server installation nor as part of the Data Protector Integration installation. Please refer to each product section to check whether they are required or optional.

SNMP Emanate Agent (required)

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

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

- The solution scales better: Additional Data Protector Cell Managers do not put additional load on the management server as the processing of SNMP traps is done 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 involvement of the management server.
- Since no SNMP trap is sent from the managed node to the management server, the network load decreases.
- The probability that SNMP traps are lost is significantly reduced as these are not transmitted over the network.
- Security over (public) networks is increased, since SNMP traps do not use a network and are sent, received and processed only on the managed node. OpC messages are sent by the OVO agent to the OVO management server using DCE/RPCs, which allows authentication and encryption.

Please check that the SNMP Emanate Agent is installed on the Data Protector Cell Manager node using the command:

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

You should see the following entry:

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

Additional Software for Windows Managed Nodes

The following software is not installed as part of the OVO management server installation nor as part of the Data Protector Integration installation. Please refer to each product section to check whether they are required or optional.

SNMP Service (required)

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

FTP Service (optional)

If you have the Data Protector Cell Manager installed on a number of Windows systems, you may consider installing the Windows FTP service. When you deploy the OVO Agent from the Unix OVO Management Server to a Windows system the most convenient way is to do it via the Windows FTP service.

For deployment of the OVO Agent to a Windows system alternative solutions exist. For details, please refer to the *HP OpenView Operations Installation Guide for the Management Server* and the HP OpenView Operations Administrator's Reference guides. However, using the Windows FTP service is the quickest and most convenient way.

Another advantage of using the Windows FTP service is if you want to conveniently distribute Data Protector configuration files from a central system to all Data Protector Cell Managers.

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

The FTP service is part of the Internet Service Manager Windows Component on Windows 2000. Configure the:

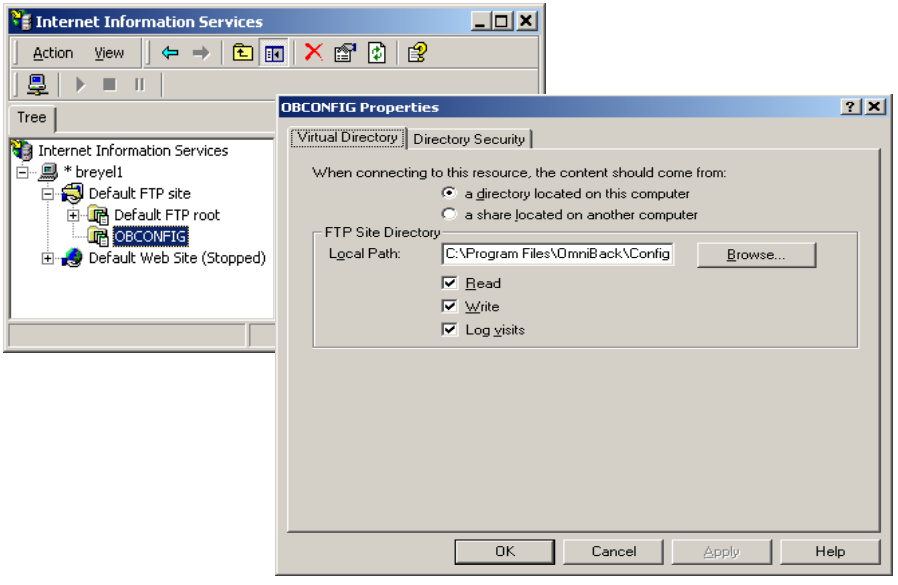
```
C:\Program Files\OmniBack\Config
```

directory (or equivalent directory, if you have chosen a custom path) as a Virtual Directory with the name:

`OBCONFIG`.

The `obusergrp.pl` tool needs precisely this name.

Figure 2-1 Configuring the Windows FTP Service



remsh Daemon (optional)

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

Disk-Space Requirements

Table 2-7 lists the disk space requirements for both the installation of the Data Protector Integration software and the Data Protector Integration's run-time files on the OVO management server and, in addition, on the managed node.

Table 2-7 Disk-Space Requirements

Machine	OVO Version	Operating System	Total
OVO Management Server	OVO 6.x and 7.x	HP-UX 11.x	5 Mb
		Solaris 7, 8	5 Mb
OVO Managed Node	OVO 6.x and 7.x	HP-UX 11.00, 11.11	1 Mb
		Solaris 7, 8	1 Mb
		Supported Microsoft Windows Nodes	1.5 Mb

Memory (RAM) Requirements

There are no specific requirements concerning the amount of RAM installed on either the OVO management server or managed nodes, beyond the requirements of OVO and Data Protector.

Installing the Data Protector Integration

The Data Protector Integration is delivered as a Software Distributor (SD) depot which is used to install the Data Protector Integration onto the OVO management server system through SD. This installs all components required for the management server and the managed nodes on the management server system. The agent software and the configuration data for these agents is then distributed by the OVO administrator to the managed nodes using OVO.

Installation

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

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

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

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

The following filesets are installed on an OVO Management Server on HP-UX or Solaris:

`SPI-DP-AGT-HP`	OVO agent files for the DP Cell Manager on HP-UX
`SPI-DP-AGT-NT`	OVO agent files for the DP Cell Manager on NT 4.0, Win2000
`SPI-DP-AGT-SOL`	OVO agent files for the DP Cell Manager on Solaris
`SPI-DP-CONF`	OVO templates and configuration files for the OVO Management Server
`SPI-DP-DOC`	Data Protector Integration's documentation in Adobe Acrobat pdf format

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

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

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

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

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

`/opt/OV/OpC/integration/obspi/bin`	Binary and script files
`/opt/OV/OpC/integration/obspi/etc`	XML template files for Service Navigation tree
`/opt/OV/OpC/integration/obspi/lib`	Libraries and message catalogs
`/opt/OV/OpC/integration/obspi/vpp`	Configuration files for Performance Agent
`/opt/OV/OpC/integration/obspi/doc`	Documentation
`/var/opt/OV/log/obspi`	Logfiles
`/var/opt/OV/share/tmp/obspi`	Temporary and runtime files
`/var/opt/OV/share/tmp/OpC_appl/obspi`	OVO files in uploadable format
`/etc/opt/OV/share/obspi/conf`	XML files uploaded by Service Manager
`/etc/opt/OV/share/bitmaps/C/omniback`	Icons and bitmaps
`/etc/opt/OV/share/registration/C/DPSPI`	Application registration file

Installation Verification

Check the following logfiles for errors:

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

To check the Software Distributor installation, enter the following command:

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

You should get the following response.

# SPI-DATAPROTECTOR-OVO	SPI-DATAPROTECTOR-OVO HP OpenView Storage Data Protector Integration into OVO		
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-HP	A.05.01	Configured	Data Protector Integration's files for the DP Cell Manager on HP-UX 11.x
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-NT	A.05.01	Configured	Data Protector Integration's files for the DP Cell Manager on NT 4.0, Win2000
SPI-DATAPROTECTOR-OVO.SPI-DP-AGT-SOL	A.05.01	Configured	Data Protector Integration's files for the DP Cell Manager on Solaris 7 and 8
SPI-DATAPROTECTOR-OVO.SPI-DP-CONF	A.05.01	Configured	Data Protector Integration's templates for the Mgmt. Server
SPI-DATAPROTECTOR-OVO.SPI-DP-DOC	A.05.01	Configured	Data Protector Integration's documentation

On HP-UX OVO Management Server:

SPI-DATAPROTECTOR-OVO.SPI-DP-SRV-HP	A.05.01	Configured	Data Protector Integration's executables and scripts for the Management Server

On Solaris OVO Management Server:

SPI-DATAPROTECTOR-OVO.SPI-DP-SRV-SOL	A.05.01	Configured	Data Protector Integration's executables and scripts for the Management Server

Agent Installation

The agent software has to be distributed to the managed nodes in two main steps:

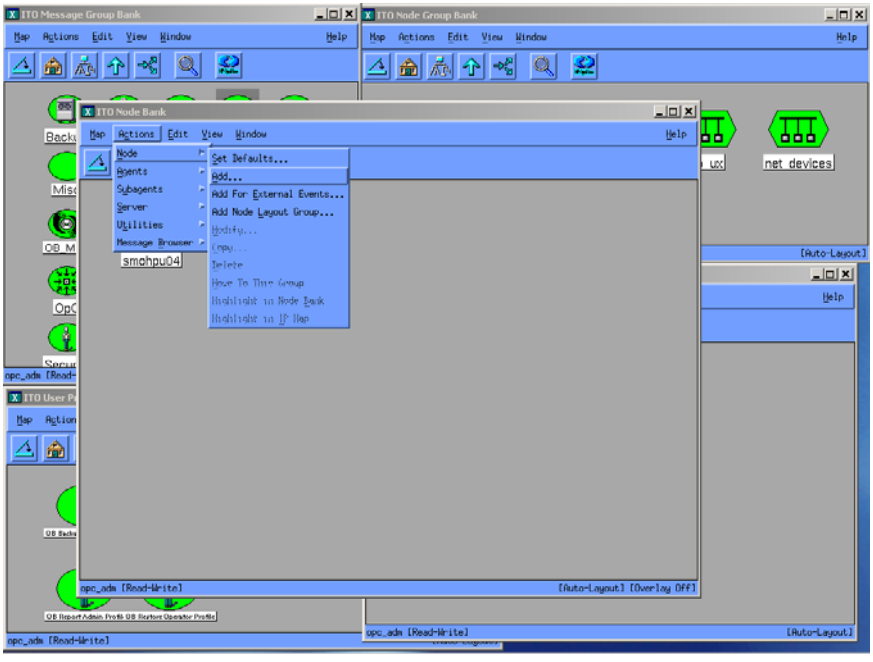
- Add the Data Protector Cell manager host system to the OVO managed environment as a managed node.
- Run the `Add Data Protector Cell` application for each Data Protector Cell manager node
- Distribute software, actions, commands, monitors and templates to the Data Protector Cell Manager managed node.

Adding the Data Protector Cell Manager System as an OVO Node

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

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

Figure 2-2 OVO Node Bank



3. Select **Actions** → **Node** → **Add...**
4. Add the label and hostname of the node that you are adding in the `Add Node` window.

You now have the Data Protector Cell manager system as a node in the `Node Bank`.

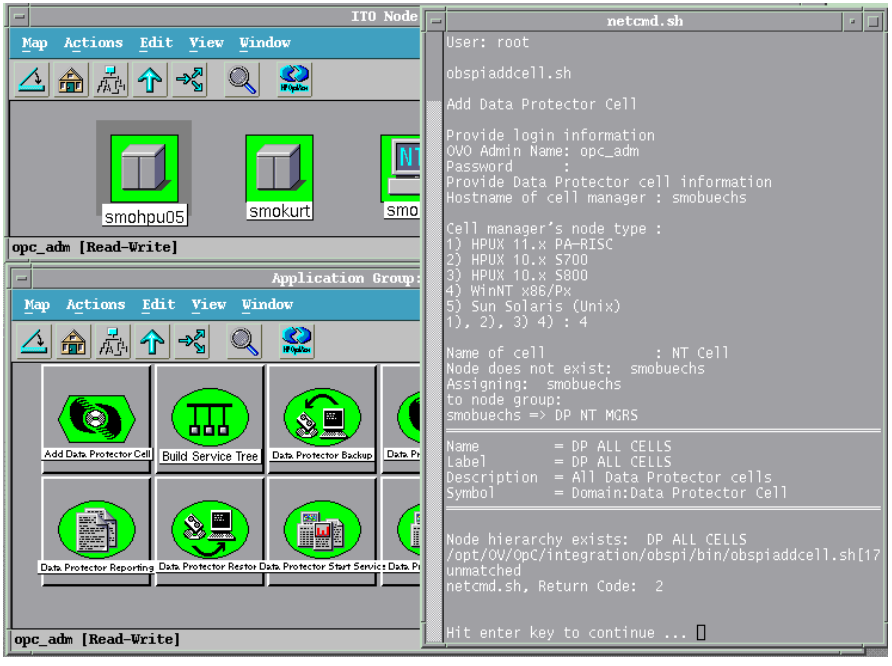
Running the Add Data Protector Cell Application

To run the Add Data Protector Cell application, as user `opc_adm`:

1. Open the `Node Bank` and the `DPSPI_Applications` window.
2. Select the **Data Protector Cell Manager** node from the `Node Bank` and drag and drop it onto the **Add Data Protector Cell** application.

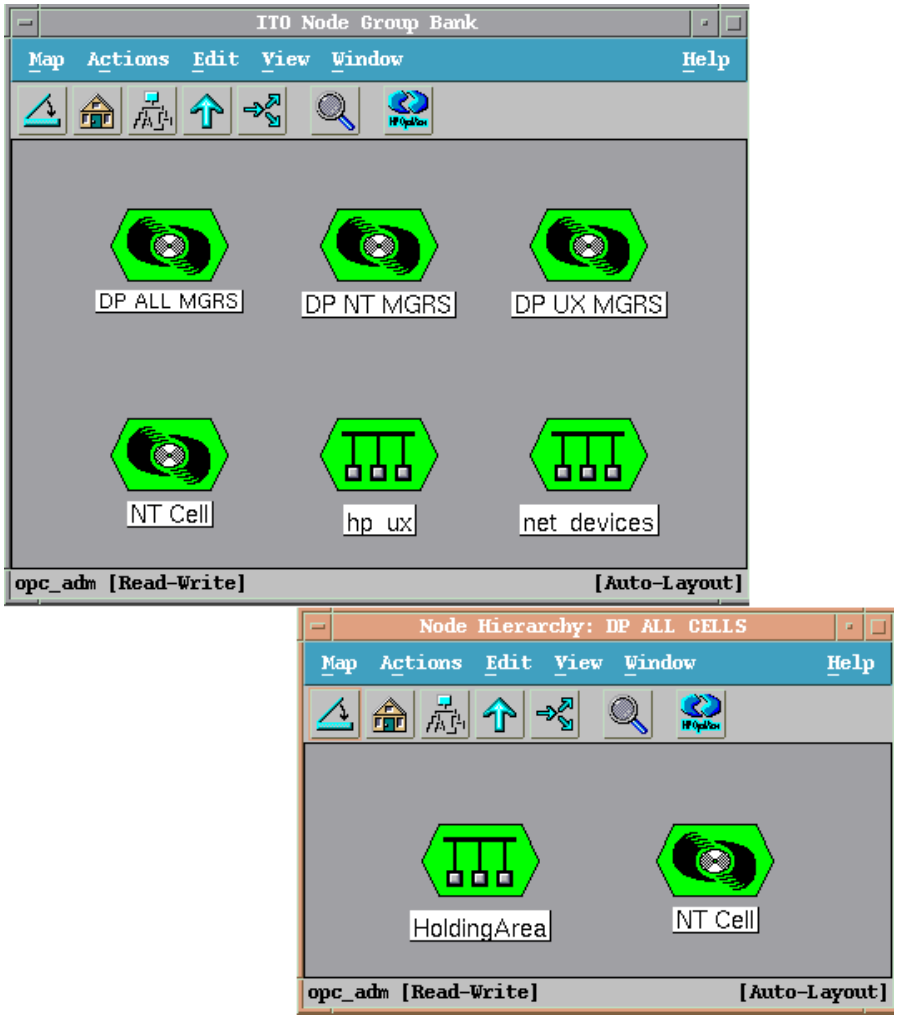
   This opens a terminal window where you are asked to input some information:

Figure 2-3 Add Data Protector Cell Application



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

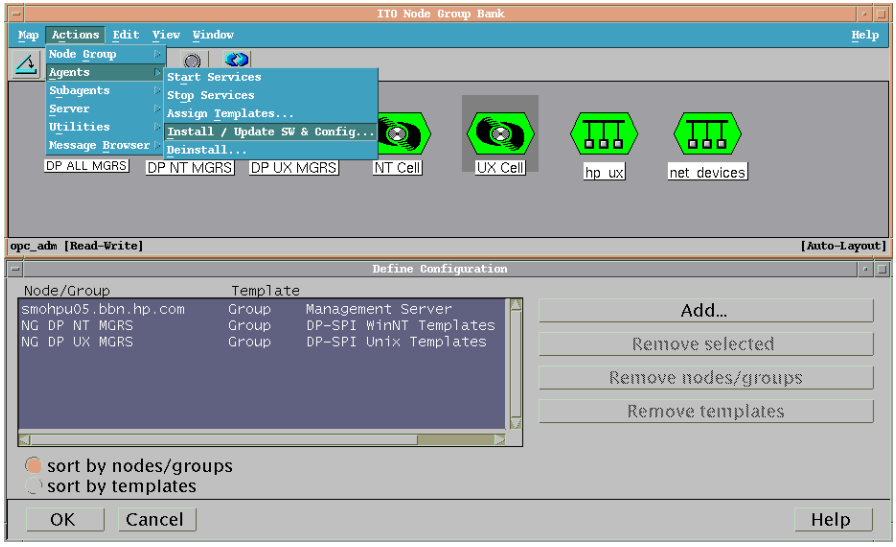
Figure 2-4 New Node Group and Layout Group for DP ALL MGRS



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

To distribute software, actions, commands, monitors and templates to the Data Protector Cell Manager managed node (the appropriate assignments have been made during installation):

Figure 2-5 Distribute to Managed Node



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

   Actions → Agents → Install / Update SW & Config...
4. Follow any instructions displayed in the terminal window.

Agent Configuration

SNMP Configuration on UNIX

To enable the OVO Agent on HP-UX nodes to receive SNMP traps from Data Protector:

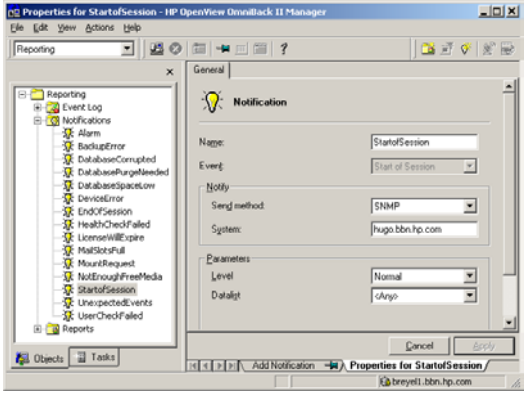
1. Add one of the following lines to the `/opt/OV/bin/OpC/install/opcinfo` file.
   - If an `ovtrapd` process is running add:

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

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

   `trap-dest: 127.0.0.1`
3. Configure Data Protector to send SNMP traps to the Data Protector Cell Manager host:
   a. Use the Data Protector GUI's **Reporting** context window to setup all Notification events to use:
      - SNMP as delivery method
      - Cell Manager host system as the destination

Figure 2-6 Data Protector GUI's Reporting context window



b. Add the Cell Manager hostname as trap destination to the `OVdests` file in `/etc/opt/omni/snmp`.

c. Disable filtering of SNMP traps by emptying the `OVfilter` file in `/etc/opt/omni/snmp`.

SNMP Configuration on Windows

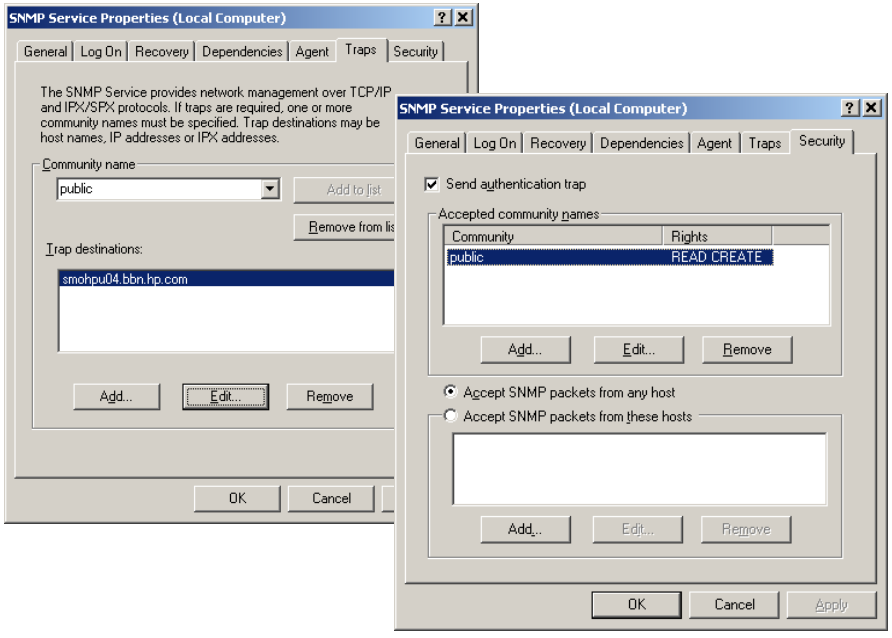
We recommend that you configure the Windows system to forward it's SNMP traps to the OVO Management Server in the following way:

1. Add the following line to the `\usr\opt\OV\bin\OpC\install\opcinfo` file.

   `SNMP_SESSION_MODE NO_TRAPD`

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

Figure 2-7 Configuring the SNMP Service on Windows



If you want to use a custom community name other than `public`, you must set this value in the Registry. This will let Data Protector use this custom community name for sending SNMP traps:

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

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

   a. Use the Data Protector GUI's **Reporting** context window to setup all Notification events to use:

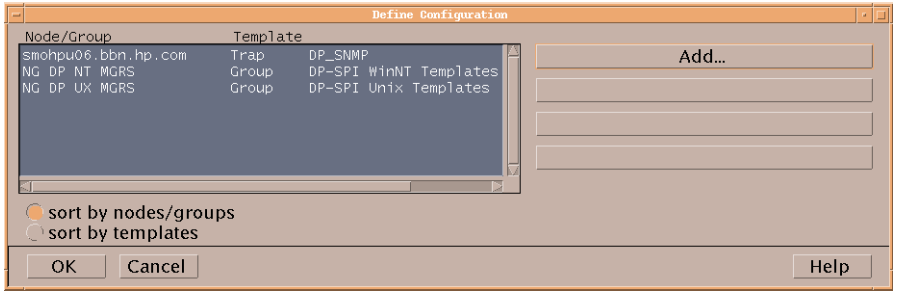
      - SNMP as delivery method
      - OVO management server system as the destination

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

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

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

Figure 2-8 SNMP template assignment to OVO management server



Data Protector User Configuration

UNIX For Data Protector on HP-UX nodes, check that the local root user is in the Data Protector's `admin` user group.

Windows For Data Protector on Windows, add the local `HP ITO account` user to Data Protector's `admin` user group.

Miscellaneous Configuration

Windows For Windows nodes, the system Variable:

`DPHomeDIR`

must be set with the Data Protector root path in order for the OVO Agent is able to find the Data Protector logfiles to be monitored.

The default location is: `C:\Program Files\OmniBack`

NOTE After changing a Windows system variable, the system must be restarted.

Program Identification

On UNIX Managed Nodes

All Data Protector Integration programs and configuration files contain an identification string which can be displayed using the UNIX command:

`what(1):`

The output is of the form:

```
HP OpenView Storage Data Protector Integration into OVO
A.05.01 (<build_date>)
```

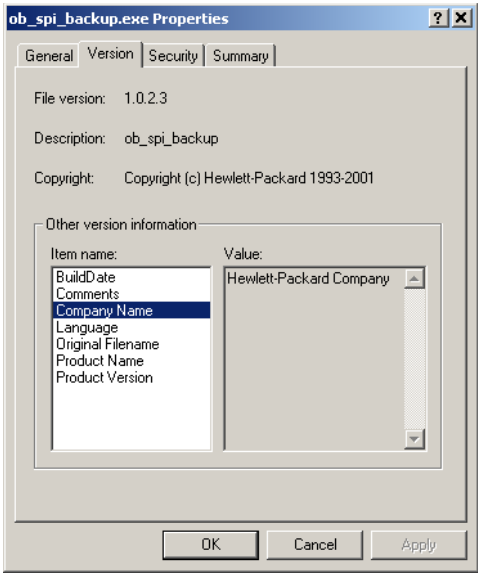
On Windows Managed Nodes

All Data Protector Integration programs and configuration files contain an identification string which can be displayed by:

1. Right-clicking the `ob_spi_backup.exe` file.
2. Select **Properties** from the popup menu.

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

Figure 2-9 Version Information



Deinstalling the Data Protector Integration

When deinstalling the Data Protector Integration, components must be removed from both the:

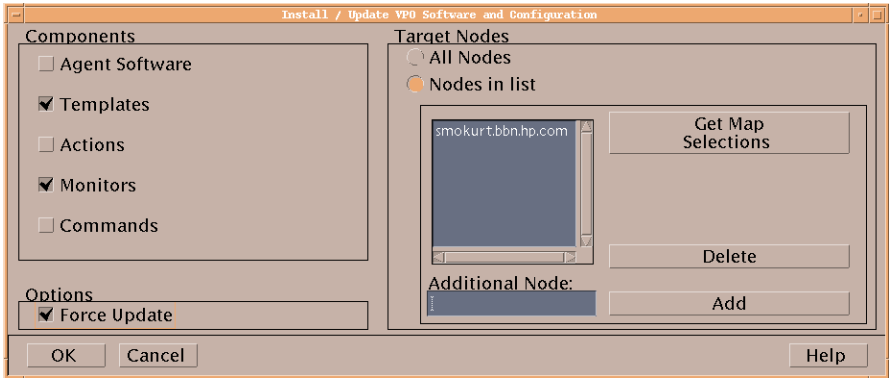
- Managed node systems (Data Protector Cell Manager)
- HP OpenView Operations management server system

Deinstalling from Managed Nodes

To deinstall the Data Protector Integration from a managed node, you must:

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

Figure 2-10 Redistribute with Force Update Option



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

Deinstalling from the Management Server System

If the OVO management server is using the default Administrator login name and password use the following command to deinstall the Data Protector Integration from the management server system:

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

In the case of a different Administrator login name or a changed password, you must carry out the following steps before you can remove SPI-DATAPROTECOR-OVO from your system.

1. Use the following swask command:

   ```
   swask SPI-DATAPROTECTOR-OVO
   ```

2. Enter the OVO management server administrator login name.
3. Enter the OVO management server administrator password.
4. Start swremove:

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

Upgrading the Omniback 4.1 Integration to Data Protector Integration

HP OpenView Storage Data Protector Integration builds upon the capabilities of its predecessor, HP OpenView Omniback II. To upgrade from Omniback II Integration to Data Protector Integration you must:

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

   `swremove SPI-OMNIBACK-OVO`

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

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

   OR

   Using the deinstallation tool provided with the Data Protector Integration:

   a. Copy the `deinstallobspi.tar` file from the CD to the OVO management server.

   b. Untar the file:

      `tar -xf deinstallobspi.tar`

   c. Start the script `deinst_OBSPI.sh` in `/tmp/OBSPI`

   d. Enter OVO administrator login name and password.

3. Install the `SPI-DATAPROTECTOR-OVO` with the following command:

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

4. Configure the Data Protector Integration using the OVO GUI:
   a. Drag & drop all managed nodes which are Data Protector Cell Managers into the `DP ALL MGRS` group.
   b. Drag & drop all managed nodes which are Data Protector Cell Managers and NT/Windows2000 platforms in the `DP NT MGRS group`.
   c. Drag & drop all managed nodes which are Data Protector Cell Managers and UX platforms in the `DP UX MGRS` group
5. Redistribute the templates and monitors to the managed nodes with the **Force Update** option (see Figure 2-10 on page 70).

Configuring the Data Protector Integration for Mixed Environments

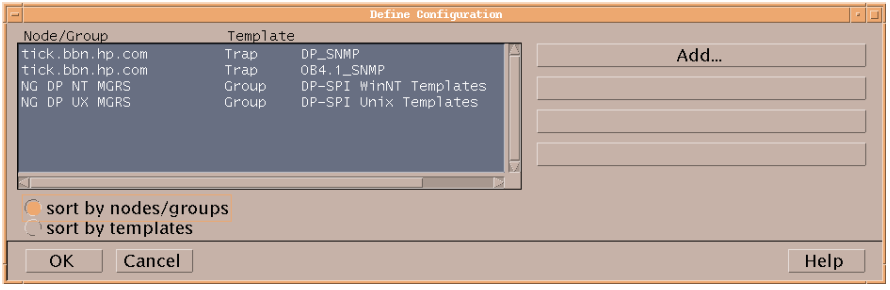
If your environment has both Omniback 4.1 and Data Protector 5.1 Cell Managers, you must configure the Data Protector Integration to also work with the Omniback 4.1 Cell Managers. The Data Protector Integration handles an Omniback 4.1 Cell Manager in the same way as a Data Protector Cell Manager. In order to be able to distribute the templates and monitors for Omniback 4.1 managed nodes and see messages in the message browser, you must include the Omniback 4.1 Cell Manager in the `DP ALL MGRS` group and, depending on the platform, either in the `DP NT MGRS` or `DP UX MGRS` group.

There is one extra consideration when using the integration for Omniback 4.1 and Data Protector Cell Manager. You can not use the `DP_SNMP` template for matching any of the Omniback 4.1 SNMP traps. Therefore, you must use the `OB4.1_SNMP` trap template for the Omniback 4.1 systems. This template is not included in either the `DP-SPI WinNT` or `DP-SPI UNIX` integration template groups, and so it is not automatically assigned to any node. It must be manually assigned if required. Manual assignment of the `OB4.1_SNMP` trap template varies, depending on the platform of the Omniback 4.1 Cell Manager as the SNMP sending methods are not the same on Windows and UNIX.

In case of an Windows Cell Manager, the SNMP trap is sent directly to the OVO management server, where intercepting and condition matching take place. Therefore, if you want to receive SNMP messages from an Omniback 4.1 Cell Manager on Windows, you must assign and distribute the `OB4.1_SNMP` template to the OVO management server

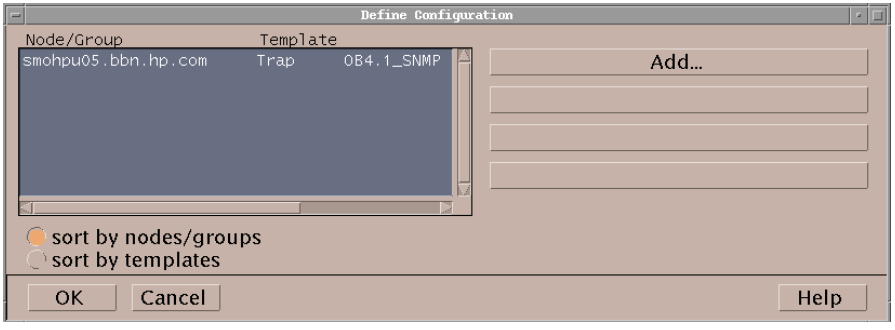
system itself. It is acceptable to assign both the DP_SNMP and the OB4.1_SNMP templates to the OVO management server because as they operate independently of each other.

Figure 2-11 Template assignment for OVO management server



In case of an UNIX Cell Manager the SNMP trap is send to itself, where intercepting and condition matching is done by the OVO agent. Therefore, if you want to receive SNMP messages from Omniback 4.1 Cell Manager on UNIX, you need to assign and distribute the OB4.1_SNMP template to the UNIX Cell Manager.

Figure 2-12 Template assignment for Data Protector Managed Node



3 Integration into HP OpenView Service Navigator

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

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

What Is HP OpenView Service Navigator?

HP OpenView Service Navigator is an add-on component of the HP OpenView Operations Java-based operator GUI. It enables you to manage your IT environment while focusing on the IT services you provide.

While OVO lets you detect, solve, and prevent problems occurring in networks, systems and applications in your IT environment, Service Navigator takes you one step further. Service Navigator lets you map the problems discovered by OVO to the IT services you want to monitor. Instead of focusing on single elements within a complex IT environment, you can now manage your IT environment by focusing on the IT services you are responsible for.

Service Navigator is based on OVO and depends on the monitoring, message, and action capabilities OVO provides. If a problem occurs on one of the objects managed by OVO, a message about this problem is generated and sent to the user responsible for the area concerned. With Service Navigator installed and configured, this message is mapped to the service that is impacted by the problem, and sent to the user responsible for that service.

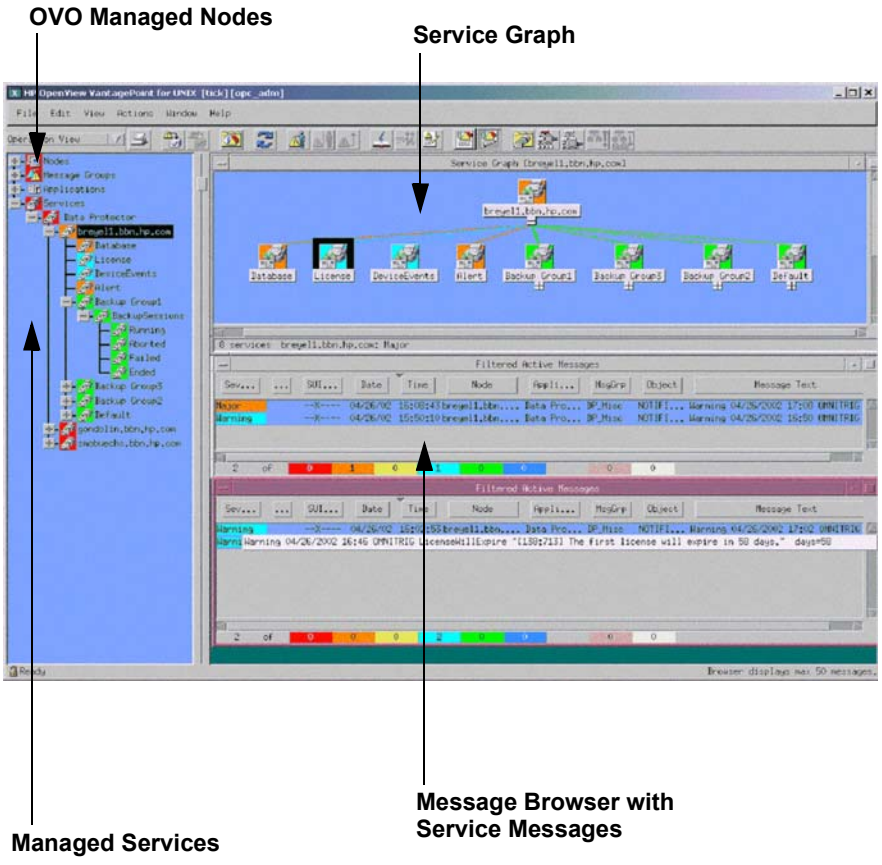
The severity status of the problem also changes the severity status of the service so that the user can easily identify services that are in a problematic state. To solve service-related problems, OVO's problem resolution capabilities have been further extended to include service-specific analysis operations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

If enabled, Service Navigator logs each change of status in the database so that reports about service availability can be generated.

Figure 3-1 on page 80 shows the main window of Service Navigator. In addition to the customary OVO managed nodes and message groups, managed services are displayed in the scoping pane on the left. The content area on the right is split into two sections. The upper section displays a service hierarchy in graphical form where each service is

represented by an icon. The lower section contains the standard OVO message browser configured to display only the messages that pertain to your service.

Figure 3-1 The Service Navigator GUI



How Does Service Navigator Work?

The concept behind Service Navigator is that of a hierarchical service structure. Service Navigator lets you build a hierarchy that reflects the relationships and dependencies between the service-relevant managed objects in your IT environment.

The following section explains the concept of a service hierarchy and how a service can be logically related to a subservice.

What Is a Service Hierarchy?

A service hierarchy is a logical organization of the services you provide, each higher level covering a wider or more general service area than the next lower level. The relationship between services in a hierarchy can be one of two types:

containment: a service is contained in a service; that is, 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 subservices.

usage: a service is contained in a service but, at the same time, is 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 of no consequence whether a service is contained in or used by another service. Note, however, that a service can be defined only once but be used or contained many times.

Service Navigator supports up to 256 hierarchical levels.

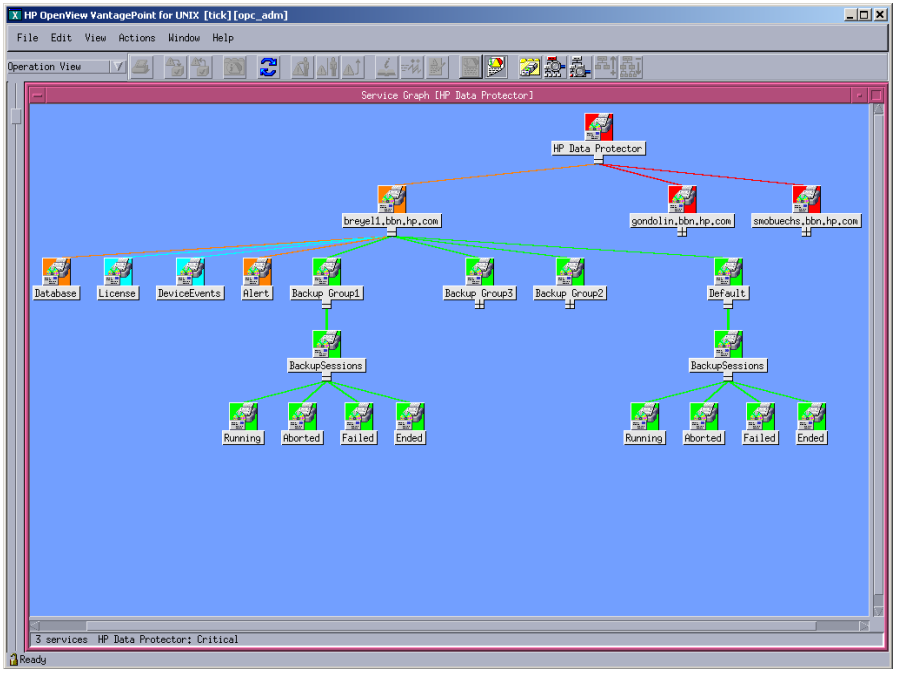
Figure 3-2 shows an example of a service hierarchy for a Data Protector Cell Manager. The Data Protector Cell Manager service includes the cell systems and their component:

- 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. Together they build the Data Protector service hierarchy. The relationship between the services is of the type containment.

Figure 3-2 Example: Data Protector Service Hierarchy

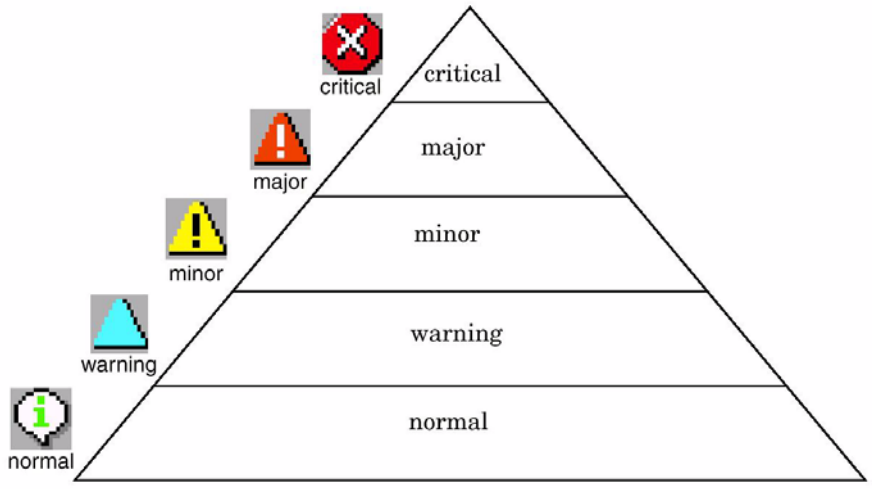


The fact that OVO allows one service using another subservice, saves you having to set up specific subservices for each of your service hierarchies. You can set up a generic service, for example monitoring the operating system on a Data Protector Cell Manager system, that can be used by any other service hierarchy responsible for monitoring a Data Protector Cell Manager system.

OVO Severity Pyramid

The status of a service is the current operational status of a service. The status is indicated by status colors, each color signalling how severe the current situation is. For example, the color red indicates a critical problem situation. See also Figure 3-3 for an illustration of the OVO severity status model.

Figure 3-3



Since a service contains or uses several subservices, and since each subservice in turn contains or uses other subservices, the severity status of the service must be determined and calculated on the basis of the severity statuses of the next lower services in addition to the severity statuses of the messages targeting the service.

This is done on the basis of status propagation and status calculation rules. These rules define the relationship of a service to its subservices in terms of how they interpret each other's severity status. Status rules are defined in the service configuration file; see the *HP OpenView Service Navigator Concepts and Configuration Guide* for more information about HP OpenView Service Navigator.

Data Protector Service Tree

This section explains how the capabilities of Service Navigator are used by the Data Protector Integration to help monitor the status and health of Data Protector cells.

Data Protector is represented as a Service Navigator service. Each Data Protector cell is represented by an icon within the Data Protector service. The service tree is updated by SNMP traps sent by the notification feature in Data Protector and by messages from the Data Protector Integration's monitors. Figure 3-4 illustrates the Data Protector service tree with three Data Protector Cell Managers.

Figure 3-4 The Data Protector Service Tree

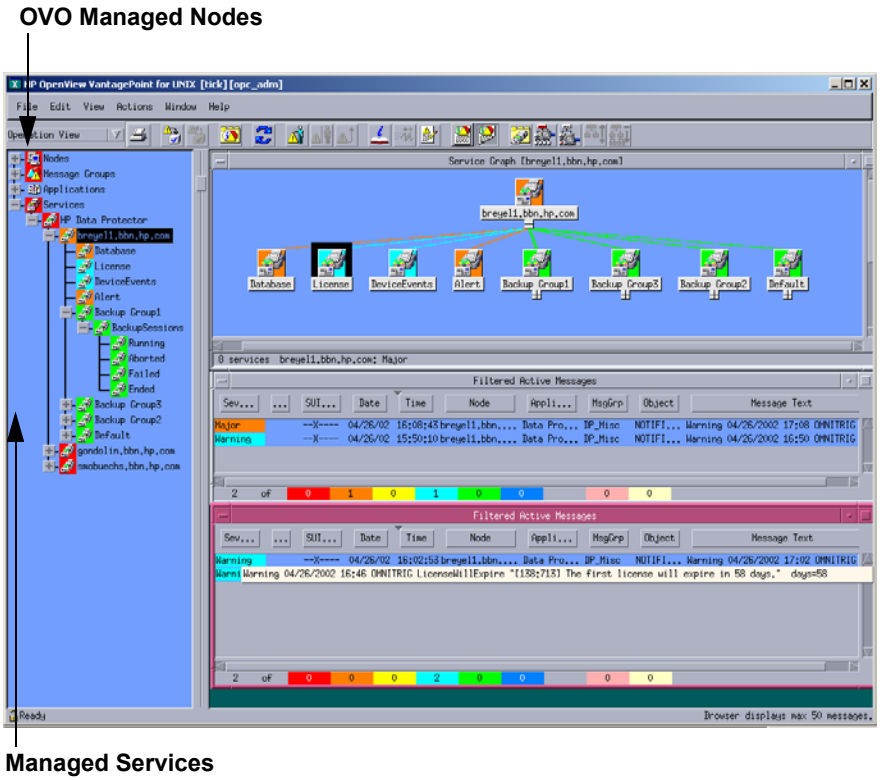


Table 3-1 lists the service tree nodes available for each cell.

Table 3-1 Cell Service Tree Nodes

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

You may apply this service to an additional user with the command:

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

Starting the Service Navigator GUI

To start the Service Navigator GUI, run:

```
ito_op
```

and login 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

During deinstallation of the HP OpenView Storage Data Protector Integration, the `SPI-DATAPROTECTOR-OVO` product is removed and the complete Data Protector service tree is de-assigned from all its users and it is removed.

Removal of the tree can also be done manually by:

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

4 Using the Data Protector Integration

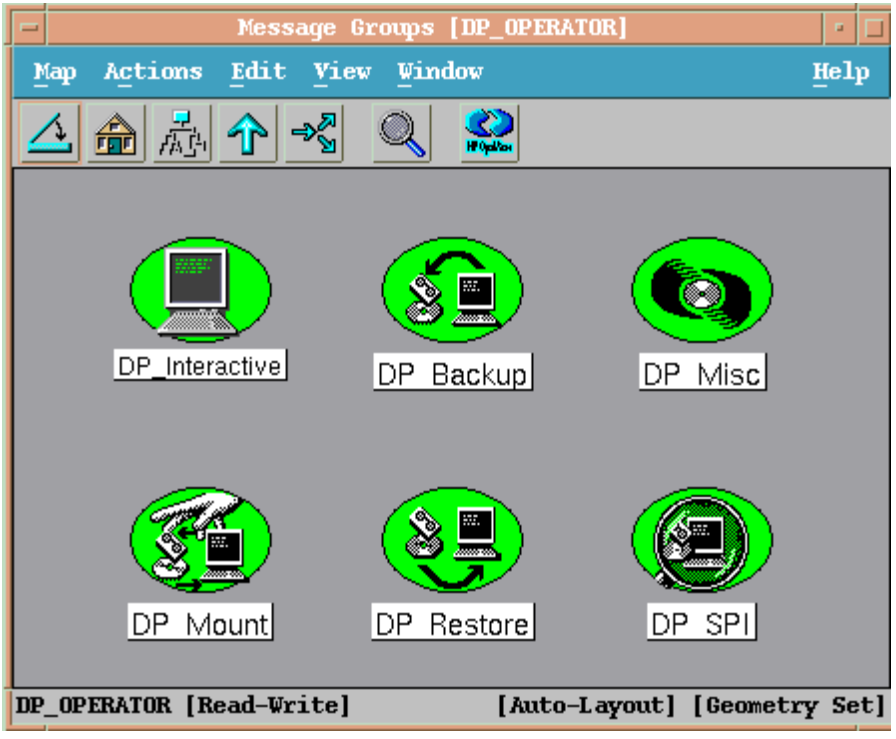
The sections in this chapter show which new components are added to OVO during the installation of the Data Protector Integration software and describe how to use them to best effect. This chapter provides detailed information about the following areas:

- “Message Groups”
- “Node Groups”
- “Application Groups”
- “Users and User Profiles”
- “Monitored Objects”
- “Monitored Logfiles”

Message Groups

The Data Protector Integration installs six message groups that are specifically designed to handle messages generated by the templates and monitors started by the Data Protector Integration. Figure 4-1 shows the Data Protector Integration message groups.

Figure 4-1 Data Protector Integration Message Groups



The Data Protector Integration generates a wide variety of messages. Where appropriate, the Data Protector Integration assigns relevant messages to existing OVO message groups. All those messages generated

by the Data Protector Integration which do not obviously belong to existing OVO message groups are assigned to the following six Data Protector Integration-specific message groups:

`DP_Backup`	Backup session related messages
`DP_Restore`	Restore session related messages
`DP_Mount`	Mount request related messages
`DP_Misc`	All other important Data Protector related messages
`DP_SPI`	Messages from the Data Protector Integration
`DP_Interactive`	Detailed messages that are normally only displayed in the Data Protector GUI. This message group is disabled as default. Enable this message group if the greatest details about Data Protector's operation is required.

Message Format

An OVO message includes the following parameters:

Message Group The following message groups are available:	`DP_Backup`	Backup session messages
	`DP_Restore`	Restore session messages
	`DP_Mount`	Mount request messages
	`DP_Misc`	All other important Data Protector messages
	`DP_SPI`	Data Protector Integration messages
	`DP_Interactive`	Detailed messages that are normally only displayed in the Data Protector GUI.
Applications	Set to `Data Protector`	

Node	Set to the hostname of the Data Protector system the event occur.
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	This depends on the impact the event has to a service. This value needs to 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 object parameter to `NOTIFICATION` Messages which origin from a: • monitored logfile, set the Object parameter to the name of the logfile. • monitor, set the Object parameter to the name of the monitor.

Node Groups

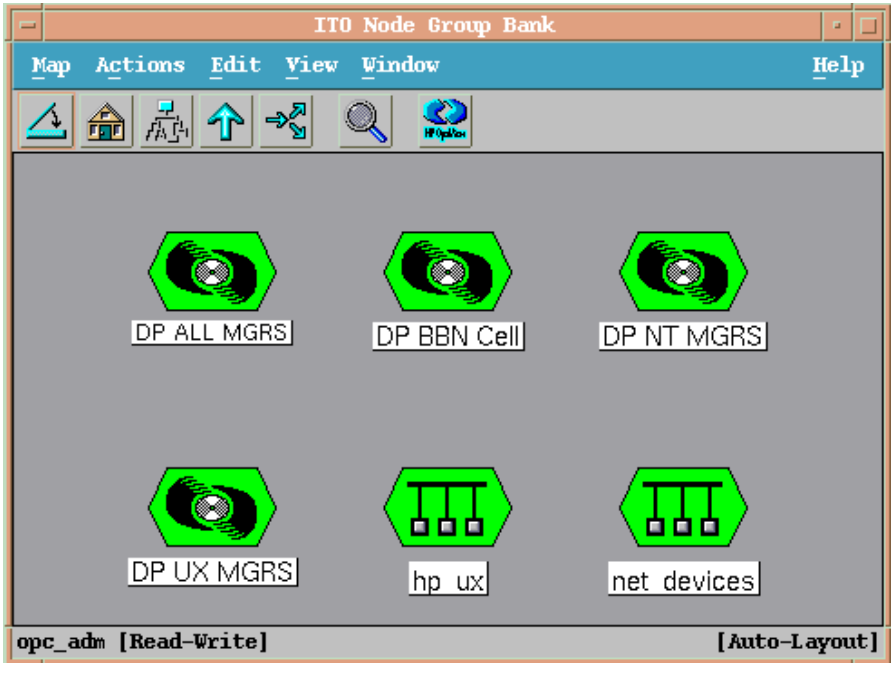
Node groups are logical groups of systems or devices which are assigned in combination with message groups to an operator to manage. Each node group is represented by an icon in the `Node Group Bank` window. All systems within a node group can be viewed by opening the node group. A system may belong 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, as illustrated in Figure 4-2.

Node groups are used to define the nodes from which a user receives messages. In combination with message groups, node groups define the:

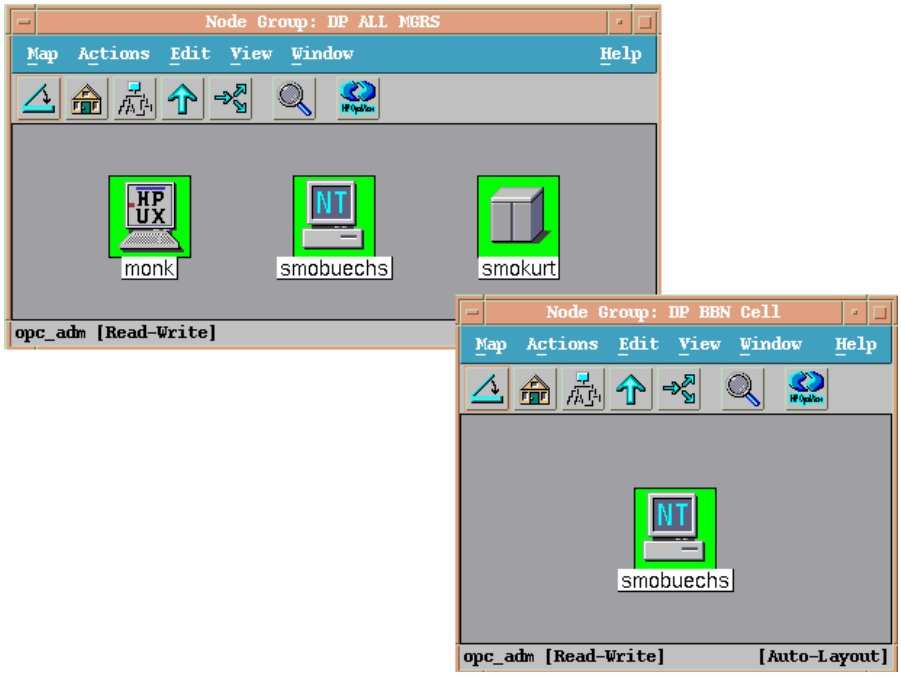
- responsibilities of a user
- messages displayed to a user in the message browser

Figure 4-2 Data Protector Integration Node Groups for opc_adm



The content of DP ALL MGRS Node Group and of the DP BBN Cell Node Group are illustrated in Figure 4-3.

Figure 4-3 DP ALL MGRS Node Group and DP BBN Cell Node Groups



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

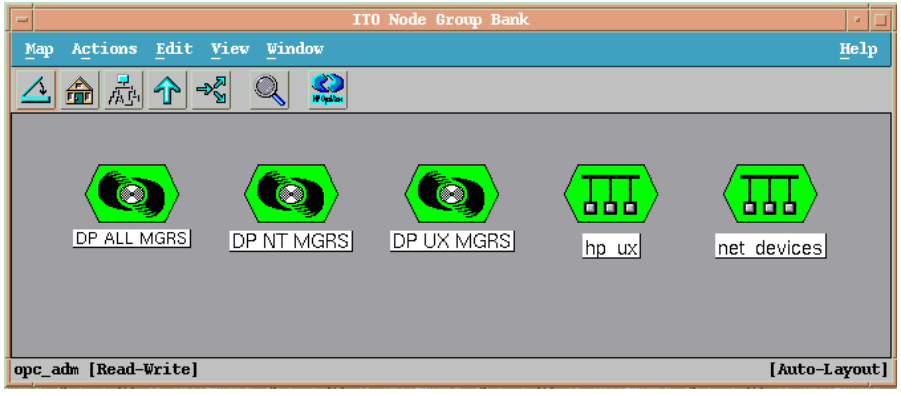
There are two further node groups which are created during installation of the Data Protector Integration:

- DP NT MGRS
- DP UX MGRS

These can be used by any OVO administrator to help assign and distribute template 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, this node get automatically deleted from the corresponding node group. The Data Protector Integration node groups are illustrated in Figure 4-4.

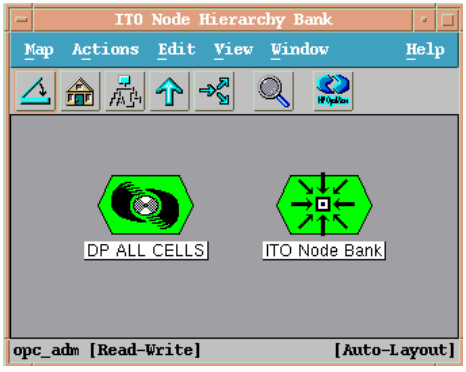
Figure 4-4 DP Node Groups Created During Installation



Node Hierarchies

Node hierarchies are used to organize each operator's `Managed Node` window and are directly assigned to OVO users (not assigned to profiles). Each node hierarchy is represented by an icon in the `Node Hierarchy Bank` window. A node hierarchy graphically represents a hierarchical organization of nodes and node layout groups.

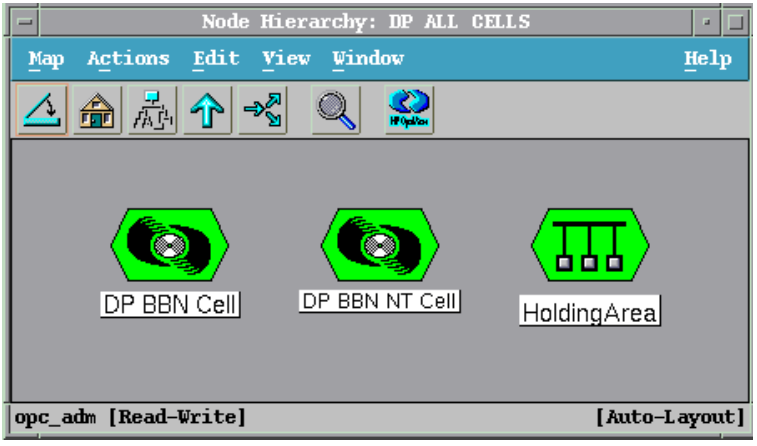
Figure 4-5 Data Protector Integration Node Hierarchy Bank for opc_adm



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

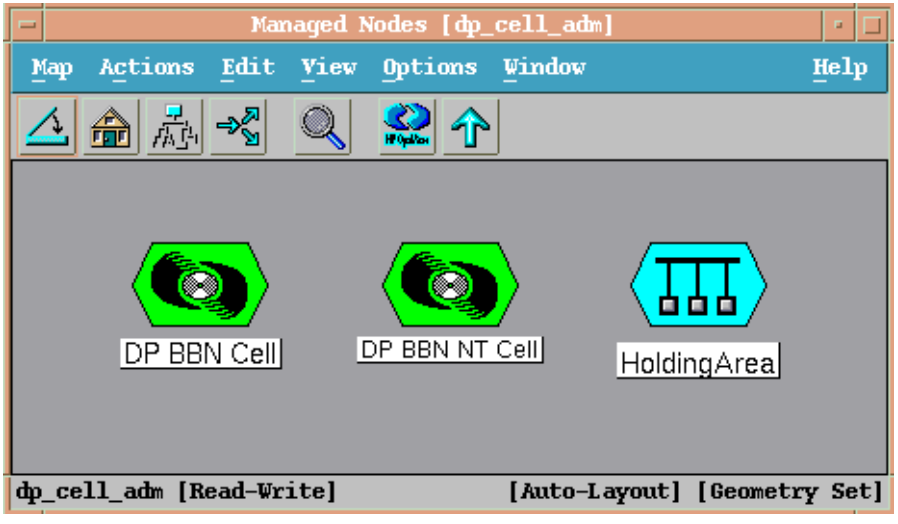
The content of DP ALL CELLS Node Hierarchy is illustrated in Figure 4-7.

Figure 4-6 DP ALL CELLS Node Hierarchy Bank



The content of the Managed Nodes window of the DP_cell_adm user who has been assign the DP ALL CELLS Node Hierarchy by opc_adm is illustrated in Figure 4-7.

Figure 4-7 DP ALL CELLS Node Hierarchy Bank



Application Groups

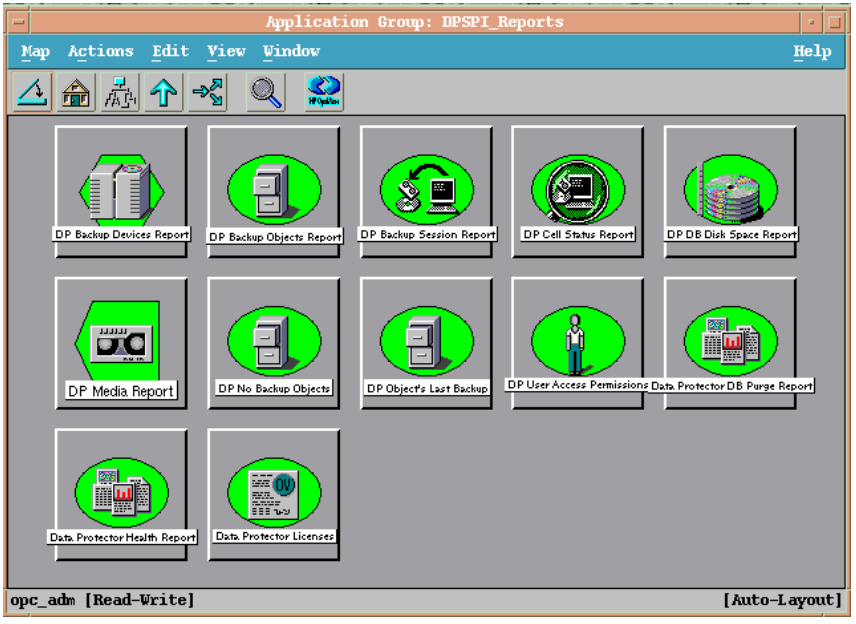
Installation of the Data Protector Integration adds a new application group, `Data Protector Integration Applications` to the OVO `Application Bank` window. It contains the Data Protector-related applications as shown in Figure 4-8. Each OVO user profile has a different set of Data Protector Integration applications to match the responsibilities of the OVO users who have been assigned one of these OVO user profiles.

The two new Data Protector Integration application groups, explained in greater detail in the sections that follow, are `DPSPI_Reports` and `DPSPI_Applications`

DPSPI_Reports Application Group

The Data Protector Integration application group `DPSPI_Reports` contains applications which are intended to be used to monitor the health and performance of the Data Protector environment.

Figure 4-8 Data Protector Integration Application Group: DPSPI_Reports

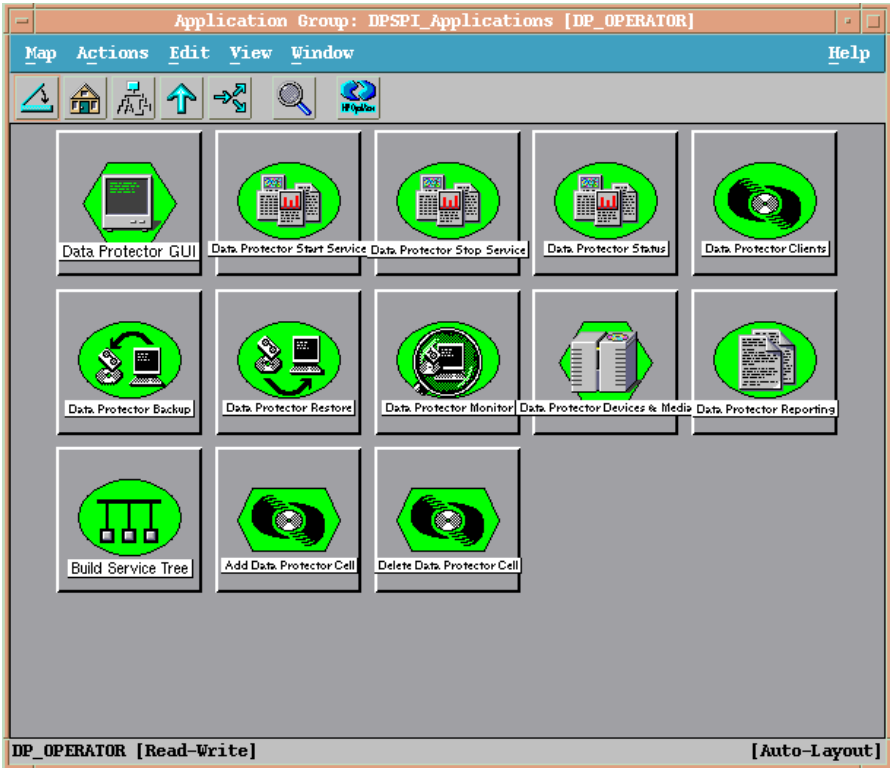


DPSPI_Applications Application Group

The Data Protector Integration application group DPSPI_Applications contains applications that are used to manage the Data Protector environment.

Table 4-9 illustrates the applications contained in the DPSPI_Applications application group.

Figure 4-9 **Data Protector Integration Application Group: DPSPI_Applications**



Users and User Profiles

This section explains the various user concepts in OVO, Data Protector and the Data Protector Integration. It also describes the users and profiles installed by the Data Protector Integration and suggest the most appropriate uses for them.

Data Protector, OVO and Operating System Users

There are two types of users used by Data Protector and OVO to provide access to users. In addition, Data Protector uses Data Protector user groups to define access rights for members of this group:

- **Operating System Users**

  Users required to login to the operating system. A valid user login is required before this user can start Data Protector or login to OVO. For example:

  `EUROPE\janesmith` is a Windows user in the EUROPE domain

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

- **OVO Users**

  OVO requires a login to OVO. Any operating system user can login as an OVO user, provided that the OVO user password is known.

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

  The Data Protector Integration generally does not set up any OVO users. The one exception is the `obspi_template_admin` user. User profiles are provided instead.

- **Data Protector User Group**

  A Data Protector user group defines a set of Data Protector access rights that are available to members of this user group. A member of a user group is identified by its operating system user.

In Data Protector, the operating system user used to log in to the system belongs to a Data Protector user group which determines the access rights and the context of the Data Protector GUI for this user. While for OVO, the operating system user identity is not relevant. The OVO user

used to log in to OVO determines which applications are available in the Application Bank window and which message groups and node groups are used for displaying messages in the message browser.

Data Protector Integration Users

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

- Applications shown in the Application Bank window
- Data Protector cell managers shown in the Managed Nodes window
- Messages groups, in combination with node groups, are used for displaying Data Protector messages in the message browser.

NOTE When the OVO user starts the Data Protector GUI from the Application Bank window, the layout of the Data Protector GUI and the permissions this user has in Data Protector are determined by the operating system user used when logging into OVO and not by the OVO user itself.

OVO User Profiles

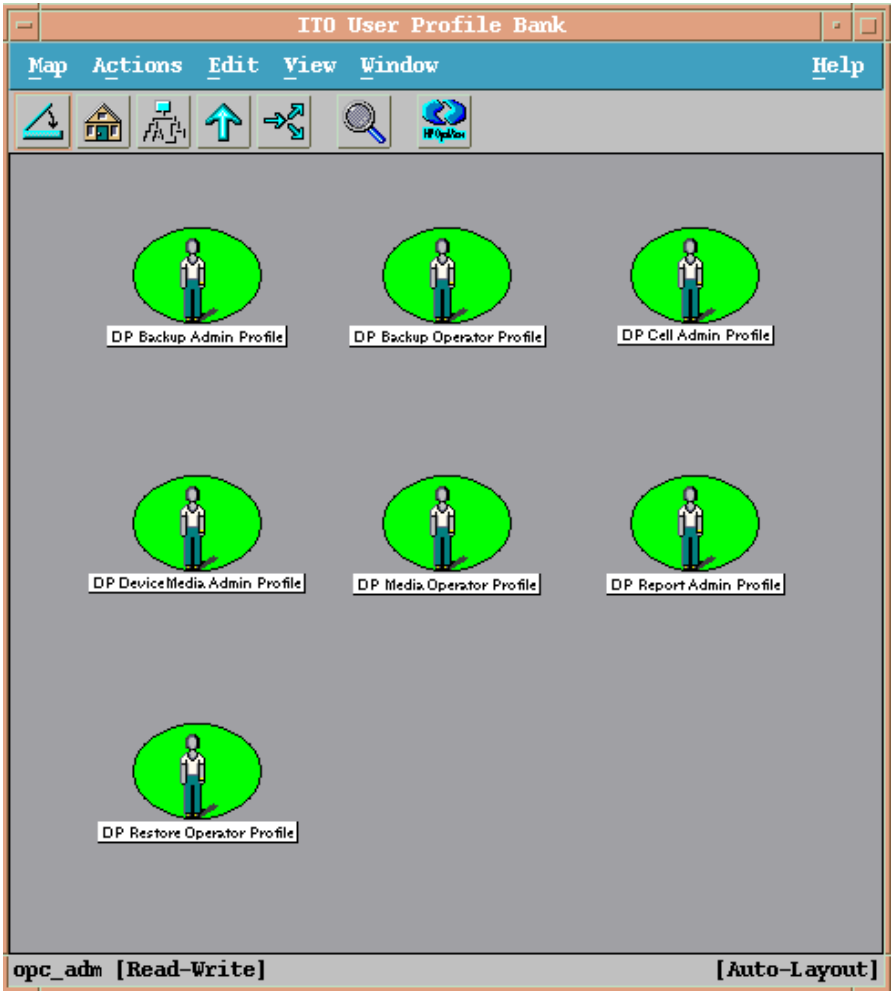
HP OpenView Operations describes the configuration of abstract users with `User Profiles`. User profiles are useful in large, dynamic environments with many OVO users and allow quick set up of OVO users with a default configuration. An OVO user may have multiple user profiles assigned and therefore may simultaneously hold multiple roles.

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

Data Protector OVO User Profiles

The installation of the Data Protector Integration software adds seven new user profiles to the OVO `User Profile Bank` window— four administrators and three operators as illustrated in Figure 4-10. The OVO administrator uses user profiles to simplify process of assigning responsibilities to OVO users.

Figure 4-10 Data Protector Integration User Profiles



The OVO user profiles described in Table 4-1 are provided by the Data Protector Integration and can be used to implement the OVO user roles described in Table 4-2 on page 105:

Table 4-1 Data Protector OVO User Profiles

Administrator / Operator Profiles	Description
DP Backup Administrator	Restricted to a Data Protector Cell. The Application Window shows icons for the following applications: • Data Protector Backup This administrator has access to messages in the OVO Message Browser, if the OVO message template for detailed Messages `DP_Detailed` is enabled.
DP Backup Operator	Restricted to a Data Protector Cell. The Application window shows icons for the following applications: • Data Protector Backup The Message Browser shows messages of the message groups: • DP_Backup • DP_Misc • DP_Mount These are backup session messages and mount requests of backup sessions messages.

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

Administrator / Operator Profiles	Description
DP Restore Operator	Restricted to a Data Protector Cell. The Application window shows icons for the following applications: • Data Protector Restore The Message Browser shows messages of the message groups: • DP_Restore • DP_Misc • DP_Mount These are restore sessions messages and mount requests of restore sessions messages.
DP Device & Media Administrator	Restricted to a Data Protector Cell. The Application Window shows icons for the following applications: • Data Protector Devices & Media This administrator has access to messages in the OVO Message Browser, if the OVO message template for detailed Messages `DP_Detailed` is enabled.
DP Media Operator	Restricted to a Data Protector Cell. The Application window shows icons for the following applications: • Data Protector Backup • Data Protector Restore The Message Browser shows mount requests of backup and restore sessions (`DP_Mount`) messages.

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

Administrator / Operator Profiles	Description
DP Cell Administrator	Restricted to clients of Data Protector Cells. The Application window shows icons for the following 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 The Message Browser shows messages of the messages groups: • DP_Misc • DP_SPI
DP Report Administrator	Restricted to Data Protector Cells. The Application window shows icons for the following applications: • Data Protector Reporting This Administrator is not shown any messages in the Message Browser.

Data Protector OVO Operators

The Data Protector OVO Operators use OVO to maintain, manage, monitor, and control multiple Data Protector cells from a single console. Table 4-2 defines the roles a Data Protector OVO Operator might have and describes the appropriate access rights of an equivalent Data Protector user.

NOTE

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

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

Table 4-2 Data Protector OVO Operators and their Roles

Role	Data Protector 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 their own backup specification.
	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.

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

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

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

Role	Data Protector Privileges	Description
Restore Operator	Starts restore on demand (from which device, what to restore, to which system), and monitors the status of the restore session, and responds to mount requests by providing media to devices.	
	Restore to other clients	Allows a user to restore an object to a system other than the one where the object was backed up.
	Restore from other users	Allows a user to restore objects belonging to another user. This is a UNIX specific user right.
	Restore as root	Allows a user to restore objects with the rights of the root UNIX user. Note that this is a powerful right that can affect the security of your system. This user right is required to run any 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.

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

Role	Data Protector Privileges	Description
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.

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

Role	Data Protector Privileges	Description
Cell Administrator	Installation and update of Data Protector client systems, add, delete, or modify Data Protector users and groups and administer the Data Protector database.	
	Client configuration	Allows a user to perform installation, and an update of client systems.
	User configuration	Allows a user to add, delete and modify users or user groups. Note that this is a powerful right.
	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.
	See private object	Allows a user to see private objects. This Data Protector user right has to be granted to database administrators.
Report Administrator	Create and modify Data Protector reports.	
	Reporting and notifications	Allows a user to create Data Protector reports. To use Web Reporting, you also need a java user under applet domain in the admin user group.

obusergrp.pl User Groups Tool

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

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

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

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

NOTE

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

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

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

Data Protector Template Administrator

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

OVO Administrator

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

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

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

Monitored Objects

OVO monitors thresholds of an object to help early detection of problems. If an object exceeds a threshold for a specified period of time, a message can be sent to the OVO operator. This message 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

The processes that run permanently on the Data Protector Cell Manager are:

- Cell Request Server (crs)
- Media Management Daemon (mmd)
- Raima Velocis Database Server (rds)

Only one instance of each process must be running.

Threshold: Number of processes <3

Polling interval: 10 min

Message structure:

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

Databases

Checks amount and percent of used available space.

Threshold: >= 95% for error
>= 80% for warning

Command: `omnidbutil -extend info`

Polling interval: 60 min

Message structure:

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

Media Pool Status

Checks if there are media pools with media status:

Poor (Critical)

Fair (Warning).

Polling interval: 60 min

Message structure:

Message Group	DP_Misc
Applications	Data Protector
Note	<name_cell_manager>.
Severity	Critical or Warning
Service Name	Services.Data Protector.<cell name>
Object	DP_CheckPoolStatus_NT on Windows DP_CheckPoolStatus_UX on UNIX
Operator Action in case of problem	Status of the Media Pool
Message Text when problem has been solved	Auto acknowledge this message and the preceding problem message

Media Pool Size

Checks the amount of used space:

Threshold: >= 95% of total available space is Critical
>= 85% of total available space is Warning

Command: `omnimm -list_pool -detail`

Polling interval: 60 min

Message structure:

Message Group	`DP_Misc`
Applications	`Data Protector`
Note	`<name_cell_manager>`.
Severity	Critical or Warning
Service Name	`Services.Data Protector.<cell name>`
Object	`DP_CheckPoolSize_NT` on Windows `DP_CheckPoolSize_UX` on UNIX
Operator Action in case of problem	Status of the Media Pool
Message Text when problem has been 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 hrs (Critical)

8 hrs (Warning).

Polling interval: 60 min

Message structure:

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

Check Important Configuration Files

HP-UX Systems

Checks if the following files exist. The usage of these files is described in:

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

Polling interval: 15 min

Windows Systems

Checks if the following files exist.

They are located in subdirectories of the Data Protector configuration directory, the default location being:

`C:\Program Files\OmniBack\Config\`

The usage of these files is described in:

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

Polling interval: 15 min

Monitored Logfiles

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

Four Data Protector logfiles are monitored for warning and error patterns. Basic information is provided in *HP OpenView Storage Data Protector Administrators' Guide*, in chapter 12, Troubleshooting, Data Protector Log Files and in Appendix A, Further Information, Data Protector Log Files Exemplary Entries.

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 fix and not language dependant. The format is:

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

The parameters for messages for the default logfiles are:

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

The following messages will be captured and forwarded to OVO's message browser:

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

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

inet.log

This logfile provides security information. The messages document requests to the `inet` process from non-authorized systems. The data/time format depends on the value of the language environment variable. The following messages are captured and forwarded to OVO's message browser:

```
06/14/01 09:42:30  INET.12236.0 ["inet/allow_deny.c /main/7":524] A.04.00 b364
A request 0 came from host Jowet.mycom.com which is not a cell manager of this client

Thu Jun 14 09:42:30 2001 [root.root@jowet.mycom.com] : .util
06/14/01 09:43:24  INET.12552.0 ["inet/allow_deny.c /main/7":524] A.04.00 b364

A request 1 came from host jowet.mycom.com which is not a cell manager of this client
Thu Jun 14 09:22:46 2001 [root.sys@jowet.mycom.com] : .util

6/14/01 10:17:53 AM  CRS.411.413 ["cs/mcrs/daemon.c /main/145":1380] A.04.00 b364
User LARS.R&D@cruise2000.mycom.com that tried to connect to CRS not found in user list
```

Data Protector Database Logfile

There is a `purge.log` logfile on Cell Manager systems only. 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 value of the language environment variable. The following messages will be captured and forwarded to OVO's message browser:

```
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.
```

The parameters for messages for the default logfiles are:

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

Data Protector Media Logfile

There is a media.log logfile on the Data Protector Cell Manager.

media.log

This logfile contains information about media:

- time
- medium id
- medium label
- type of operation or session id in which medium is used

The following messages will be captured and forwarded to OVO's message browser:

```
06/13/01 13:58:19 0a1104aa:3b27555a:4057:0001 "Default File_1" [INITIALIZATION]
06/13/01 14:30:33 0a1104aa:3b275ce9:6bb6:0001 "Default File_4" [INITIALIZATION]
06/14/01 14:38:43 0a1104aa:3b275ce9:6bb6:0001 "Default File_4" [2001/06/14-1]
06/18/01 14:05:14 0a1104aa:3b28a5f4:5e64:0001 "Default File_1" [2001/06/18-1]
06/19/01 10:44:23 AM b902110a:3b2727e1:00b9:0001 "Default File_3" [AUTOINITIALIZATION]
06/19/01 10:44:23 AM b90 2110a:3b2727e1:00b9:0001 "Default File_3" [2001/06/19-12]
06/21/01 1:38:13 PM 3578880f:3ce24f81:05c4:0001 "Default File_1" [IMPORT]
06/21/01 1:42:54 PM 3578880f:3ce39b3c:08fc:0001 "Default File_2" [COPY]
```

The parameters for messages for the default logfiles are:

Message Group	DP_Misc
Applications	Data Protector
Note	<name_system> on which logfile resides
Severity	Operation type or session id exists NORMAL All other messages WARNING
Service Name	Services.Data Protector.<cell name>
Object	<logfile name>
Automatic Action	

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, for example, SNMP traps.

debug.log	Exception messages that have not handled
RDS.log	Raima Database service messages
readascci.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	Contains detailed errors during backup or restore sessions, i.e. error while parsing the backup specification. No message catalog is used. The time/date format differs depending on the language environment variable.

5 Performance Measurement with the HP OpenView Performance Agent

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

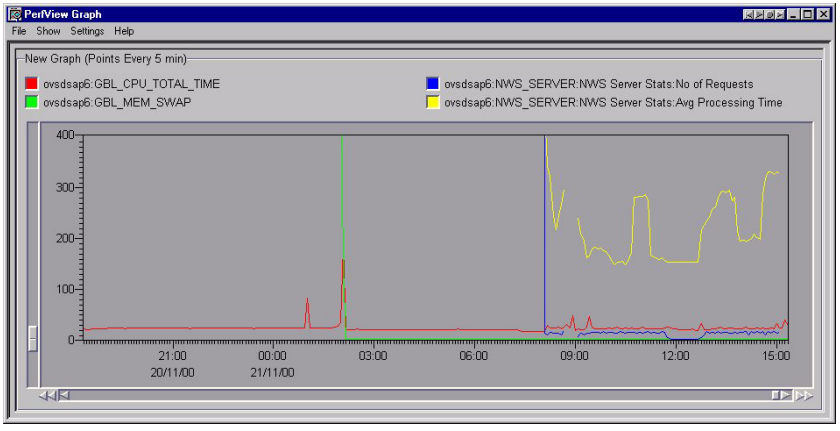
- Storing of Performance data
- Configuration
- Installation
- De-installation

Integration Overview

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

The OVPA also collects many metrics from the operating environment, for example, I/O, network, and processes, and stores them in logfiles. Data Protector uses the ARM interface to measure the duration of transactions. These transaction durations are also collected by the HP OpenView Performance Agent. It is possible to direct additional sources of performance data into the OVPA via DSI (Data Source Integration) which is used to put performance data for the Data Protector environment into the OVPA. The collected data can be viewed centrally by the OVP Console to show trends and can also be combined with the internal data or data from other applications to get correlations, for example, to the CPU utilization or network data.

Figure 5-1 HP OpenView Performance Console

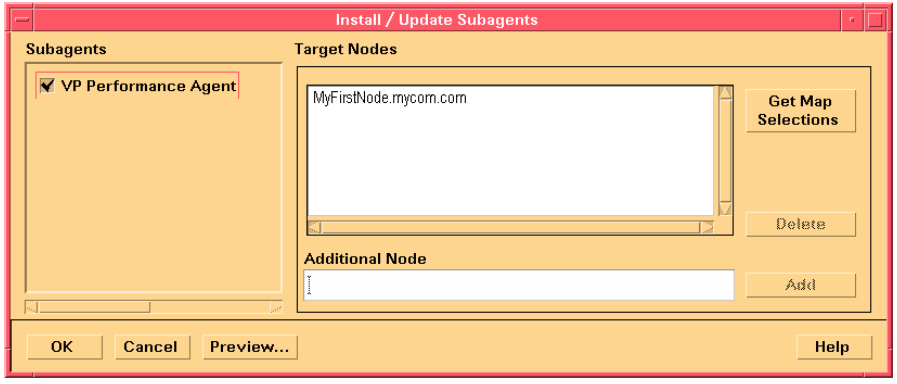


The performance measurement forms the basis for evaluating what corrective actions need to be made in order to optimize performance and resource utilization of the Data Protector environment. Typically, this is an off-line operation where a window of time is selected for detailed analysis of system performance,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

Installing Performance Agent

To be able to use the Performance Integration of the Data Protector Integration, the OVPA has to be running on all agent nodes running Data Protector Cell Managers. This can be accomplished by performing the following steps:

Figure 5-2 Installing the Performance Integration



Distribute and start the HP OpenView Performance subagent and starting it:

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

Installing Performance Integration Components

Installation Steps for Window Nodes

After installation of the Data Protector Integration on the OVO management server the configuration files for the OVPA integration reside in the directory:

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

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

1. Transfer the zip file to the managed node by using ftp.
2. Install the files in the OVPA directory. While unzipping the zip file, ensure that the files are copied to the appropriate OVPA directories. To do this:
   a. Open the `obspi_vpp.zip` file with the WinZip application.
   b. Select the parent directory of the OVPA Installation as the extraction directory, which is usually:

      `C:\`

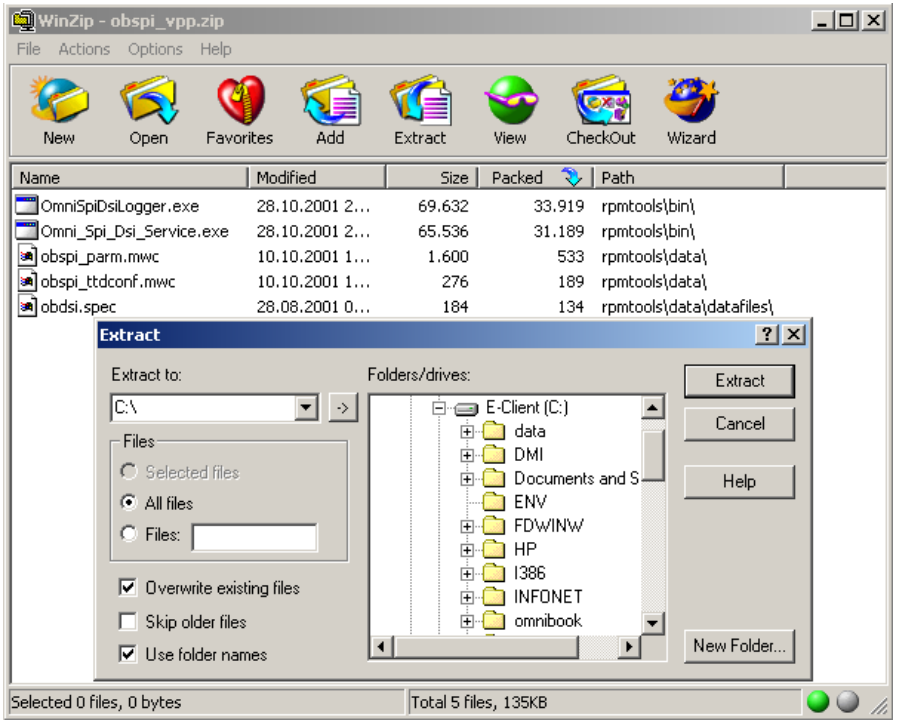
   c. Click the extract button to unzip the files to the chosen directories.

After unzipping, the following files are installed:

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

- `rpmtools\data\datafiles\obdsi.spec`

Figure 5-3 Installing the Performance Integration



Installation Steps for UNIX Nodes

After installation of the Data Protector Integration on the OVO management server, the configuration files for the OVPA integration reside in the directory:

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

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

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

   `tar -xf obspi_vpp.tar`

After decompressing, the following files reside in the directory:

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

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

Collect ARM Transactions

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

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

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

Windows	`rpmtools\data\parm.mwc`
	`rpmtools\data\ttdconf.mwc`
UNIX	`/var/opt/perf/parm`
	`/var/opt/perf/ttd.conf`

Modifying the parm File

To modify the `parm` file to enable ARM transaction tracking:

1. Open the `parm` file in an editor.
2. Find the line which specifies the types of data that the OVPA is to log.

   The entry has the form:

   ```
   log global process application transaction dev=disk
   ```

3. Set transaction parameter to:

   `transaction=correlator`

Modifying the ttd.conf File

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

1. Before you make any changes to the `ttd.conf` file, shut down:
   - the HP OpenView Performance Agent service
   - all ARM instrumented applications.

   See the HP OpenView Performance Agent handbook “Tracking your Transactions” for further information.
2. Open the `ttd.conf` file in an editor.
3. Delete the default line:

   ```
   tran=* range=0.5,1,2,3,5,10,30,120,300 slo=5.0
   ```
4. Add the following lines to collect all Data Protector ARM transactions.

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

   You can find the complete syntax for monitoring the Data Protector ARM transactions in the following files, after installation of the Data Protector OVPA integration:

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

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

   See Table 5-1 for an overview of the syntax.

Table 5-1 ARM Transactions Syntax Overview

Transaction Name	Additional Information	Transaction Description
BS-<Backup_specification>	Time	Duration of a backup session
RS-<Session_ID>	Time	Duration of a restore session
BO-<Object_name>	Time	Duration of a backup of a specified object
DP	Number of purged records and database size in MB	Duration of the Data Protector database purge
DC	Database size in MB	Duration of the Data Protector database check

5. On HP-UX 11.x:

   Replace the `/opt/omni/lib/arm/libarm.sl` with a softlink of the same name to `/opt/perf/lib/libarm.0`

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

Once these modifications are made to the `ttd.conf` file, you can collect transaction information about the task executed by Data Protector listed in Table 5-1.

Collecting Data Protector Process Data

Data Protector runs processes dedicated to the specific tasks handled by the Cell Manager, the Media Agent, the Disk Agent, and the Installation Server. You can use the OVPA to collect process data from the various tasks. To do this, you must modify the `parm` file.

You can find the complete syntax for monitoring the Data Protector processes in the parm files which are located in:

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

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

directory after the installation of the Data Protector OVPA integration.

NOTE It is possible to collect process information about any nodes that are Data Protector clients, because a Data Protector Disk Agent or a Data Protector Media Agent runs on all Data Protector nodes.

Modifying the parm File on a Data Protector Cell Manager

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

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

Modifying the parm File on a Data Protector Media Agent

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

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

Modifying the parm File on a Data Protector Disk Agent

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

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

Modifying the parm File on a Data Protector Installation Server

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

```
application Installation_Server
file OmniInet bmsetup
```

Performance Agent Data Source Integration

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

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

The metrics collected are:

- Number of clients controlled by the Data Protector Cell Manager
- Size of the database used by the Data Protector Cell Manager

To collect these metrics, you must complete the following steps:

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

Compiling the obdsi.spec File

To be able to store the collected data in the OVPA database, you must create a logfile set. To create the logfile, set you need to compile the class specification file `obdsi.spec` with the OVPA command `stdlcomp`. The `obdsi.spec` files are located in the following directories after the installation of the Data Protector OVPA integration:

Windows	`<Performance Agent Root>\Data\Datafiles`
UNIX	`/opt/OV/OpC/integration/obspi/vpp/`

The `sdlcomp` command has the following syntax:

```
sdlcomp specification_file logfile_set
```

`specification_file`	Name of the class specification file. If it is not in the current directory, it must be fully qualified.
`Logfile_set`	Name of the logfile set. For the Data Protector Data Source Integration, the name *must* be **`omniback`**. If you do not specify a path, the logfile set is created in the current directory. There is no restriction to where you choose to store your logfiles during compilation, but you *must not* move them once they have been compiled.

An example of the usage of the `sdlcomp` command for compiling the Data Protector specification file:

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

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

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

Collecting Data on Windows Nodes

Installing the Data Protector DSI Log Service

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

After the installation of the Data Protector OVPA integration, the service installation file `omni_spi_dsi_service.exe` resides in the directory:

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

To install the Data Protector DSI Log service, type the following command:

```
Omni_spi_dsi_service.exe -i
```

This registers the service in the Service Control Manager.

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

Start → Settings → Control Panel → Administrative Tools → Services

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

Starting the Data Protector DSI Log Service

To start collecting data, you must start the Data Protector DSI Log service in one of the following ways:

- Enter the command:

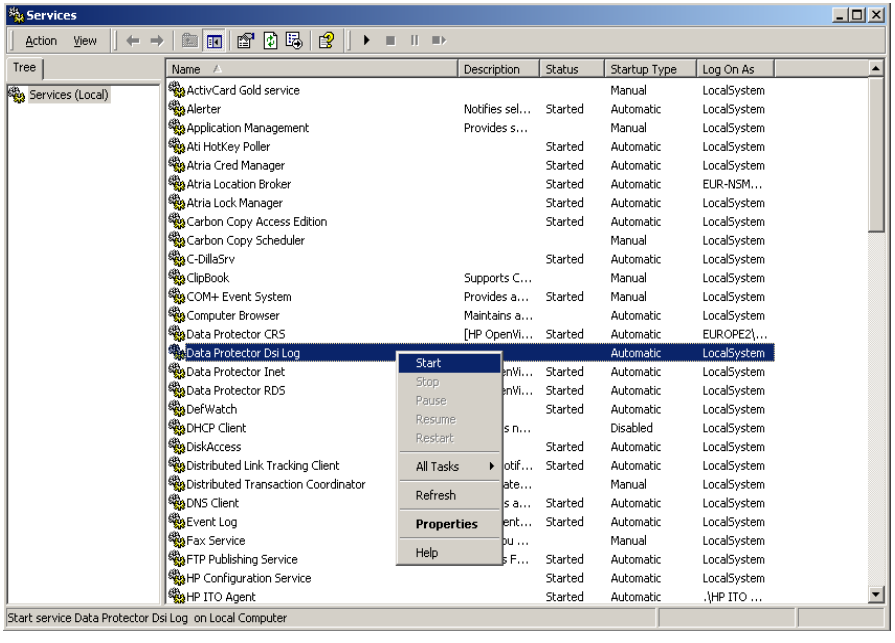
  `Omni_Spi_Dsi_Service.exe -s`

- From the Service Control Manager GUI, go to:

  Start → Settings → Control Panel → Administrative Tools → Services

  and right-click the `Data Protector Dsi Log` service and select the start option in the context menu (see Figure 5-4 on page 137).

Figure 5-4 Starting the Data Protector Dsi Log Service



Specifying the Data Collection Frequency

The default data collection frequency is 12 minutes. This is the same time configured in the `obdsi.spec` file which is used to create the OVPA logfile set. If you want to change the collection frequency, you need to change the appropriate entry in the `obdsi.spec` file (see HP OpenView Performance *Agent Data Source Integration Guide*), create a new logfile set using sdlcomp, and configure the Data Protector `Dsi Log` service accordingly.

To to specify a a new data collection frequency, you must do one of the following:

- Enter the command:

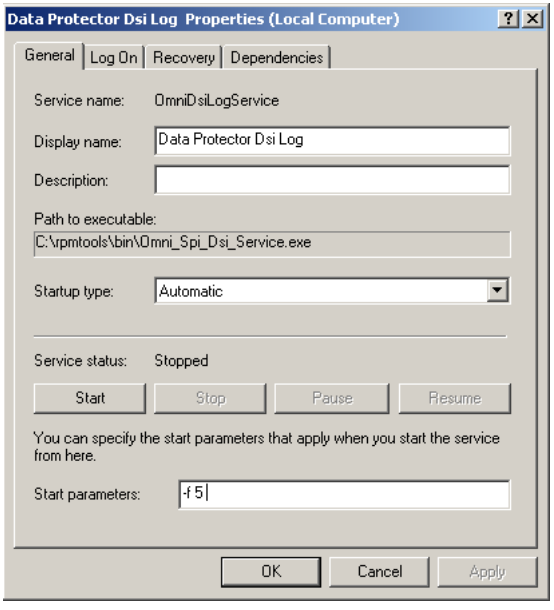
  `Omni_Spi_Dsi_Service.exe -s -f <minutes>`

- From the Service Control Manager GUI, go to:

  Start → Settings → Control Panel → Administrative Tools → Services

  and double click the `Data Protector Dsi Log` service, select the **General** tab and input the start `parameter -f` minutes in the textbox (see Figure 5-5).

Figure 5-5 Data Protector Dsi Log Properties



Configuring the Data Protector DSI Log Service

To enable tracing options for the `Data Protector Dsi Log` service, you must configure the service to provide the path of the trace file and the level of tracing information. You can do this with the command:

`Omni_Spi_Dsi_Service.exe -t [TracePath]`

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

If the `-t` option is not used to enable tracing, no trace files will be written.

To specify the type of information that is written to the trace files, you can configure the trace level for the `Data Protector Dsi Log` service. There are 4 tracing levels which contain the following information.

Trace Level 1: Error Information

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

Trace Level 3: Shows information about the current service activities.

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

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

`Omni_Spi_Dsi_Service.exe -v tracelevel`

where the `tracelevel` value must be between 1 and 4.

The `Data Protector Dsi Log` service uses another executable, the `OmniSpiDsiLogger.exe` to collect the data. These executable reside after the installation in the:

`<Performance Agent Root>\Bin`

directory. By default, the service uses this directory to find the executable. So if you have relocated this file, you must specify the new path to the file. To do this use the command:

`Omni_Spi_Dsi_Service.exe -x path/name`

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

The configuration data is stored in the registry. It is possible to modify this data manually from the registry itself. The information is stored under the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OmniDsiLogService`

To disable tracing, you must remove the registry value:

`TraceFilePath`

from the registry key above.

Deinstalling the Data Protector DSI Log Service

Before you can remove the files `Omni_Spi_Dsi_Service.exe` and `OmniSpiDsiLogger.exe`, you must uninstall the registered service. To do this use the command:

```
Omni_Spi_Dsi_Service.exe -u
```

Collecting Data on UNIX Nodes

In order to collect the Data Protector data and store it in the compiled logfile set on UNIX nodes, you must make the `obdsi.ksh` script run as a shell-independent daemon.

To do this, use the UNIX at command as follows:

```
at now

'/opt/OV/OpC/integration/obspi/vpp/obdsi.ksh | dsilog
/var/opt/perf/datafiles/Omniback OMNIBACKII'

Ctrl-D
```

Performance Alarms for the Performance Agent

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

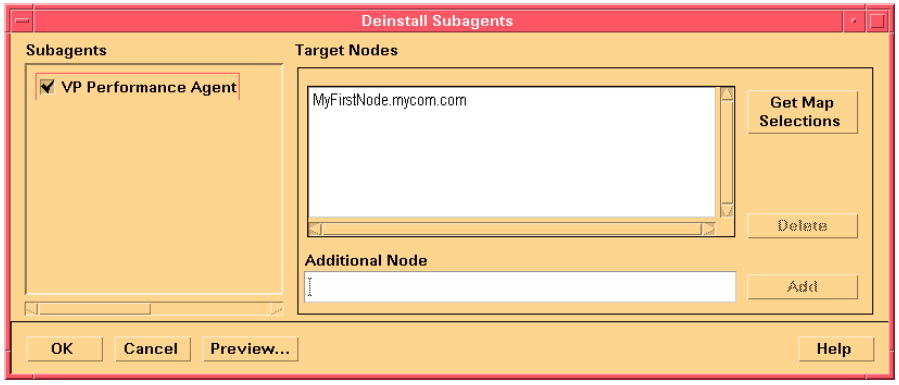
Deinstalling the Performance Agent

If desired and if they are not being used by other solutions, the HP OpenView Performance Agent can be deinstalled after deinstallation of the Data Protector Integration. To do this:

Delete running HP OpenView Performance subagents with the following commands:

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

Figure 5-6 Deinstalling the Performance Integration



Index

Index

Index

Index

Index