HP OpenView Storage Data Protector

Integration Guide
for
HP OpenView

Version: A.05.50

HP-UX, Solaris and Windows

Manufacturing Part Number: B6960-90117

October 2004

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. UNIX® is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

X Window System is a trademark of the Massachusetts Institute of Technology.

Motif is a trademark of the Open Software Foundation, Inc. in the U.S. and other countries.

Windows NT™ is a U.S. trademark of Microsoft Corporation. Microsoft®, MS-DOS®, Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle®, SQL*Net®, and Net8® are registered U.S. trademarks of Oracle Corporation, Redwood City, California. Oracle Reports™, Oracle7™, Oracle7 Server™, Oracle7 Backup Utility™, Oracle8™, Oracle8 Server Manager™ and Oracle8 Recovery Manager™ are trademarks of Oracle Corporation, Redwood City, California.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

ARM® is a registered trademark of ARM Limited.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

VisiCalc® is a U.S. registered trademark of Lotus Development Corp.

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.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation.

OpenView® is a registered U.S. trademark of Hewlett-Packard Company.

Other reserved names are trademarks of the respective companies.

Contents

1. Introduction

Overview 18
Data Protector 18
OpenView Products Integrated with Data Protector 18
OpenView Operations 18
Service Level Management Integrations 18

2. Data Protector-SIP Integration

Introduction 20
Prerequisites 20
Product Capabilities and Integration Benefits 20
Component List 21
Dependencies 21
Data Protector/SIP Integration 22
Data Protector Integration Module 23
Cell Request Server (CRS) 23
How Data Protector Integrates with SIP 23
Deployments 25
Deployment A 25
Deployment B 26
Deployment C 27
Setup Process 28
Installation Procedures 28
Prerequisite Information 28
On the Data Protector Server 29
Establishing Data Protector/SIP Communication 29
Installing on a SIP Server 29
Installing on a Windows NT SIP Server 29
Installing on an HP-UX SIP Server 29
Installing on a Web Server 30
Installing on a Windows Web Server 31
Installing on an HP-UX Web Server 31
Customization 33
Setting Up Backup Groups on Data Protector 33
Editing ConfigSpec.xml 34
Creating Customer Models and Portal Views 38
Customer Models 38
Importing the Customer Model 39

Management Data Filter 40

Adding and Removing Services in a Portal View 41

Error Messages Module 42

Understanding Data Protector Error Messages 42

Data Protector Error Messages 42

Editing Data Protector Message Modules 44

Editing the PortalView.XML File Directly 44

Protection Status Module 45

Understanding the Protection Status Module 45

Protection Status Gauge 45

All Hosts Backup Statistics Report 46

Client Host Backup Report 47

Host Statistics Report 48

Detail View 49

Editing the Backup Health Module 50

Using the Backup Health - Edit page 50

Backup Health Criteria 51

Directly Editing the PortalView.xml File 51

Data Protector Reports Module 52

Understanding Data Protector Reports 52

Data Protector Reports 52

Editing the Data Protector Reports Module 54

Using the Reports - Edit page 54

Directly Editing the PortalView.xml File 55

Establishing Global Settings for Reports 55

Troubleshooting 56

Error Messages 56

Data Unavailable 56

Parse Rest of Config 56

3. Data Protector-OVO-SIP Integration

Introduction 58

Prerequisites 58

Product Capabilities and Integration Benefits 58

Component List 60

Data Mappings 61

Dependencies 62

Setup Process 64

Installation 64
Configuration 65
Sample Configuration Files 65
Editing Configurations 66
Configuring the Management Stations 66
Updating the Customer Model 67
Creating a SIP User/Role Package 68
Add Password Authentication (optional) 71
Finalize the Configuration 73
Troubleshooting 76

4. Data Protector-OVR Integration
Introduction 78
Prerequisites 78
Product Capabilities and Integration Benefits 78
Component List 80
How Data Protector Integrates with OVR 81
Dependencies 82
Data Protector/OVR Integration 83
DP/OVO/OVR Integartion 83
DP/OVPA/OVR Integration 83
DP/OVR Integration 83
Setup Process 84
Configuration 84
Error Messages 84
Troubleshooting 85
Creating Custom Reports 86
Introduction. 86
Creating Data Protector Custom Reports 86
Data Source 87
Message Format 90

5. Data Protector-OVO-OVSD Integration
Introduction 94
Prerequisites 94
Product Capabilities and Integration Benefits 94
Component List 96
Import Mapping and Data Exchange 97

Integration Feature for Backup Operations 98
Dependencies 99
Setup Process 100
Installation and Configuration for General Integration. 100
On the Service Desk Application Server:. 101
On your OVO Server Running on UNIX:. 101
Exporting OVO Services as Services into Service Desk 101
Installation and Configuration for a Backup-Specific Integration 102
On your OVO Management Server Running on UNIX. 102
On the Service Desk Application Server 104
Customization 106
Example 106
On the Service Desk Application Server 106
On your OVO Server Running on UNIX:. 108

Printing History

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

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

Table 1 **Edition History**

Part Number	Manual Edition	Product
B6960-90069	August 2002	HP OpenView Storage Data Protector A.05.00
B6960-90090	April 2003	HP OpenView Storage Data Protector A.05.10
B6960-90117	October 2004	HP OpenView Storage Data Protector A.05.50

Conventions

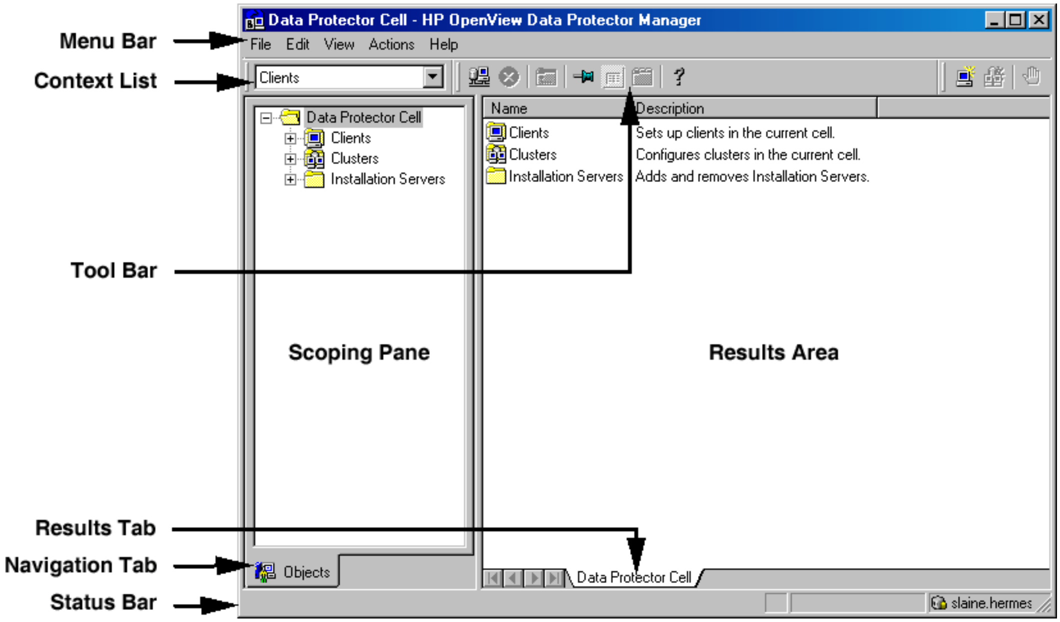
The following typographical conventions are used in this manual.

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...
	Text that you must enter	At the prompt, type: `ls -l`
Keycap	Keyboard keys	Press **Return**.

Data Protector provides a cross-platform (Windows and UNIX) graphical user interface.

Figure 1 **Data Protector Graphical User Interface**



Name	Description
Clients	Sets up clients in the current cell.
Clusters	Configures clusters in the current cell.
Installation Servers	Adds and removes Installation Servers.

Contact Information

General Information

General information about Data Protector can be found at

http://www.hp.com/go/dataprotector

Technical Support

Technical support information can be found at the HP Electronic Support Centers at

http://support.openview.hp.com/support.jsp

Information about the latest Data Protector patches can be found at

http://support.openview.hp.com/patches/patch_index.jsp

For information on the Data Protector required patches, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

HP does not support third-party hardware and software. Contact the respective vendor for support.

Documentation Feedback

Your comments on the documentation help us to understand and meet your needs. You can provide feedback at

http://ovweb.external.hp.com/lpe/doc_serv/

Training Information

For information on currently available HP OpenView training, see the HP OpenView World Wide Web site at

http://www.openview.hp.com/training/

Follow the links to obtain information about scheduled classes, training at customer sites, and class registration.

In This Book

The *HP OpenView Storage Data Protector Integration Guide for HP OpenView* describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Information Portal, HP OpenView Service Desk, and HP OpenView Reporter.

NOTE

This manual describes Data Protector functionality without specific information on particular licensing requirements. Some Data Protector functionality is subject to specific licenses. The related information is covered in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Audience

This manual is intended for backup administrators or operators who plan to install and configure the integration of Data Protector with HP OpenView Service Information Portal, HP OpenView Service Desk, and HP OpenView Reporter.

Conceptual information can be found in the *HP OpenView Storage Data Protector Concepts Guide,* which is recommended in order to fully understand the fundamentals and the model of Data Protector.

Organization

The manual is organized as follows:

Chapter 1	“Introduction” on page 17.
Chapter 2	“Data Protector-SIP Integration” on page 19.
Chapter 3	“Data Protector-OVO-SIP Integration” on page 57.
Chapter 4	“Data Protector-OVR Integration” on page 77.
Chapter 5	“Data Protector-OVO-OVSD Integration” on page 93.

The integrations of Data Protector with the following database applications are described in the *HP OpenView Storage Data Protector Integration Guide*:

- Microsoft SQL Server 7.0/2000
- Microsoft Exchange
- Microsoft Exchange 2000

The integrations of Data Protector with the following applications is described in the *HP OpenView Storage Data Protector Administrator's Guide*:

- Microsoft Cluster Server
- MC/ServiceGuard
- Data Source Integration
- Application Response Measurement
- ManageX

1 Introduction

Overview

This chapter provides a brief overview of Data Protector, the HP OpenView product integrated with it to create an enterprise-wide solution that provides service level management, and the integration itself.

Data Protector

HP OpenView Storage Data Protector is a backup and recovery solution that provides reliability and protection for your fast growing business data. Data Protector offers comprehensive backup and restore functionality designed specifically for enterprise wide and distributed environments.

Data Protector also provides information that can be used, through reports and messaging tools, to help you monitor the status of your processes, in addition to providing backup and recovery functionality.

OpenView Products Integrated with Data Protector

Data Protector is designed to allow the integration of other HP OpenView products, in order to provide you with an enterprise-wide solution for your IT environment. Integrations with HP OpenView is described in this manual.

OpenView Operations

OpenView Operations is a central management point for various remote OpenView applications. Collects and analyzes data, automates critical response, as well as message forwarding to other services.

Service Level Management Integrations

Data Protector and the HP OpenView products listed above are integrated to create an enterprise-wide solution that provides service level management. The integrations are introduced below:

2 Data Protector-SIP Integration

Introduction

This section describes how to install, configure, and use Data Protector with OpenView Service Information Portal to serve customer-defined reports in the portal.

Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Service Information Portal

Product Capabilities and Integration Benefits

The integration of Data Protector and OpenView Service Desk (Service Desk) helps enable Service Level Management (SLM) to help you achieve a specific, consistent, measurable level of service. In short, this integration helps you achieve maximum service availability by providing a simple, effective way to:

- Convenient data protection service monitoring through web access from any machine.
- Specification of resource in terms of machine and group names.
- Segmentation of accessible data by the different backup administrators.
- Information aggregation from other services (not related to Data Protector) to the portal, using SIP's configuration mechanisms. Single presentation format for all modules.
- Easy configuration: GUI configuration editor and XML document editing only.
- Stability and reliability. The integration modifies very little code and relies upon SIP customization features and components.

Component List

- Data Protector - A backup solution that provides reliable data protection and maximum accessibility for your business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.
- OV SIP (OpenView Service Information Portal) - A tool that aggregates information collected from various services. The information is presented and formatted through various portal components and is made available through a web page. Portal components and modules include Service Browser, Service Graph, and Service Cards.

Dependencies

- Sun's Java Developer's Kit 1.3 is required for SIP.
- Some OpenView components require that Netscape Navigator 4.7 be installed. This step is unnecessary and may be skipped as long as alternative means of browsing HTML pages is available (e.g., a web browser on a separate machine, or an alternative compatible web browser).
- Successful configuration must also comply with the software requirements as described in the table below.
- The environment must be properly set and configured prior to the installation of the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about the specific requirements, please refer to the installation guides for those components.
- This integration uses Data Protector backup specification groups. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* and the Data Protector online help for more information about backup specification groups and how to configure them.

Table 2-1 Software Requirements

Component	Version	Operating System
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
SIP	3.0	HP-UX 11.0 Solaris 8 Windows 2000

Table 2-2 Patch Requirements

Platform	Patch Number	Description
HP-UX	PHSS_28254	SIP Server patch
	PHSS_28268	SIP Topology Module patch
Solaris	OVSIPSOL_00012	SIP Server patch
	OVSIPSOL_00013	SIP Topology Module patch
Windows 2000	OVSIPNT_00011	SIP Server patch
	OVSIPNT_00012	SIP Topology Module patch

Data Protector/SIP Integration

The Data Protector/SIP integration consists of two major elements:

- The *Data Protector Integration module*, installed on the SIP server or on a separate web server.
- The *Cell Request Server process*, installed on the Data Protector cell manager.

These elements are described in detail in the sections that follow.

Data Protector Integration Module

The Data Protector Integration module components are automatically installed along with SIP, and are located either on your SIP web server or on a separate web server, depending on your deployment.

This integration module consists of two primary elements:

- SIP components, including SIP XML, XSL, and module definitions.
- SIP-Data Protector servlets, including the Java servlets described below, as well as the Configuration Specifications, `ConfigSpec.xml`.

This integration uses three Java servlets to communicate between SIP and Data Protector.

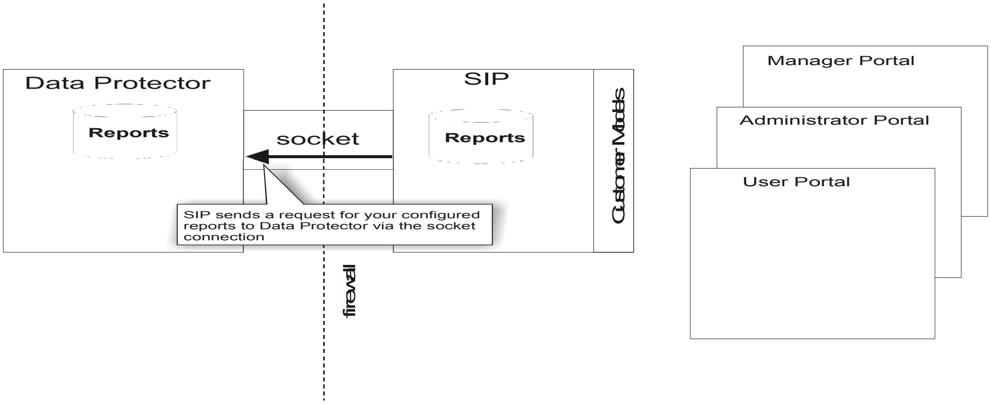
- The `CustomerGroup` servlet provides the customer model to the SIP Management Data Filter.
- The `Reporter` servlet generates and creates XML reports, and also includes a configurable threading option.
- The `StatusGauge` servlet generates status gauges.

Cell Request Server (CRS)

The other main element of the Data Protector-SIP integration is the Cell Request Server (CRS) process in Data Protector cell manager. The CRS serves reports to SIP via the socket. For information on configuring this module, see “Setup Process” on page 28.

How Data Protector Integrates with SIP

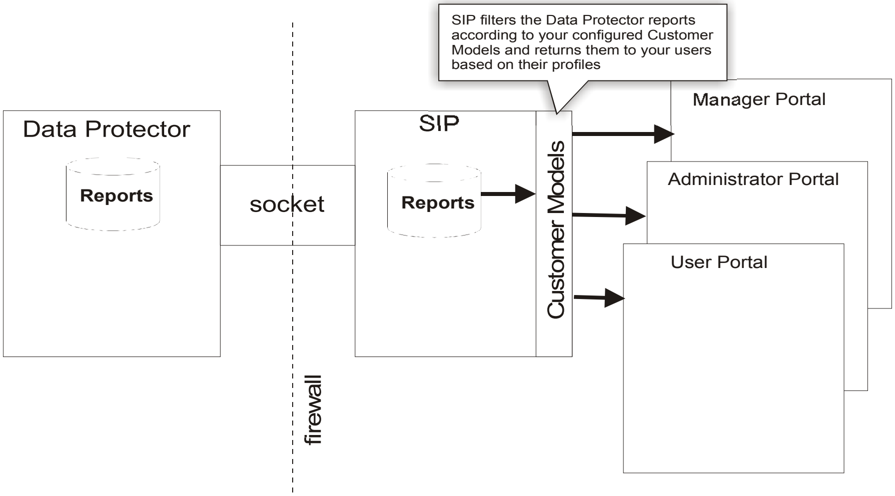
To integrate with SIP, Data Protector’s CRS daemon serves reports to the Java servlets on the SIP or web server, as shown in the following illustrations.



SIP sends a request for your configured reports to Data Protector via the socket connection

When a user requests a report, as in the illustration above, the request goes to the Customer Group servlet, which then maps that user to the group or groups in his or her customer profile. The Customer Group servlet then sends the request to Data Protector's report database via the socket connection between the SIP portal and Data Protector.

After Data Protector receives the user request for data, it sends report data via the socket connection to the Docs servlet and/or the Gauges servlet to be formatted.


SIP filters the Data Protector reports according to your configured Customer Models and returns them to your users based on their profiles

Finally, the information is formatted, then the final reports and gauges pass through the security filter, and are returned to the user who initially requested them.

See “Deployments” on page 25 for more detailed information about how SIP and Data Protector work together.

Deployments

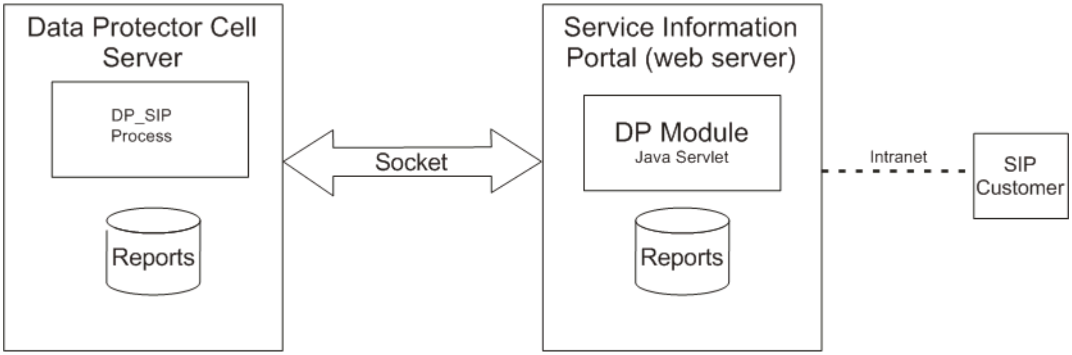
The first step in setting up your Data Protector cell manager with SIP is to determine which deployment model to use. There are three basic models you can use to deploy your services, each of which is described in this chapter.

- Deployment A describes a deployment option in which Data Protector and SIP communicate through a socket that runs through a firewall. The SIP portal host may also be exposed through the firewall and accessed by an external customer.
- Deployment B describes a deployment option in which the Data Protector integration module resides on a web server, which then communicates with SIP via HTTP through the firewall.
- Deployment C describes an option in which Data Protector and SIP communicate through a socket completely contained within the firewall.

Deployment A

This option can be implemented either completely behind a firewall or with access to SIP via port 8080 to a user portal outside the firewall.

Figure 2-1 Deployment A

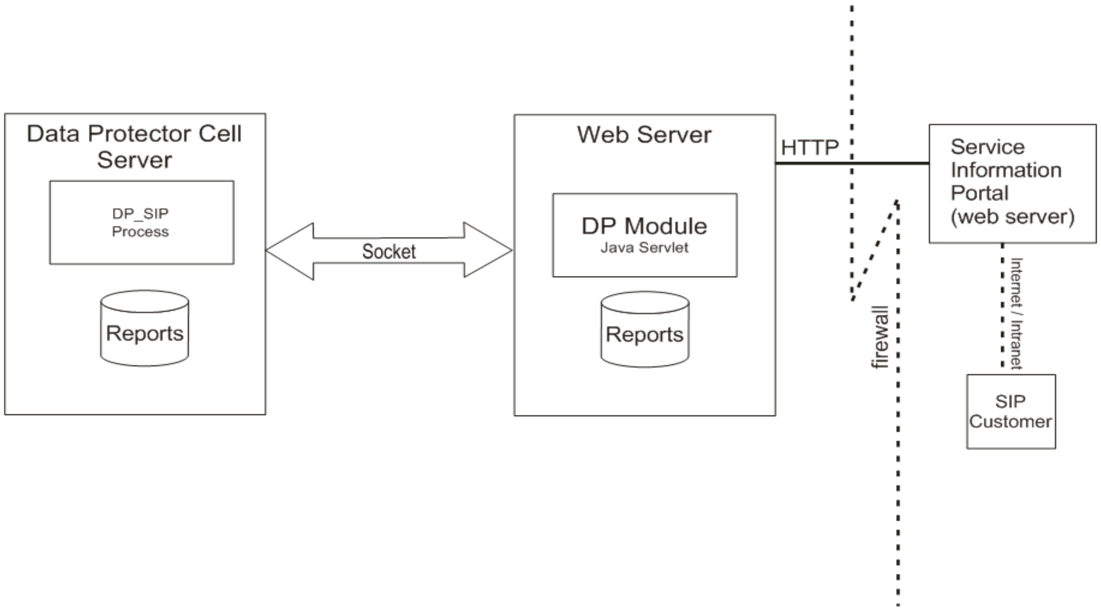


This option is for cases in which all customers are internal. In this model, the Data Protector module runs on the SIP server and communicates with the cell manager and intranet users via socket. The SIP portal host may also be exposed through the firewall via the web server's port (i.e., 8080) and accessed by an external customer.

Deployment B

In this deployment option, the Data Protector module for SIP is run on a web server within the firewall. This module communicates with SIP remotely through the firewall via HTTP, and communicates with the Data Protector cell manager through sockets that are completely contained within the firewall.

Figure 2-2 **Deployment B**

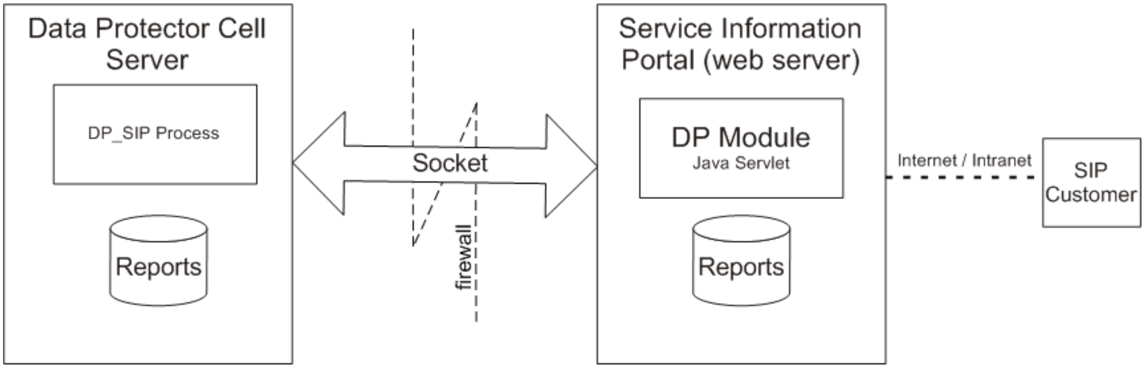


The benefits of this model are that socket connections are secured and deployment functions are compartmentalized. It does, however, require that you run a separate web server for the Data Protector module.

Deployment C

In this deployment, the Data Protector module for SIP is run on the SIP server, outside of the corporate firewall, and it communicates with the Data Protector cell manager via socket on port 5555 through the firewall.

Figure 2-3 Deployment C



This deployment model is simple, effective, and accessible to users, but it can be difficult to secure due to the socket connection running through the firewall.

Setup Process

This section describes how to install and configure the integration modules that let Data Protector 5.0 and Service Information Portal communicate and work together.

The following sections are included in this chapter:

- Installation Procedures
- Customization

Installation Procedures

The Data Protector server and the SIP server communicate by way of a socket connection, which provides a dedicated two-way channel through which SIP can request reports from the Data Protector cell manager, and Data Protector can send them. See “Deployments” on page 25 for more information on the architecture of a Data Protector-SIP integration.

This section describes the procedures for installing the integration modules that let Data Protector and SIP communicate and work together.

For instructions on installing SIP, refer to the Service Information Portal Installation Guide.

For instructions on installing Data Protector, refer to the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Prerequisite Information

Before you begin the installation (on any platform or server), you should be sure that you know the following:

- Base language of the SIP server.
- Fully qualified path name of each cell manager you want to track.
- Fully qualified path name of the SIP server.

On the Data Protector Server

Data Protector can communicate with SIP without any additional modules. There are no integration-specific installation procedures. However, the Data Protector Administrator must configure backup groups which must then be associated with a SIP role and user.

Establishing Data Protector/SIP Communication

After the installation you must establish communication with the Data Protector server from the SIP side. To do this, you must associate the Data Protector organizations (imported via the customer model) with Roles. Refer to the *SIP Deployment and Integration Guide* for more information.

Installing on a SIP Server

To install the Data Protector integration servlets on a SIP server, follow the steps below. Note that the steps are different depending on the operating system of the server.

Installing on a Windows NT SIP Server

1. Insert the Data Protector Windows installation CD-ROM.
2. CD to `DP_Service_Mgmt_Integr`.
3. Run `DP-SIP-WIN.exe`.
4. Follow the steps in the Setup Wizard.
5. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 38
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize `ConfigSpec.xml` as described in “Customization” on page 33.

Installing on an HP-UX SIP Server

1. Insert the Data Protector HP-UX installation CD-ROM.
2. As root, use `swinstall` to install the following depot:

   ```
   DP-SIP-HPUX.depot
   ```

3. Select and install all the components.
4. When the installation is complete, run the following setup script:

   ```
   /opt/OV/SIP/dp_setup.sh
   ```

   Follow the on-screen instructions. At the end of Data Protector Management Server list, enter **q** or **Q** to quit.
5. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 38
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize `ConfigSpec.xml` as described in “Customization” on page 33.
8. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) by doing the following:

   a. Edit the file `APACHE_HOME/apache/conf/jk.conf`

   b. Find the line:

   ```
   JkMount /ovportal/* ajp12
   ```

   c. Add the following lines:

   ```
   JkMount /dpreporter/* ajp12

   JkMount /dpreporter ajp12
   ```

   d. Stop and restart Apache and TOMCAT.

Installing on a Web Server

To install the Data Protector integration servlets on a web server, follow the steps below. The steps are different depending on the operating system of the server.

If you install this integration on a web server, only the Java servlets are installed on that server. The other components must be installed subsequently on the SIP server.

NOTE

If you have chosen this installation option, it is assumed that you have IIS with TOMCAT running on Windows and Apache with TOMCAT running on HP-UX. You are responsible for configuring the application server that hosts these servlets. The servlets must be directly accessible via `http://hostname/servlet` and *not* via a specified port (`http://hostname:8080/servlet`).

This may mean that you must perform special configuration steps for your application server and may need to restart both the web server and the application server. These special configuration steps are not addressed in this installation. Refer to your application server and web server documentation.

Installing on a Windows Web Server

1. Insert the Data Protector Windows installation CD-ROM.
2. CD to `DP_Service_Mgmt_Integr`.
3. Run `DP-SIP-WIN.exe`.
4. Follow the steps in the Setup Wizard, selecting `SIP Servlet Only`.

On the SIP portal machine, insert the Data Protector Windows installation CD.

1. CD to `DP_Service_Mgmt_Integr`.
2. Run `DP-SIP-WIN.exe`.
3. Follow the steps in the Setup Wizard, selecting the `SIP Module Component` option.
4. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 38
5. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
6. Customize `ConfigSpec.xml` as described in “Customization” on page 33.

Installing on an HP-UX Web Server

To install the integration on an HP-UX web server:

1. Insert the Data Protector HP-UX installation CD-ROM.
2. As root, use `swinstall` to install the following depot:

   ```
   DP-SIP-HPUX.depot
   ```

3. Select and install the `Java Servlets` and `Setup Scripts` components.
4. When the installation is complete, run the following setup script:

   ```
   /opt/OV/SIP/dp_setup.sh
   ```

   Follow the on-screen instructions. At the end of Data Protector Management Server list, enter **`q`** or **`Q`** to quit.
5. Customize `ConfigSpec.xml` as described in “Customization” on page 33.
6. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) by doing the following:

   a. Edit the file `APACHE_HOME/apache/conf/jk.conf`

   b. Find the line:

   ```
   JkMount /ovportal/* ajp12
   ```

   c. Add the following lines:

   ```
   JkMount /dpreporter/* ajp12

   JkMount /dpreporter ajp12
   ```

   d. Stop and restart Apache and TOMCAT.

On the SIP portal machine, insert the Data Protector HP-UX CD.

1. As root, use `swinstall` to install the following depot:

   ```
   DP-SIP-HPUX.depot
   ```

2. Select and install the `HP-UX SIP` component.
3. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 38
4. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.

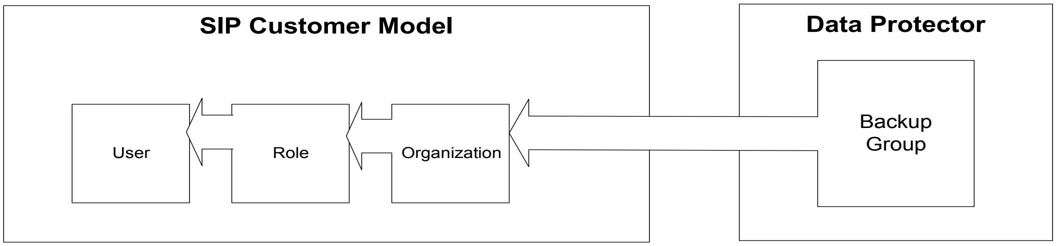
Customization

This section describes how to customize the integration.

Setting Up Backup Groups on Data Protector

In order to receive reports via SIP, you must set up appropriate backup groups on Data Protector. These groups are mapped to Organizations within SIP, which then maps those Organizations to Roles, and Roles to users, as shown in Figure 2-4. For more information about configuring groups, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

Figure 2-4 Backup Group Mappings



IMPORTANT Use the following guidelines when setting up Data Protector backup specification groups:

1. Backup specification group names may NOT include periods (.) or question marks (?).
2. If you define a role containing overlapping backup groups, users with that role will see redundant data in their reports.

Editing ConfigSpec.xml

The `ConfigSpec.xml` file, located in `$SIP_HOME/webapps/dpsip` (for servlets installed on the SIP server) or `$TOMCAT_Home/webapps/dpsip` directory (for servlets installed on a web server), provides you with several options for customizing your integration. The following sections describe these options.

Log Location, Log Level

The log level you set in your configuration determines the level at which events will be logged. In the example below, the log level is 3, so events with a severity of 3, 2, or 1 will be logged. Valid event severities are 1 - 5.

The log location parameter determines the name and location of your log file. You must specify an existing directory. To set the refresh rate, edit the following line:

```
<LogLoc logLevel = "x">qualified_path/log_file_name</LogLoc>
```

In the example below, the log file `msgtxt` is located in the directory `d:/tmp/logging/`.

```
<LogLoc logLevel = "3">d:/tmp/logging/msgtxt</LogLoc>
```

Filter Level

The filter level you set in your SIP configuration determines which types of messages are delivered. You must set each of the message types as true (delivered) or false (not delivered).

In the following example, messages tagged as Major and Critical are delivered, while messages tagged as Minor and Warning are not.

```
<FilterLevel Warning = "false" Minor = "false" Major =
"true" Critical = "true"/>
```

NOTE Message filters in the ConfigSpec.xml file are applied at the system level. That is, any message levels you choose to filter out here will not be logged to your SIP or web server.

Refresh Rate

By default, Data Protector reports refresh when SIP requests a report from the servlet (which it does every time a user logs on). You can, however, set the refresh rate variable so that reports refresh automatically at specified intervals. In this case, the reports are gathered at each refresh interval and are archived on the system. Note that this is a universal parameter, so setting a value for it will cause all reports to refresh and expire at the specified rate.

To set the refresh rate, edit the following line:

```
<RefreshRate update_rate = "time" archive_rate = "time"
file_loc = "path"/>
```

Note that this variable has three parameters:

- **`update_rate`** determines the refresh rate for the report, in minutes. It is recommended that you refresh reports no more than once every ten minutes.
- **`archive_rate`** determines the rate at which archived reports are expired from the system. The value you enter here is the amount of time, in minutes, that a recently accessed report will be maintained on your system. The recommended minimum is five minutes. `Archive_rate` should be greater than `update_rate`.
- **`file_loc`** specifies the location of the files that are gathered and archived to support `RefreshRate`. The location you specify must be a valid, existing directory. Note that this repository may need to be very large if you anticipate large numbers of users to be logging on at the same time.

In the example below, the refresh rate for updates is set to ten minutes and the archive rate for archived reports is set to thirty minutes.

```
<RefreshRate update_rate = "10" archive_rate = "30" file_loc
= "d:/tmp/"/>
```

Gauge Settings

System gauges display your Data Protector system’s health graphically using a gauge that has three ranges: green, yellow, and red, indicating the status of backup health.

You may, however, choose to change the default settings to reflect the sensitivity of your data or the critical nature of the systems you are backing up. To do this, change the ranges according to the health percentage you would like to fit into each range.

To set the gauges, edit the following line:

```
<BackupGauge green_band = "range" yellow_band = "range"
red_band = "range"/>
```

Note that you must not overlap different color bands, so if the green band ranges from 0 to 70, you must also change the lower value for the yellow band range in order not to overlap. For example:

```
<BackupGauge green_band = "0-60" yellow_band = "60-80"
red_band = "80-100"/>
```

NOTE

Gauge settings in `ConfigSpec.xml` are applied at the system level. That is, any gauge settings you enter here will be applied to your entire system. If you want some settings to be specific to a given module view, see “Editing the Backup Health Module” on page 50 for instructions. You may still change the bands for each gauge that you create.

Cell Manager Setting

The CellServer variable provides the integration with information about your Cell Managers, including the language, the port number, and the Java user password. If the Data Protector Administrator has changed either the Data Protector port or added a password for a Java user, you must edit this variable in order for the integration servlets to communicate with Data Protector.

To identify a cell manager, edit the following line:

```
<CellServer locale = "language" port = "xxxx" password =
"pwd">host_name</CellServer>
```

where:

- *locale* is a required parameter that specifies the language of the cell manager.
- *port* identifies the port the integration will use to communicate with the cell manager. Port defaults to 5555 if there isn’t a specified number.
- *password* is an optional parameter necessary only if the Data Protector Administrator wants to create a Java user account. The parameter defaults to no password.
- *host_name* is a required value that identifies the cell manager using a fully qualified host name or IP address.

NOTE If you edit the cell manager setting directly, you must verify that the cell manager is visible to the Data Protector/SIP integration. Ping the fully qualified host name or IP address to make sure that the integration can resolve the host name and find the cell manager.

In the following example, cellserver_1.example.com has English as its language, uses port 5555, and has a password of pwd.

```
<CellServer locale = "english" port = "5555" password =
"pwd">cellserver_1.example.com</CellServer>
```

Creating Customer Models and Portal Views

Once you have set up a communications socket between SIP and Data Protector, you can start setting up your customer models and configuring SIP to display custom portal views for each customer group.

This chapter provides a brief overview of the concept of customer models, and a description of how SIP uses these models to filter the data a user sees.

For more information on customer models, see the *SIP Deployment and Integration Guide*.

This section discusses:

- "Customer Models"

  This section describes the concept of customer models and how they are used within Data Protector and SIP.

- "Management Data Filter"

  This section describes the Management Data Filter and how it is used to serve the appropriate information to your users.

- "Adding and Removing Services in a Portal View"

  This section describes how to configure Data Protector services for display within a SIP portal view.

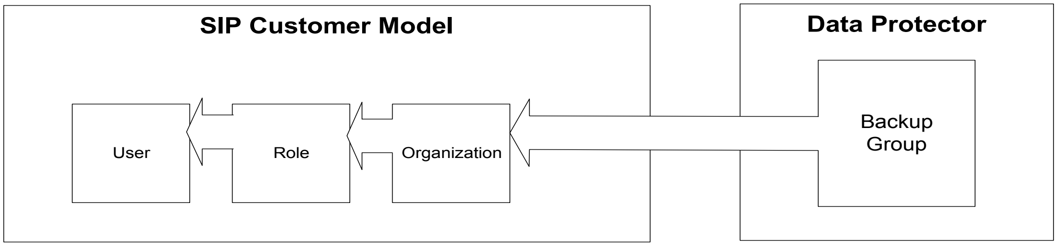
Customer Models

To help you present exactly the right information to all of your users, SIP employs an expandable concept of customer models, which allows you to create and fine-tune different portals for users according to the department they work in, their job functions, security considerations, or anything else you would like to sort by.

Each cell manager is used to create a basic organization where the host is specified; the name of the organization is group@cellserver. This mapping is required to properly generate reports. For detailed instructions for segmenting data and creating customer models, refer to the SIP Deployment and Integration Guide.

A customer model maps users to different hosts, interfaces, and services.

Figure 2-5 **Customer Model**



Importing the Customer Model

Import the customer model from the SIP servlet by following these steps:

1. Log in to SIP as `admin`
2. Navigate to the `Customer Model` tab
3. Scroll to the `Customer Model Sources` section
4. In the `New Customer Model Source URL` field enter the following:

   `http:\\servlet_host.com\dpreporter\customer`

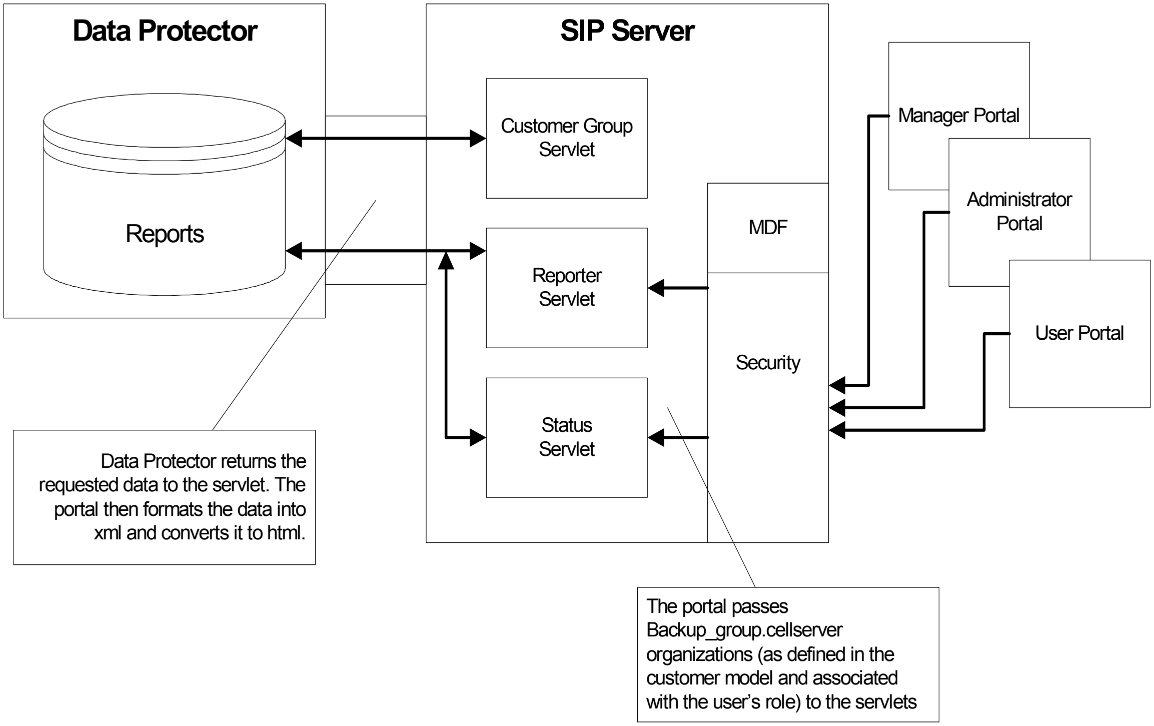
   where

   `servlet_host.com` is the fully qualified host name of the web server on which the servlets are installed.
5. Click `Add`
6. Click `Apply` at the bottom of the page.

Management Data Filter

After SIP receives reports from Data Protector, it passes them through management data filtering.

Figure 2-6 Management Data Filter Overview



Data Protector returns the requested data to the servlet. The portal then formats the data into xml and converts it to html.

The portal passes Backup_group.cellserver organizations (as defined in the customer model and associated with the user's role) to the servlets

Customers are mapped to a user and the user is mapped to a role. The role has organization information that maps a backup group to a cell manager. The role can include multiple organizations.

Filtering uses organizations to return only report data that is applicable to the defined customer.

For a more detailed explanation of SIP's filtering process, see the *SIP Deployment and Integration Guide*.

Adding and Removing Services in a Portal View

To add a Data Protector module to a portal view:

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the `Storage` tab.
3. At the bottom of either wide column, either:
    - Select a Data Protector module from the `Select Module to Add` list box, and click [Add], or
    - Click `Edit` to access the `Modify Column` page. Insert the Data Protector module and place it in the desired location among other modules in the column. Click `OK` to save the changes and return to the main portal page.

A copy of the default version of the Data Protector module you chose is inserted into your PortalView.xml file and is displayed in the portal view. For instructions on how to edit the modules, refer to “Error Messages Module” on page 42, “Protection Status Module” on page 45, or “Data Protector Reports Module” on page 52.

Error Messages Module

This chapter provides an overview of what Data Protector Messages are and how to configure and use them.

This chapter contains the following sections:

- "Understanding Data Protector Error Messages"

  This section describes what Data Protector Messages are and how you can use them in your organization.

- "Editing Data Protector Message Modules"

  This section describes how to set up new Data Protector message modules, as well as how to edit and eliminate existing messages.

Understanding Data Protector Error Messages

The Messages module presents backup and recovery process messages from Data Protector running on one or more Data Protector stations within your management domain.

This module displays changes each time the portal view is displayed or refreshed. The message lists are continually updated in SIP memory.

Data Protector Error Messages

The Data Protector Error Messages module provides access to the following messages from your SIP portal:

- Alarm
- Backup error
- Database corrupted
- Database purge needed
- Database space low
- Device error
- End of session
- Health check failed
- License will expire

- Mail slots full
- Mount request
- Not enough free media
- Unexpected events

For more information on these messages and how to configure them, see the chapter “Monitoring, Reporting, Notifications and the Event Log” in the *HP OpenView Storage Data Protector Administrator’s Guide*.

Adding a Data Protector Error Message Module to your Portal View - GUI

To add a Data Protector message module to a SIP portal, follow the steps below.

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the `Storage` tab.
3. At the bottom of the right column, either:
    - Select `Data Protector 5.0 Error Messages` from the `Select Module to Add` list box, and click `Add`, or
    - Click `Edit` to access the `Modify Column` page. Choose `Data Protector 5.0 Error Messages` from the list of `Available Modules` and place it in the desired location among other modules in the column. Click `OK` to save the changes and return to the main portal page.
4. If the module displays no messages, click on the `Edit` button on the upper right corner of the module and configure the module to point to the correct servlet for a suitable timeframe.

    If the timeframe you select does not provide any messages, a message appears indicating that no messages were available for that timeframe.

Editing Data Protector Message Modules

To modify the Message module in your SIP portal, follow the steps below.

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the `Storage` tab.
3. Scroll to the Error Message module you want to edit.
4. Click on the `Edit` button on the upper right corner of the module.
5. From the `Over the last:` menu, choose a timeframe.
6. In the `Data Protector Servlet host:` field, enter the qualified host name and port of the appropriate servlet.
7. Click `OK` to apply the changes and return to the main portal view.

Editing the PortalView.XML File Directly

Refer to the *SIP Deployment and Integration Guide* for more information.

Protection Status Module

This chapter provides an overview of what Protection Status gauges are and how to configure and use them.

Understanding the Protection Status Module

The Data Protector Protection Status module displays a visual representation of the success rates of your backups.

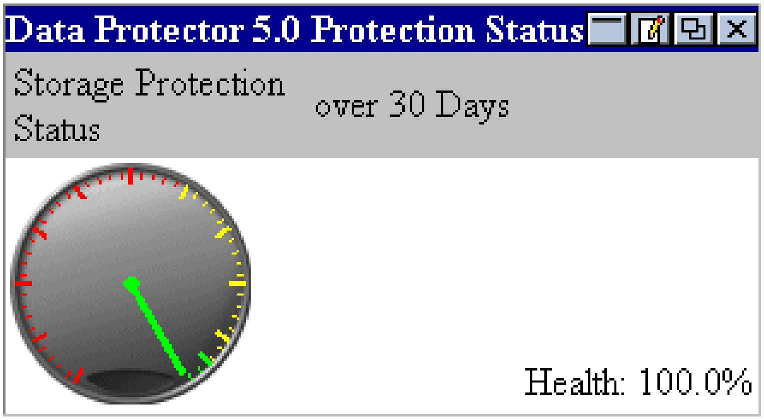
This module has two components: Protection Status gauge and Host Status report.

Gauges appear when the tab first displays in your portal. They indicate the overall health rating for selected or all services that are being monitored by that particular gauge. You can view the details by clicking on a gauge or a health title link to display information about the backups.

Protection Status Gauge

The Protection Status Gauge provides a visual depiction of the status of the backup statistics for all organizations associated with the current role. This is calculated by averaging information from all the organizations.

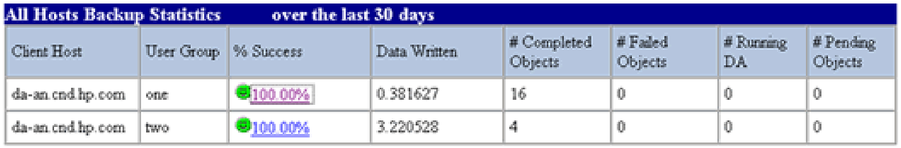
Figure 2-7 **Protection Status Gauge**


Data Protector 5.0 Protection Status
Storage Protection Status
over 30 Days
Health: 100.0%

All Hosts Backup Statistics Report

If you click on a Protection Status Gauge from the main portal window, you can see the `All Hosts Backup Statistics` report, a detailed listing of information about your system's backup health.

Figure 2-8 **All Hosts Report**



All Hosts Backup Statistics over the last 30 days

Client Host	User Group	% Success	Data Written	# Completed Objects	# Failed Objects	# Running DA	# Pending Objects
da-an.cnd.hp.com	one	100.00%	0.381627	16	0	0	0
da-an.cnd.hp.com	two	100.00%	3.220528	4	0	0	0

Table 2-3 describes the fields displayed on this screen.

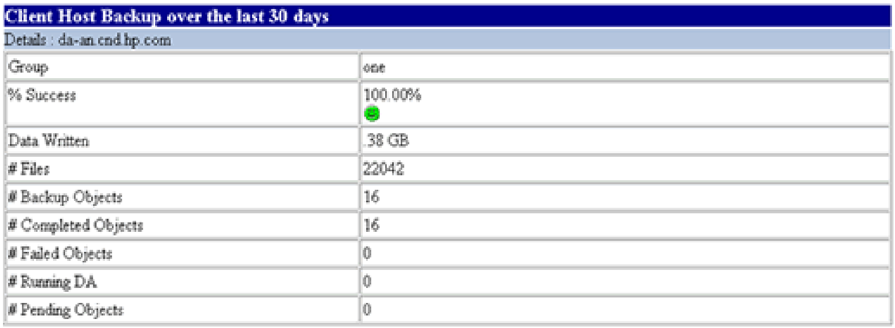
Table 2-3 **Fields in the All Hosts Backup Statistics Report**

Client Host	The name of the cell manager.
User Group	The name of the customer group.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for detailed information about this expanded information.
Data Written	The amount of backup data written (in gigabytes).
# Completed Objects	The number of completed backup jobs.
# Failed Objects	The number of failed backup jobs.
# Running DA	The number of disk agents currently running.
# Pending Objects	The number of backup jobs that are pending.

Client Host Backup Report

When you click on the `% Success` field in the `All Hosts Backup Statistics` page, you can see the `Client Host Backup Report`, an expanded detail view of the backup health for the selected customer group on the selected cell manager.

Figure 2-9 **Client Host Backup Report**



Client Host Backup over the last 30 days

Details : da-an.cnd.hp.com

Group	one
% Success	100.00% ☺
Data Written	.38 GB
# Files	22042
# Backup Objects	16
# Completed Objects	16
# Failed Objects	0
# Running DA	0
# Pending Objects	0

The fields on this screen are described in Table 2-4.

Table 2-4 **Client Host Backup fields**

Details:	The name of the cell manager to which the report applies.
Group	The name of the customer group.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for detailed information about this expanded information.
Data Written	The amount of backup data written.
# Files	The number of files backed up.
# Backup Objects	The number of objects backed up. A **backup object** is any data selected for a backup, such as a disk, a file, a directory, a database, or a part of the database.

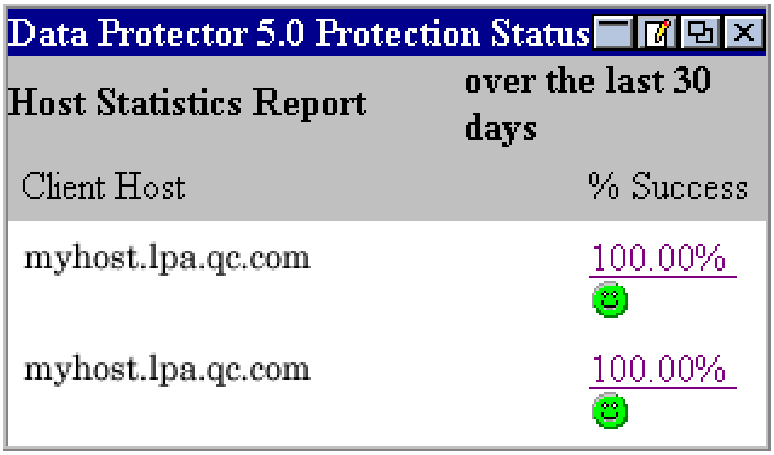
Table 2-4 **Client Host Backup fields (Continued)**

# Completed Jobs	The number of completed backup jobs.
# Failed Objects	The number of failed backup jobs.
# Running DA	The number of disk agents currently running.
# Pending Objects	The number of backup jobs that are pending.

Host Statistics Report

The Host Statistics report provides backup statistics for all hosts associated with the current role.

Figure 2-10 **Host Statistics Report**



Data Protector 5.0 Protection Status

Host Statistics Report over the last 30 days

```
Client Host            % Success
myhost.lpa.qc.com      100.00%
myhost.lpa.qc.com      100.00%
```

Table 2-5 describes the fields displayed on this screen.

Table 2-5 **Host Statistics fields**

Host Statistics Report	The name of the report.

Table 2-5 **Host Statistics fields (Continued)**

Time Frame (i.e., `over the last 30 days` in Figure 2-10)	The time frame for which data is collected/displayed.
Client Host	The qualified host name of the cell manager.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for information about the detailed view.

Detail View

If you click on a percentage in the main portal window, you can see the `All Hosts Backup Statistics` report, a detailed listing of information about your system's backup health. Refer to "All Hosts Backup Statistics Report" on page 46 for more information about this report.

Clicking on a percentage in the `All Hosts Backup Statistics` report displays the `Client Host Backup Report` and a further level of detail. Refer to "Client Host Backup Report" on page 47 for more information about this report.

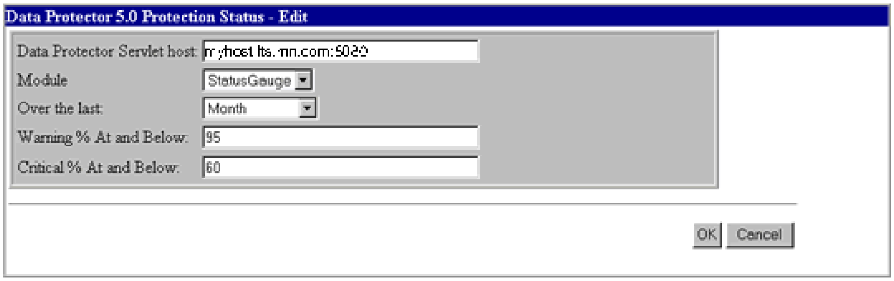
Editing the Backup Health Module

The Backup Health Module provides a gauge or a report that displays information about the overall health of the backup process for all of a customer's groups. You can use the Edit page to customize the Backup Health module.

Using the Backup Health - Edit page

To customize the Backup Health module, click on the `Edit` button in the title bar. The `Data Protector 5.0 Protection Status - Edit` pane is displayed.

Figure 2-11 **Data Protector 5.0 Protection Status - Edit**



Data Protector 5.0 Protection Status - Edit

Data Protector Servlet host: myhost.lts.mn.com:5020
Module: StatusGauge
Over the last: Month
Warning % At and Below: 95
Critical % At and Below: 60

Table 2-6 **Edit Fields**

Data Protector Servlet host:	The fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Module	A drop down menu from which you can choose which version of the module to display, `Status Gauge` or `Host Status`.
Over the last:	The time frame from which to display results.
Warning % At and Below:	The success percentage at (and below) which the protection status is considered to be warning. Anything above this is considered to be normal/successful.
Critical % At and Below:	The success percentage at (and below) which the protection status is considered to be critical.

Backup Health Criteria

The criteria for gauging backup health have been pre-configured in this system, so no additional steps are necessary for you to configure these gauges. You can, however, configure the thresholds for the general backup health status, or severity.

Backup health statuses are generally defined as described in Table 2-7.

Table 2-7 **Backup Health Status**

Normal	A safe health range, in which the severity and incidence of errors is acceptable.
Minor	Although there is probably no imminent danger of data loss from system errors, the administrator should look into the situation.
Critical	Loss of data is likely imminent, and the situation should be resolved immediately.

You can change the thresholds for these statuses globally based on factors within your unique environment. See “Editing ConfigSpec.xml” on page 34 for more information on setting these thresholds.

Directly Editing the PortalView.xml File

You can edit the PortalView.xml file directly. You should be careful, if you choose to edit directly, as incorrect editing may cause anomalous results in the integration. Refer to the *SIP Deployment and Integration Guide* for more information about direct editing.

Data Protector Reports Module

This chapter provides an overview of what Data Protector Reports are and how to configure and use them.

This chapter contains the following sections:

- “Understanding Data Protector Reports”
- “Editing the Data Protector Reports Module”
- “Establishing Global Settings for Reports”

Understanding Data Protector Reports

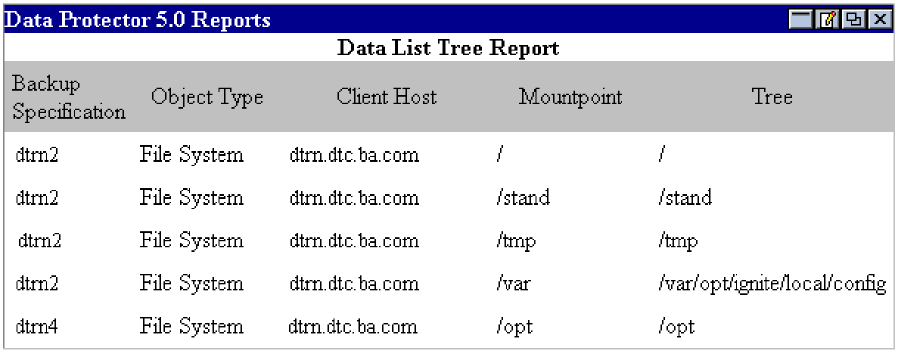
The Reports module provides a variety of information from Data Protector on one or more cell managers in your management domain.

Data Protector Reports

The following Data Protector reports are pre-configured for SIP:

Data List Trees This basic report has information on all directory trees backed up by the cell manager, but is limited to the directories of the groups associated with the SIP customer. Note that this option provides one report per group; customers with multiple groups get multiple reports.

Figure 2-12 **Data List Tree Report**



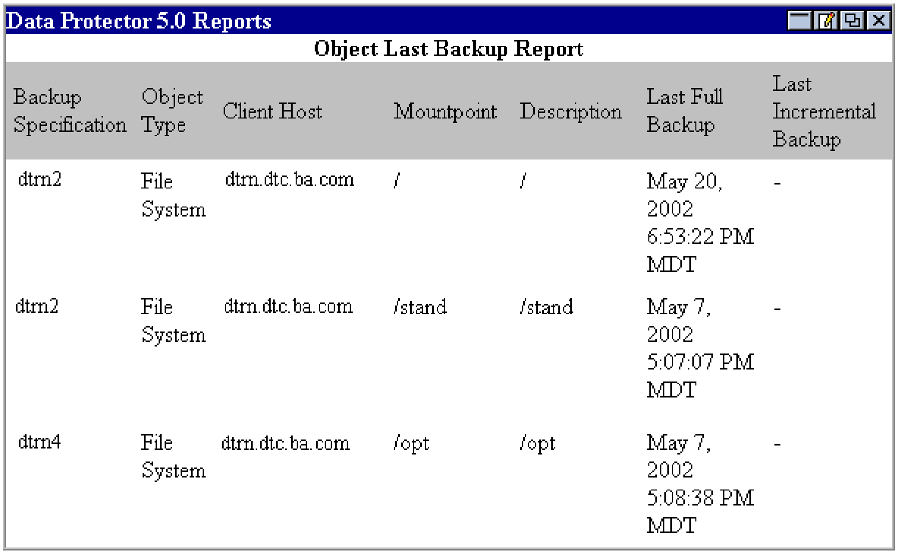
Data Protector 5.0 Reports

Data List Tree Report

Backup Specification	Object Type	Client Host	Mountpoint	Tree
dtrn2	File System	dtrn.dtc.ba.com	/	/
dtrn2	File System	dtrn.dtc.ba.com	/stand	/stand
dtrn2	File System	dtrn.dtc.ba.com	/tmp	/tmp
dtrn2	File System	dtrn.dtc.ba.com	/var	/var/opt/ignite/local/config
dtrn4	File System	dtrn.dtc.ba.com	/opt	/opt

Object Last Back Up This is a basic report showing all objects owned by a group and the data of the last full and partial backup for that group. Note that this option provides one report per group, so customers with multiple groups get multiple reports.

Figure 2-13 Object Last Back Up Report



Object Last Backup Report

Backup Specification	Object Type	Client Host	Mountpoint	Description	Last Full Backup	Last Incremental Backup
dtrn2	File System	dtrn.dtc.ba.com	/	/	May 20, 2002 6:53:22 PM MDT	-
dtrn2	File System	dtrn.dtc.ba.com	/stand	/stand	May 7, 2002 5:07:07 PM MDT	-
dtrn4	File System	dtrn.dtc.ba.com	/opt	/opt	May 7, 2002 5:08:38 PM MDT	-

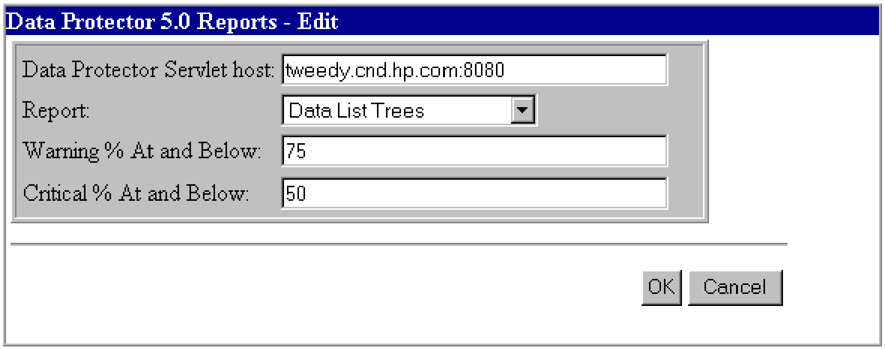
Editing the Data Protector Reports Module

You can use the Edit page to customize the Reports module.

Using the Reports - Edit page

To customize the Reports module, click on the `Edit` button in the title bar. The `Data Protector 5.0 Reports - Edit` pane is displayed.

Figure 2-14 **Data Protector 5.0 Reports - Edit**



Data Protector 5.0 Reports - Edit

Data Protector Servlet host: tweedy.cnd.hp.com:8080
Report: Data List Trees
Warning % At and Below: 75
Critical % At and Below: 50

Table 2-8 **Edit Fields**

Data Protector Servlet host:	The fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Report	A drop down menu from which you can choose which report to display, `Data List Trees` or `Object Last Backup`.
Warning % At and Below:	The success percentage at (and below) which the protection status is considered to be warning. Anything above is considered to be normal/successful.
Critical % At and Below:	The success percentage at (and below) which the protection status is considered to be critical.

Directly Editing the PortalView.xml File

It is possible to edit the PortalView.xml file directly. You should be careful, if you choose to edit directly, as incorrect editing may cause anomalous results in the integration. Refer to the *SIP Deployment and Integration Guide* for more information about direct editing.

Establishing Global Settings for Reports

For more information about establishing global settings for reports, refer to “Editing ConfigSpec.xml” on page 34.

Troubleshooting

Error Messages

This section lists some error messages you may see while using this integration and discusses how to respond to them.

Data Unavailable

If, while viewing reports, you get a *Data Unavailable* error message after adding a module, you are missing either a valid servlet host or data within the specified timeframe.

Check the following in the `ConfigSpec.xml` file, located in `$SIP_HOME/webapps/dpsip` (for servlets installed on the SIP server) or `$TOMCAT_Home/webapps/dpsip` directory (for servlets installed on a web server):

- The hostname (including port number) is valid.
- The set timeframe is reasonable in size to have data.

Parse Rest of Config

If, while using this integration, you get the Java exception message *Exception: parse Rest of Config*, the log directory may not have been installed correctly. Verify that the log directory is present (at the location specified in the `ConfigSpec.xml` file) and that read/write access for the directory is set to `all`.

3 Data Protector-OVO-SIP Integration

Introduction

The integration of Data Protector with the OpenView Service Information Portal (SIP) offers pertinent information to the managers of the backup service of a specific group. The portal allows for tailoring of the page for each user.

This chapter describes how SIP and OpenView Operations integrate with Data Protector to provide additional network visibility to Data Protector and to allow integration of Data Protector-specific information with other SIP services.

Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Operations
- OpenView Service Information Portal
- Supported Oracle Database (third party software)
- Data Protector Integration for OVO for UNIX

Product Capabilities and Integration Benefits

This integration provides the following capabilities:

- Convenient data protection service monitoring through web access from any machine.
- Various forms of data presentation: service health gauges, service graphs, service cards, and a service browser.
- The specification of resource in terms of machine and backup specification group names.
- Segmentation of accessible data by the different backup administrators.
- Support for various authentication mechanisms including a generic authentication mechanism.

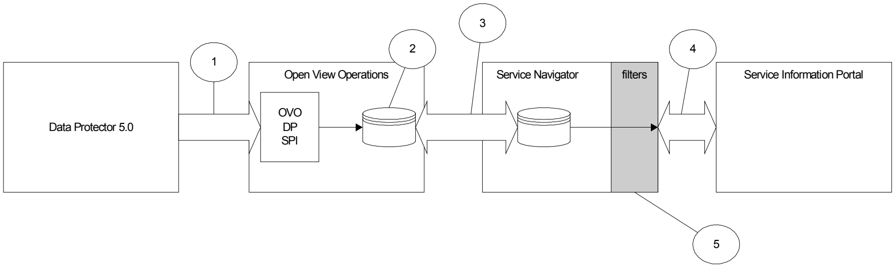
- Information aggregation from other services (not related to Data Protector) to the portal, using SIP's configuration mechanisms. A single presentation format for all modules.
- Easy configuration: GUI configuration editor and XML document editing only.

Component List

- Data Protector - A backup solution that provides reliable data protection and maximum accessibility for your business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.
- OpenView Operations (OVO) - A central data collection and management point capable of reading messages from a variety of modules on various machines, acting on them when such action is defined, and transmitting them (the messages) further if asked. OVO has the potential of serving as a central management point for various remote systems. OVO offers both command line and graphical user interfaces for local and remote administration.
- Data Protector Integration for OVO for UNIX - A component that implements the data passing interface between Data Protector and OVO. This component resides on both ends and is integrated into both products.
- OpenView Service Navigator - A system that maps messages to services to ease the control of complicated systems.
- OpenView Service Information Portal (OV SIP) - A tool that aggregates information collected from various services. The information is presented and formatted through various portal components and is made available through a web page. Portal components and modules include Service Browser, Service Graph, and Service Cards.

Data Mappings

The illustration below shows the data mappings for this integration.



1. OVO receives information from Data Protector via the Data Protector Integration for OVO for UNIX.
2. OVO stores the information locally in its database.
3. Service Navigator receives the Data Protector records from OVO.
4. SIP queries Service Navigator about the OVO information.
5. Service Navigator filters the records received from OVO by service name, according to the SIP query.

If the customer also integrates OV Reporter in this configuration, SIP may provide URLs to the reports as generated by Reporter. It is up to the administrator to configure the links. The Reporter-Data Protector integration generates these reports as statically linked HTML documents.

Dependencies

- If Reporter is included in the integration, the configuration of the URL links for the reports depend on the names that Reporter gives to those reports.
- The Backup Service pie chart module will only be available if the OpenView Reporter integration is installed.
- If you choose to use the Backup Service pie chart module, the Data Protector backup specification group names must be names that Windows NT accepts for file names. A folder named “machinename.DPServiceName” is created for them on the Reporter machine, which is a Windows machine. The names must contain only ASCII characters.
- OVO requires a supported Oracle database to be installed. The exact version depends on the OVO version. For more information, refer to the OVO Installation Guide.
- Sun's Java Developer's Kit 1.3 is required for SIP, OVO, and Service Navigator.
- Some OpenView components require that Netscape Navigator 4.7 be installed. This step is unnecessary and may be skipped as long as alternative means of browsing HTML pages is available (e.g., a web browser on a separate machine, or an alternative compatible web browser).
- Successful configuration must also comply with the software requirements as described in the table below.
- The environment must be properly set and configured prior to the installation of the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about the specific requirements, please refer to the installation guides for those components.
- This integration uses Data Protector backup specification groups. Refer to the *HP OpenView Storage Data Protector Administrator’s Guide* and the Data Protector online help for more information about backup specification groups and how to configure them.

Table 3-1 Software Requirements

Component	Version	Operating System
OVO	6.0, 7.0, 7.10	HP-UX 11.0
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVO Agent	6.05, 7.0, 7.10	HP-UX 11.0, 11.11 Windows NT 4.0, Windows 2000
OVO Database	Oracle 8i	HP-UX 11.0, 11.11
SIP	3.0	HP-UX 11.0 Solaris 8 Windows 2000
Service Navigator	6.0	HP-UX 11.0

Setup Process

The setup process for this integration consists of two main procedures:

- Installation of the components
- Configuration of those components

Installation

Service Navigator, OVO, SIP, and Data Protector can be installed on a mix of HP-UX and Windows machines. All the necessary and required components should be installed and working.

1. Data Protector 5.0 should be installed on the data protection cell manager. If the cell manager is an HP-UX machine, the DCE-KT-Tools component must also be installed.

   See the Data Protector 5.0 Installation Guide for detailed instructions.

2. Install the following Oracle products, version 8.1.6.0.0, on the management station:

   - Oracle8i Server (Optional components not required)
   - Net8 Products (All components are required)
   - Oracle Utilities (All components are required)
   - Oracle Installation Products (All components are required)

3. Use `swinstall` to install the ITOEngDoc and ITOEngOraAll OVO components (assuming the chosen language is English) on the management station. See the *OpenView Operations Installation Guide* for detailed instructions.

4. Install Service Navigator on the management station. See the *HP OpenView Operations and Service Navigator Integration with SIP* document for detailed instructions.

5. Install Data Protector Integration for OVO for UNIX on the management station. This component is located on the Data Protector CD. (This step includes various related patches for Service

Navigator and OVO.) See the *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations* for detailed instructions.

6. Install the OVO agent on the cell manager. See the OpenView Operations Installation Guide for detailed instructions.
7. Install SIP on the portal server. See the Service Information Portal Installation Guide for detailed instructions.
8. Install the integration package (listed below) on the SIP server.

   - Windows

     a. Insert the Windows installation CD.

     b. Run the following executable:

     `\DP_SERVICE_MANAGEMENT_INTEGR\DP-OVO-SIP-WIN.exe`

     c. Follow the on-screen instructions

   - HP-UX

     a. Insert the HP-UX installation CD.

     b. Use `swinstall` to install the following depot:

     `/OV_INTEGRATIONS/DP-OVO-SIP-HPUX.depot`

     c. Follow the on-screen instructions.

Configuration

SIP maintains its configuration documents in XML format. The XML must be modified to present customized portal views, implement user data segmentation and separation, and map resources to the users.

Sample Configuration Files

The integration package will place sample configuration files in the following directory:

Windows 2000	`<SIP>\ovo\SIP\integration\DP`
HP-UX	`<SIP>/ovo/SIP/integration/DP`

See the `readme` file for details about the sample files.

Editing Configurations

There are three basic ways to create and update the configuration. You can use any of the following methods:

- The SIP Administrator view can be used to restart the engine, to accept new customer models, and to help design the portal page when viewing a role with ViewAdmin.
- The configuration editor is a Java tool supplied with SIP that guides the user through the process of configuration, including user/role mapping and management station declarations.
- The XML files can be edited by hand. The customer model must be defined via manual XML editing. You can also perform any other configuration tasks by editing the XML files directly.

Configuring the Management Stations

1. On the portal machine, use the SIP configuration editor to select and right click the `ManagementStation` folder. From the shortcut menu, click `New...`
2. Type the fully qualified hostname in the `New Management Station` Window.
3. Select the OVO tab and check the "`OVO Is Installed On This System`" and "`Service Navigator Is Installed On This System`" boxes.
4. Accept the default values, or change the values and continue.

The configuration file is located as follows:

Windows 2000	`SIP\conf\...`
HP-UX	`/SIP/conf/share/stations/mgmtStations.xml`

Following is an example of a management station element in the `mgmtStations.xml` file. Notice that it contains the definitions of all the OVO stations SIP communicates with.

```
<ManagementStation hostname="ovo.example.com">

       <OVOStation

           serviceNavPort="7278"

           serviceDataSource="yes"

           dbPort="1521"

           dbUser="opc_op"

           dbPassword="OpC_op"

           maxConnections="10"

           minConnections="5"

           maxCachedStmts="10"/>

    </ManagementStation>
```

For more information about management stations, refer to `mgmtStations.dtd`, `ovoConfig.dtd`, and the online help in the SIP configuration editor.

Updating the Customer Model

The customer model is where Organizations are defined in terms of accessible resources. The file that describes the model is:

Windows 2000	`<SIP>\conf\share\CustomerModel.xml`
HP-UX	`<SIP>/conf/share/CustomerModel.xml`

Make a copy of the existing model and amend CustomerModel.xml to include the organization you want your users to access. Add `<Organization>` tags as an element in `<SimpleCustomerModel>`. The specification of backup services requires neither `<NodeList>` nor `<InterfaceList>`, so those tags will be empty if present at all. If you include resources other than Data Protector backup services as described in this integration, you may need to use the `<NodeList>` and `<InterfaceList>` tags.

For more information, consult the chapter “Segmenting Data by Customer Organization” in the SIP Deployment and Integration Guide.

The example below shows a description of a backup service. The <ServiceLevel> tag is used to describe the service level. The <Service> tag is where the backup service is referenced. Its name must be specified as software name (e.g., “Data Protector”), fully qualified machine name, backup specification group name (if defined in Data Protector), and service name with full hierarchy (full hierarchy means the path in the service graph starting at the root and ending in the required node). The service navigator requires a format of a service description to be topnode separated by a dot followed by its child node, and so on till the last node to be described All items should be separated by a dot.

```
<Organization name="firstOrg" type="customer">       <ServiceLevel>Gold
Service</ServiceLevel>

    <NodeList/>

    <InterfaceList/>

    <ServiceList>

       <Service name="Data Protector.example.com.group1.BackupSessions"
       type="server"/>

      <Service name="Data Protector. ..." type="server"/>

</ServiceList>

</Organization>
```

Creating a SIP User/Role Package

The SIP security model is based on segmentation. Services are mapped to roles (not necessarily uniquely) and users are given access to those roles (each user may have more than one role). The information about the user/role model is then processed and saved in a format SIP can use.

To create a new user/role package:

1. Highlight User Role Packages
2. Select New in the drop down menu in the Configuration Editor

The list of active user/role packages is located in:

Windows 2000	`<SIP>\conf\share\roles\index.xml`
HP-UX	`<SIP>/conf/share/roles/index.xml`

NOTE Remove any packages you do not use. Each package contains doors through which one may enter your system. Leaving unused packages on your system can create unnecessary risk by introducing security holes.

To define a SIP user/role package, follow the steps below. In this example, the SIP configuration editor is used.

For more information about user role/model and definition, use the online help in the SIP configuration editor.

Define the management data

1. Create the `managementData` items in the package you defined.
2. Select the “Show Data for the Following Organizations:” button, select the name for the management data, and click Add.
3. The list of available organizations is displayed in a new window. Select all organizations (previously defined in the customer model) and click OK. (You may later remove organizations from the management data, e.g. for security purposes.)
4. Repeat the previous steps for each group of resources.

Define user roles

1. Select Roles from the package you created. Right click and select New from the shortcut menu.
2. In the General tab, choose a Role Name (the name used in the configuration to reference the role) and a Display Name (the name appearing on SIP for that role).
3. Select a setting from the drop down menu for the Edit Permissions field. User Preferences is the recommended setting, as it allows users to select their own skins--or predefined display settings--for their pages.
4. Select Portal View File. This file may be any portal view you have already defined or one of the demo portal views, such as samples/liveDemo.xml (Use the browse button to help you navigate through these files.)

5. Type a new name in Modified View File field. The name should have the extension .xml. When you do this, the file used in the Portal View File is copied and the role has its own portal view. If you do not want to do this (for example if you would like any change to a portal view of one role to be reflected by all roles who share that view), do not specify a Modified View File.
6. Click the Management Data tab and select “Use specific management data.”
7. Choose the management data you would like to associate with the role.
8. Click OK.

You now have a new role.

Define a User

1. Select Users in the package, right click and select “New...” from the shortcut menu to add the user.Choose the user login name (the name used to refer to that user in the configuration) and display name.
2. Click the Roles tab and choose the user's roles and initial role. You may override the edit preferences of a role for a user by specifying the role in the Other Roles block, adding the role there and editing its “Override Permissions” field.
3. To allow easy editing of the portal views for all roles, you may want to either give an existing administrator access to those roles or create a new portal view administrator. To create a new portal view administrator, create a new user with access to all the Roles you want the user to be able to configure portals for. Make sure the Override Permission field for these roles is set to ViewAdmin for this user. (See the Roles tab in the user definition window).
4. Click the save button in the SIP portal configuration editor.

The configuration is saved.

Design portal views

1. Now that your users are set, you must restart the SIP engine before the changes take effect.
2. To design portal views, log in as a portal views administrator (a user with ViewAdmin permission to the configured role) and design the portal views for the various roles. You may add, remove, and edit any module that has access to the information spanned by the role's management data. When finished, log out, then log back on as a user with access to the role to view your new view as users will see it.
3. Please refer to the “Designing a Custom Look and Feel to Your Portals” section of the “Customizing Portal View” chapter in the SIP Deployment and Integration Guide for more details on customizing your portal view.

Add Password Authentication (optional)

The system configured so far offers little security. Access to a user's view is given upon request with only a user name.

To add a level of security to the system, you can configure password authentication to the portal.

This step is optional as the customer may choose to have a different security model, or no security at all.

Enable password authentication

Follow the steps below to add a user/password authentication scheme to the portal. For all other authentication options, or for further information, refer to the “Configuring Authentication” chapter in the SIP Deployment and Integration Guide.

Enable user password authentication in SIP. Authentication is a portal-wide setting configured in the OVPortalConfig.xml file, located in the following directory:

Windows 2000	`<SIP>\conf\framework\`
HP-UX	`<SIP> /opt/OV/SIP/conf/framework/`

Find the Authentication element and change it as shown below:

```
<Authentication LoginPage="/ovportal/jsp/security/login_html.jsp"
    AuthenticationProviderClass=
       "com.hp.ov.portal.security.FileAuthenticationProvider"
    ShowLogoutButton="yes"
    LogoutPage="/ovportal/jsp/security/logout_html.jsp"/>
```

Once you enable password authentication you can begin to add authorized users to SIP.

Add authorized users to SIP

SIP provides a program, `htpasswd`, for configuring user logins. It also comes with a password file containing one user:

username: `ovuser`

password: `ovuser`

1. The password file is manipulated the same way a UNIX password file is. You must add a user and its password to the password file to allow users access their SIP accounts. To add a user:

   Windows 2000:

   ```
   %SIP_HOME%\bin\htpasswd
   %SIP_HOME%\etc\passwd <username>
   ```

   UNIX: (as root)

   ```
   /opt/OV/SIP/bin/htpasswd
   /opt/OV/SIP/etc/passwd <username>
   ```

   where *`<username>`* is the user you want to add to the portal.

2. Enter a password for the user when prompted.

   The location of the default password file is:

   Windows 2000: `%SIP_HOME%\etc\passwd`

   UNIX: <SIP>/etc/passwd

   Once you have created new user accounts, you may remove `ovuser` from the password file by deleting its entry and saving the file.

Finalize the Configuration

1. If an authentication module was configured, restart the engine.
2. Log on to the system from the web and access the admin view for the configured role.
3. If the reporting system (OVR) is integrated into the system, you should now associate users with reports.

NOTE It is important to note that only the Backup Health Report is currently customized per group. None of the other included OVR reports have been customized and so will contain information regarding all groups. Users who have access to these reports can easily gain information regarding other services. It is recommended, in the interest of segmentation, that you do not give regular users not designated as administrators links to the non-customizable reports. You should give these users a link to their respective group report only.

Backup Administrators with jurisdiction over all backups may be given a link to all reports. These references are represented as URL links in the portal.

4. To add a reference, log in as a user with ViewAdmin privilege for the role you want to add a report for.
5. In the new window, click the Add Bookmark button.
6. Complete the following fields:

   Bookmark Name The name the portal will display for the link. In most cases, you can use Backup Health Report (unless it is a different report you give a link to).

   HREF The URL itself.

   Window Name (optional) A title for the new window the user will open by clicking that link.

7. Click OK.
8. Return to the bookmarks window and click OK again.

   The bookmark will now display in the portal view for this role.

NOTE

OVR reports are not secured, and unless special actions are taken, can be accessed by any user who has the link names. If there is a concern about the security and sensitivity of the displayed information, OVR should not be integrated with SIP

SIP is delivered with a generic demo portal that includes graphics files of sample logos. You may want to remove these samples.

To remove these files, follow the procedure below.

1. On the machine with the web server installed, go to the directory where the default header is stored.

Windows 2000	`<SIP>\webapps\ovportal\jsp\core`
UNIX	`<SIP>/webapps/ovportal/jsp/core`

2. Save a copy of `header.jsp` and edit `header.jsp` to eliminate the link to `generic_net.gif` or `hplogo.gif` or, alternatively, replace them with links to your favorite logos.

   The portal view has many details that can be customized. For more information on this, refer to the *SIP Deployment and Integration Guide*.

If the OVR Data Protector integration has also been installed, then there is a Backup Service Health pie chart module available. The following steps will activate the module.

1. Verify that the OVR Data Protector integration is installed correctly by locating <…>HP OpenView\bin\split.exe on the OVR machine.
2. Open the file <SIP>/registration/defaults/OVDefaultOVRRep.xml. It should contain the following content and can be found in the release package:

```
<Generic>

  <Submodule>

    <Url href="http://<reporterAddress>/hpov_reports/DP/
    SessionHealthStatus_m/SIP_USERS/$OVROLE[OVName].jpg"

    displayMethod="inline" inlineHeight="400"
    anchorText="Backup Service Health Status"/>

...</Submodule>

</Generic>
```

NOTE The “_m” that precedes `SessionHealthStatus` in the link above specifies the 30 days period report. If you want the daily or weekly period report, you can redefine the link to `SessionHealthStatus_d` or `SessionHealthStatus_w` *provided* that the corresponding steps on the OVR side are taken, too. By default, OVR is only configured to split the monthly report.

Substitute <reporterAddress> with the machine name and the port number, if required, of your reporting station.

3. Restart the SIP engine. Verify that the configuration of the Backup Service Health pie chart module is correct by viewing the log file as a SIP administrator. The log should show details if the configuration has problems.

4. You can now add the Backup Service Health pie chart module by modifying a Data Protector user's portal view. If the pie chart does not appear and an error message is displayed, please refer to the Troubleshooting section.

Troubleshooting

Table 3-2 **Troubleshooting**

Problem	Resolution
The module in the portal displays an error description.	Click the refresh button.
The module displays a message: Currently not configured - the management station is not connected to SIP or attempt to use information from service outside the resources defined for the given role.	Reconfigure and reprocess configuration. (Run create_role_db if the customer model changed. Otherwise, restart the engine.)

4 Data Protector-OVR Integration

Introduction

The integration of OpenView Reporter, via OpenView Operations, with Data Protector provides additional capabilities for monitoring and reporting on the backup and recovery processes.

Data Protector deals effectively with the backup, recovery, and protection of valuable data, but problems occur that are beyond the control of an administrator. Media goes bad, storage runs low, and machines die, get disconnected, or lose power. The administrator or IT staff must be able to deal with these situations in a timely manner and requires that pertinent information be available easily, quickly, and immediately in the most accessible manner.

This chapter describes how Reporter integrates with Data Protector to provide detailed and in depth information concerning the health and status of Data Protector's data protection services.

Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Operations
- OpenView Reporter
- Supported Oracle 8i, 9i Database (third party software)
- Data Protector Integration for OVO/UNIX

Product Capabilities and Integration Benefits

This integration maximizes the potential of OVO, OVR, and Data Protector, providing all of the following benefits:

- Enterprise-level data is presented in easy to read charts, tables, and graphs, making it simpler to review and analyze.
- Information is available through any compatible web browser on your network, so administrators aren't tied to a single location for accessing the Data Protector or Operations machines.

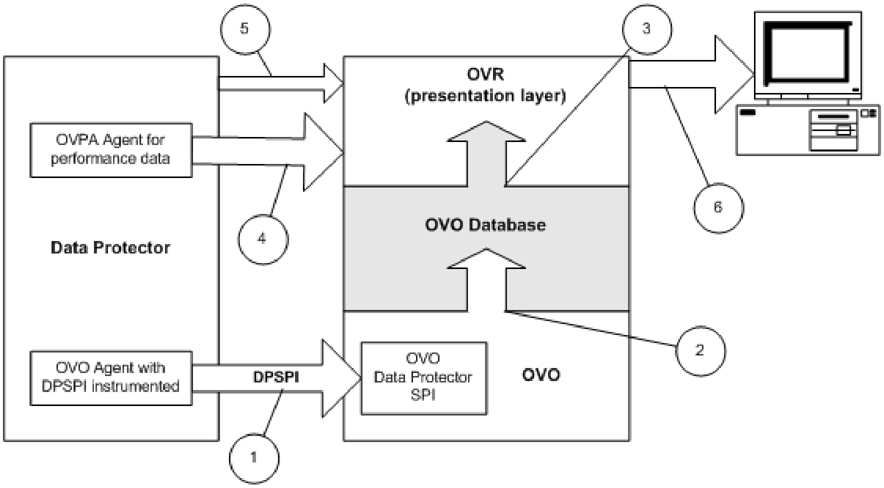
- Additional reports can be generated, customized, or modified using Crystal Reports (a tool that can be used to create interactive content from data sources, to publish reports to the Web in a variety of formats, and to integrate reports with applications). This product is not included with OVO, OVR, or Data Protector. Refer to the Crystal Reports documentation for template and configuration information.
- The administrator has convenient access to critical information concerning Data Protector services.
- Information is collected in convenient report formats.
- The reports provide a high-level view of the data protection services for the whole enterprise.

Component List

Table 4-1

Data Protector	A data protection service that handles data backup and recovery across various systems and media types.
OpenView Operations	A central management point for various remote OpenView applications. Collects and analyzes data, automates critical response, as well as message forwarding to other services.
OpenView Reporter	A reporting service that further analyzes, inspects, and collects data gathered by OVO and formats them into a human readable and usable web-based presentation.
Data Protector Integration for OVO/UNIX	A software package that helps 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 (OVP) Agent.

How Data Protector Integrates with OVR



1. OVO receives information from Data Protector via the DP-OVO integration.
2. The information is stored in the OVO database.
3. OVR extracts necessary Data Protector-specific data from the OVO database.
4. OVR also collects performance related data from the Data Protector server using the OV performance agent.
5. Cell Request Server serves skipped files data to OVR via port 5555.
6. OVR generates Data Protector reports using data collected in steps 3, 4, and 5.

Dependencies

- OVO requires Oracle 8i or 9i. Refer to the OVO Installation Guide
- Java™ Developers Kit 1.3 is required for OVO
- Netscape Navigator 4.7 is listed as a required component at some points, but this is unnecessary if a web browser on another machine is available
- The proper environment is required prior to installation of the components of the integration. This may include various patches, software, and settings to be made. Please refer to the corresponding installation guides for more information.

Table 4-2 **Software Requirements**

Application	Version	Platform
OVO	6.0, 7.0, 7.1	HP-UX 11.0, and 11.11 Solaris 8, 9.
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVO Agent	6.05, 7.0, 7.10	HP-UX 10.20, 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVO DB	Oracle 8i/9i	HP-UX 10.20, 11.0, 11.11
OVR	3.0	Windows 2000 and Windows NT

Data Protector/OVR Integration

The Data Protector/OVR integration consists of three major elements:

- DP/OVO/OVR Integartion
- DP/VPPA/OVR Integartion
- DP/OVR Integartion

These elements are described in greater detail in the sections that follow:

DP/OVO/OVR Integartion

The Data Protector-OVO Integration populates Data Protector specific data into OVO database. To produce Data Protector specific reports, OVR reads the OVO database (an Oracle 8i/9i client should be installed on OVR server) to retrieve data.

DP/OVPA/OVR Integration

OVR gathers performance and transaction data from the Data Protector Management server based on a specified metric list and produces a report.

DP/OVR Integration

The final main element of the Data Protector-OVR integration is the Cell Request Server (CRS) process in Data Protector cell manager. The CRS serves data to OVR via the socket 5555. If any other port than 5555 is used, this part of integration will not work. The password for the user `Java` must be the default password.

Setup Process

Setup and install of the OVR Report package is very simple, assuming you have a working Data Protector-OVO integration and a working OVO-OVR installation. Please refer to the *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations* or the OVR installation documents for more information.

To install the Data Protector-OVO-OVR integration:

1. On the OVR system, insert the Data Protector Windows CD
2. Run: `\DP_Service_Management_Integr\DP-OV-Reporter-WIN.exe`
3. Follow the on screen instructions

Configuration

If you have followed the suggested order of installation and the Data Protector-OVO integration has already been installed and configured, no configuration of the Data Protector-OVR integration should be necessary, as the integration installs a set of complete report templates that should work out of the box. The report package include a set of reports tailored for a working Data Protector-OVO integration, so if the reports don't work, please check the Data Protector-OVO integration.

To manually configure a transaction report, you must integrate Data Protector with ARM® by linking the libarm.sl files in Data Protector and OVPA. For detailed instructions, see the *HP OpenView Storage Data Protector Administrator's Guide*.

Error Messages

This section provides an overview of Data Protector Skipped Files report error codes & error messages.

3 => "Can not create/close control file: <CheckFile>"

4 => "Can not create/close Nodes.Sql"

5 => "SQL Query failed!"

6 => "No DP Cell Manager is added to OVO Node Bank"

7 => "Can not create/close Cells.txt file"

8 => "Exception in main thread!!"

100 => "Can not able to create sfReport.htm"

101 => "Can not open/close outFile"

102 => "Base directory doesn't exist"

103 => "Already one instance of skipped file report generator is running\nso run this latter"

Troubleshooting

Table 4-3 Troubleshooting Tips

Problem	Resolution
While attempting to install the report package, setup was unable to detect HP OpenView Reporter on the machine	Make sure the machine you're installing on has HP OpenView Reporter A.03.01.00 or above. If it does not, install it.
HP OpenView Reporter was not installed properly on this machine	Reinstall or repair HP OpenView Reporter A.03.01.00
Installed HP OpenView Reporter version is not A.03.01.00	Upgrade or install HP OpenView Reporter A.03.01.00 or above
Not enough free disk space on Drive *selected drive*. Available disk space on drive *selected drive* is *space* MB. Required disk space is 5MB	Free up 5 or more MB of disk space on the selected drive and continue installing the OpenView Reporter Data Protector report package.

Creating Custom Reports

Introduction

The Data Protector integration with OpenView Reporter comes with a carefully chosen set of reports on the general health of the backup system and overall backup statistics. Reporter also offers a high degree of flexibility in changing the default report settings. If, however, you want to report on data from new or modified metric lists, new custom report templates are necessary.

You can create or modify report templates with Seagate Crystal Reports to customize the default report templates or create your own templates.

NOTE

For detailed instructions on how to create custom reports and software requirements, refer to:

- OpenView Reporter online Help “Creating Your Own Reports” topics
- *HP OpenView Reporter Concepts Guide*
- *Customizing HP OpenView Reporter With Seagate Crystal Reports* (found on the Reporter product CD).

Crystal Reports Professional 8.5 was used to develop the default templates.

Creating Data Protector Custom Reports

When you create a new Data Protector report template in Crystal Reports, you must select a data source that defines where the data for each metric list is stored. You also need to understand the data format in order to retrieve appropriate performance data and use it to the best effect.

This section provides an overview of the main database tables and data format used for Data Protector-specific messages.

Data Source

The Data Protector Integration with OpenView Operations (DP-OVO) generates a wide variety of messages that enables you to monitor and manage the health and performance of your Data Protector environment with OpenView Operations (OVO).

Messages are stored in two sets of OVO message tables: active messages and history messages. The active and history messages, although they have the same attributes, are kept separate to improve performance when loading and inserting active messages. Acknowledged and unacknowledged messages are first marked and then moved in groups of 50 by an asynchronous process to reduce the impact on GUI. The message text and original message text are also stored in separate text tables for performance reasons.

OVO message tables include:

- OPC_ACT_MESSAGES

  This table contains the main entry for messages that are currently in the Message Browser window. This table can also contain a maximum of 50 acknowledged messages. When more than 50 messages have the `ackn_flag` set to `Yes`, they are moved to the history table.

- `OPC_ANNO_TEXT`

  This table contains the annotation text for messages in `OPC_ACT_MESSAGES`.

- `OPC_ANNOTATION`

  This table contains the main entry of message annotations for messages in `OPC_ACT_MESSAGES`.

- `OPC_ESCAL_ASSIGN_M`

  This table contains the message numbers of the owned messages and messages that were escalated to or from another management server.

- `OPC_FORWARD_MSGS`

  This table contains list of messages that have been forwarded to other management servers.

- `OPC_HIST_ANNO_TEXT`

This table contains the annotation text for history messages in OPC_HIST_MESSAGES.

- OPC_HIST_ANNOTATION

  This table contains the annotations for a history message in OPC_HIST_MESSAGES.

- OPC_HIST_MESSAGES

  This table contains the main entry for history messages (messages that were acknowledged or are log-only). Some acknowledged messages may still be in OPC_ACT_MESSAGES.

- OPC_HIST_MSG_TEXT

  This table contains the message text, divided into 254-byte parts, for messages in OPC_HIST_MESSAGES table.

- OPC_HIST_ORIG_TEXT

  This table holds the original message text, divided into 254-byte parts, of a history message in OPC_HIST_MESSAGES.

- OPC_INSTR_INTERF

  This table contains the definition of instruction text interfaces.

- OPC_INSTRUCTIONS

  This table contains the text of normal instructions.

- OPC_MSG_TEXT

  This table contains the message text for messages in the OPC_ACT_MESSAGES table. To allow for various text lengths, the text is split into chunks of 254 characters.

- OPC_ORIG_MSG_TEXT

  This table contains the original (unprocessed) text of messages in OPC_ACT_MESSAGES.

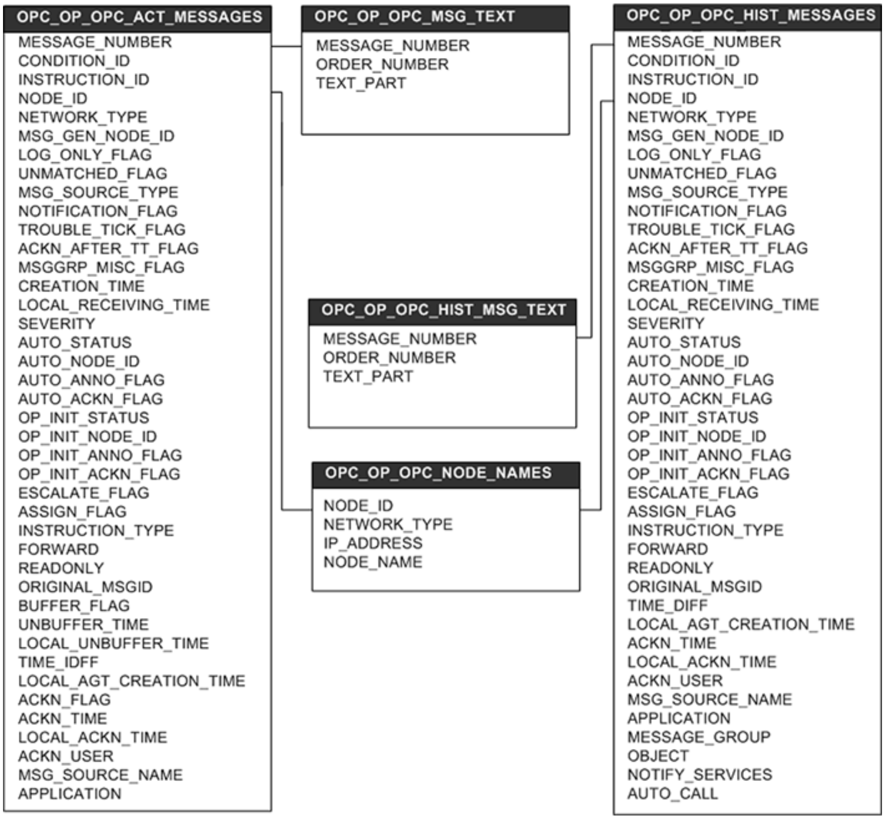
NOTE For detailed definitions and contents of the OVO database tables, please refer to *HP OpenView Operations for UNIX Reporting and Database Schema*.

The following four OVO message tables are among the most frequently used in the default report templates provided by this integration: OPC_ACT_MESSAGES, OPC_MSG_TEXT, OPC_HIST_MESSAGES, and OPC_HIST_MSG_TEXT.

Most message tables contain the field node_id, which identifies the node where the event occurred. If the node is in an internet network, you can get each node's IP address and the identifying name from another table: OPC_NODE_NAMES.

The relationship between these tables is illustrated in Figure 4-1:

Figure 4-1 **Relationship Diagram**



Message Format

The DP-OVO integration installs six message groups that are specifically designed to handle messages generated by the templates and monitors started by the DP-OVO integrations. The messages generated by Data Protector are assigned to the six message groups where appropriate:

Table 4-4 **Data Protector 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 DP-OVO integration
DP_Interactive	Detailed messages that are normally displayed only in the Data Protector interface. This message group is disabled by default. Enable this message group if you want to receive the greatest level of details about Data Protector 's operation.

An OVO message includes the following parameters:

Table 4-5 **OVO Message 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	DP-OVO integration messages
Applications	Set to Data Protector	
Node	Set to the hostname of the Data Protector system where the event occurred.	

Table 4-5 OVO Message Parameters (Continued)

Severity	Reflection of the impact that the event has on Data Protector. For messages derived from SNMP traps, 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 on a service. This value needs to map with a node in Data Protector's service tree.
Object	This depends on the impact the event has on a service. This value needs to map with a node in Data Protector's service tree. Data Protector SNMP traps set the object parameter to NOTIFICATION Messages that originate 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.

NOTE For a detailed description of different message formats based on `Message Group`, `Service Name`, and `Object`, please refer to the *HP OpenView Storage Data Protector Integration Administrator's Reference for HP OpenView Operations*.

5 Data Protector-OVO-OVSD Integration

Introduction

Data backup and recovery are critical elements in Information Technology Service Delivery and Management. Proactive management and monitoring of service quality and continuity is fundamental to any successful IT business.

HP OpenView Storage Data Protector automates the backup and recovery process for all your enterprise systems. This integration maximizes the potential of the Service Desk and OpenView Operations applications by adding seamless backup and recovery to their capabilities.

This chapter describes how OpenView Service Desk and OpenView Operations integrate with Data Protector to provide support and network-wide availability for Data Protector's backup and recovery tools.

Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Operations
- OpenView Service Desk
- Supported Oracle Database (third party software)

Product Capabilities and Integration Benefits

The integration of Data Protector, OpenView Operations (OVO), and OpenView Service Desk (Service Desk) lets you use Service Desk as a trouble ticket interface for Data Protector, and enables Service Level Management (SLM) to help you achieve a specific, consistent, measurable level of service. In short, this integration helps you achieve maximum service availability by providing a simple, effective way to do all of the following:

- Manage backup operations across geographical boundaries.
- Diagnose problems across firewall.

- Extend management perspectives beyond standard operational events and up to a business service level.
- Provide Service Level Management (SLM) to help you ensure that services are up and running. Also returns information you can use to monitor services, to react to outages, and to document conformance to SLAs.

Component List

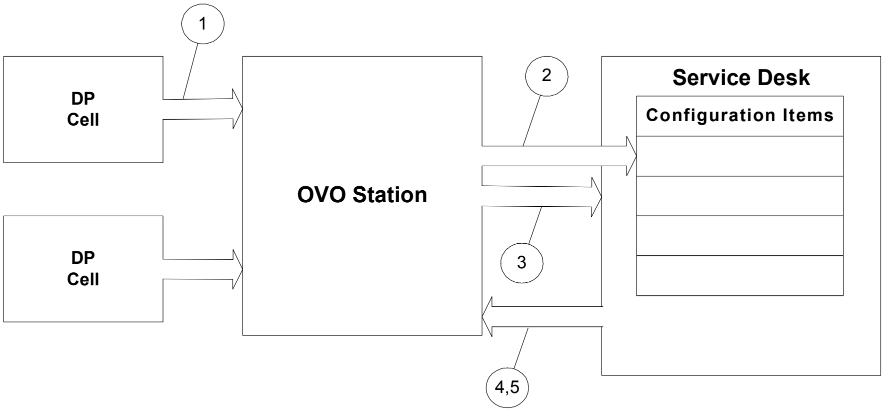
OpenView Operations

A central data collection and management point for various remote OpenView applications. Collects and analyzes data, automates critical response, as well as message forwarding to other services.

OpenView Service Desk

A central problem management point for systems, applications, and services. Systems, applications, and services are defined as “configuration items” by OVSD. OVSD registers incidents and monitors their resolution for its configuration items. OVSD manages problem resolution to ensure compliance with a configuration item specific SLA.

Import Mapping and Data Exchange



1. The administrator imports/maps Data Protector nodes managed by OVO into Service Desk as configuration items.
2. The administrator imports/maps selected OVO services, dependencies, and relations into Service Desk as configuration items.
3. OVO forwards selected events to Service Desk as incidents for the associated configuration items.
4. Service Desk sends an annotation to OVO when an incident is created for an OVO event.
5. Service Desk sends an acknowledgement to OVO when an incident associated with an OVO event is closed.

Integration Feature for Backup Operations

Data Protector normally generates two Simple Network Management Protocol (SNMP) traps for each backup session; the two traps correspond to StartOfSession and EndOfSession events in OVO. In the default configuration Data Protector forwards these event pairs to Service Desk as independent incidents, requiring operator intervention and activity to correlate the StartOfSession and EndOfSession incidents.

The following remedy not only automatically correlates the two incidents for each session, it also enables proactive management of the backup operations:

- Forward the StartOfSession event to Service Desk.
- Do not forward any EndOfSession event (completed successfully, completed with failure, session aborted, etc.); instead configure them to invoke a post-event script.

This post-event script takes four parameters: session id, backup specification, completion time, and completion status. It searches the sd_event log file for a matching StartOfSession event, retrieves its message id, and sends a request to Service Desk to update the incident associated with the StartOfSession event.

The update includes modification of:

- status (from registered to completed)
- actual finish (completion time)
- actual duration (automatically calculated based on actual start/finish)
- closure code (successful, failed, aborted)

Dependencies

Table 5-1 **Software Dependencies**

Application	Version	Platform
OVO	7.1	HP-UX 11.0 Solaris 8
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVO Agent	6.05, 7.0, 7.10	HP-UX 11.0, 11.11
OVO Database	Oracle 9i	HP-UX 11.0
OVSD Agent	4.5	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVSD (client and server)	4.5	HP-UX 11.0 Solaris 8 Windows 2000

Setup Process

The setup process for this integration consists of two main procedures:

- Installation and configuration for general integration
- Installation and configuration of backup specific integration

Installation and Configuration for General Integration

NOTE For more configuration and troubleshooting information concerning Data Protector and OpenView Operations integrations, please refer to Chapter 4, "Data Protector-OVR Integration," on page 77.

Before installing components specific to this integration, you must have the following installed:

- Data Protector. See the Data Protector Installation and Configuration Guide for detailed instructions.
- OpenView Operations. See the OpenView Operations Installation and Configuration Guide for detailed instructions.
- OpenView Operations - Service Desk Integration. This section is pertinent to general OVO and Service Desk integration, which should be in place prior to the specific integration for backup operations depicted in next section. See the *HP OpenView Service Desk 4.5 OpenView Operations Integration Administrator's Guide* for detailed instructions.

Installation The OVO and Service Desk Integration includes a number of files and tools that need to be installed on the Service Desk and the OVO servers. The following checklist shows the recommended order of installation:

1. OVO application (refer to the OVO documentation).
2. Service Desk server application (refer to the Service Desk documentation).
3. Service Desk database.

4. Integrations with Data Exchange and HP OpenView Integration Option (Service Desk part) options selected.
5. `sdagent`, `sdevent` and `sdovointegration` depot files on the OVO for UNIX server. These files are on the Service Desk CD-ROM.

Configuration

On the Service Desk Application Server:

1. Create an OVO server account starting with the letters: **OVU**.
2. Set the environment variable for Service Desk.
3. Import managed nodes as configuration items.
4. Import services as configuration items.
5. Modify the import mapping for events (vpunix events) to ensure backup properties to be imported are mapped to type incident.
6. Configure the database rules.

On your OVO Server Running on UNIX:

1. Modify the `sd_event.ini` file.
2. Make Service Desk an OVO user.
3. Move the `Service Desk` application to the `Application Bank`.
4. Modify the message source templates.
5. Deploy the monitoring policies.
6. Configure the Service Desk agent.

Exporting OVO Services as Services into Service Desk

To export OVO services as services into Service Desk:

1. On the OVO for Unix server, run:

```
/opt/OV/bin/OpC/extern_intf/sd_addservice.sh  <SD_Server>

SD account name: system

SD account passwd:
```

2. On the Service Desk server, manually execute the following steps for each exported service:
   - Set the SN socket address.
   - Set the Service Manager Person.
   - Set the associated Managed CIs.
   - Set the associated SLAs.

Installation and Configuration for a Backup-Specific Integration

This section describes the installation and configuration steps necessary for a backup-specific integration.

On your OVO Management Server Running on UNIX

1. Insert the Data Protector CD-ROM.
2. Use swinstall to install:

HP-UX	`OV_INTEGRATIONS/DP-OVO-HPUX-INTEGRATION.depot`
Solaris	`OV_INTEGRATIONS/DP-OVO-SUN-INTEGRATION.depot`

   Follow the on-screen instructions.
3. Modify the message source templates.
   a. Open `Message Source Templates`.
   b. Select `Data Protector SPI`.
   c. Double click `Group DP-SPI Unix Templates`.
   d. Select `OB_SNMP trap` and click on `Conditions`.
   e. Select `Start Of Session` notification and click on `Modify`.
   f. Select `Forward to Trouble Ticket`, and click OK.
   g. Select `Session Completed` notification and click on Modify.
   h. Go to the `Variable Bindings` section and modify `$6` to:

   ```
   <*.text1><S><*.endtime><S>BSM<S>EndOfSession<*>
   [138:701]<*>Session<S><@.sessionid><*>backup<S>
   specification<S><*.bckupspec>,<S> backup<S>group
   <S>"<*.bckupgrp>"<*.text3>Completed<*.text4>
   ```

i. Go to the Actions section, Automatic row.

j. Enter the following in the text box under Node:

```
<$OPC_MGMTSV>
```

k. Enter the following in the text box under Command.

```
/opt/OV/bin/OpC/extern_intf/informSD.sh
-t "<endtime>" -s <sessionid> -n "<bckupspec>"
-u Completed
```

l. Select Session Aborted notification and click on Modify.

m. Go to the Variable Bindings section and modify $6 to:

```
<*.text1><S><*.endtime><S>BSM<S>EndOfSession<*>
[138:701]<*>Session<S><@.sessionid><*>backup<S>
specification<S><*.bckupspec>,<S> backup<S>group
<S>"<*.bckupgrp>"<*.text3>Aborted<*.text4>
```

n. Go to the Actions section, Automatic row.

o. Enter the following in the text box under Node:

```
<$OPC_MGMTSV>
```

p. Enter the following in the text box under Command.

```
/opt/OV/bin/OpC/extern_intf/informSD.sh
-t "<endtime>" -s <sessionid> -n "<bckupspec>"
-u Aborted
```

q. Select Session Failed notification and click on Modify.

r. Go to the Variable Bindings section and modify $6 to:

```
<*.text1><S><*.endtime><S>BSM<S>EndOfSession<*>
[138:701]<*>Session<S><@.sessionid><*>backup<S>
specification<S><*.bckupspec>,<S> backup<S>group
<S>"<*.bckupgrp>"<*.text3>Failed<*.text4>
```

s. Go to the Actions section, Automatic row.

t. Enter the following in the text box under Node:

```
<$OPC_MGMTSV>
```

u. Enter the following in the text box under Command.

```
/opt/OV/bin/OpC/extern_intf/informSD.sh
-t “<endtime>” -s <sessionid> -n “<bckupspec>”
-u Failed
```

v. Repeat steps *d* and *e* for additional notifications that you want to be monitored. Examples of notifications are:

- DB Corrupted
- DB Purge Needed
- DB Space Low
- License Expires
- Mount Request
- Device Error

On the Service Desk Application Server

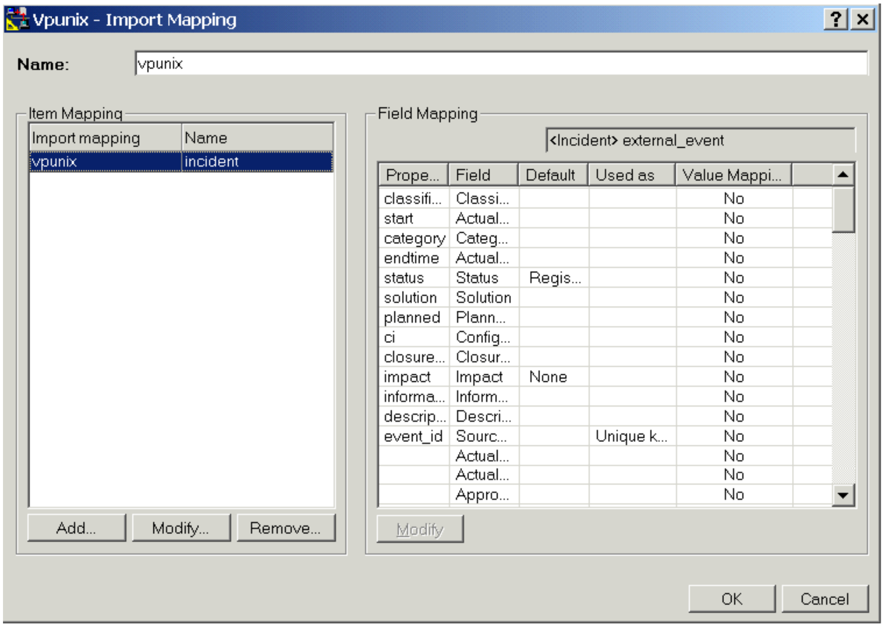
1. Import nodes for Data Protector as configuration items, if not already done.

   You may create or modify vpunixci.ini file to export managed nodes from OVO to an xml file; then use vpunixci import mapping to import the xml file to Service Desk as configuration items. You can also create them manually through Service Desk Client Console.

2. Import Data Protector-specific services as configuration items, if not already done.

   You must create or modify `ovounixservices.txt`, `ovounixservices.ini`, and schema.ini to import services listed in the text file as configuration items to Service Desk. You can also create them manually through Service Desk Client Console.

3. Modify the import mapping for events as shown below to ensure backup properties to be imported are mapped to type incident.



Name: vpunix

Item Mapping

Import mapping	Name
vpunix	incident

Field Mapping

<Incident> external_event

Prope...	Field	Default	Used as	Value Mappi...
classifi...	Classi...			No
start	Actual...			No
category	Categ...			No
endtime	Actual...			No
status	Status	Regis...		No
solution	Solution			No
planned	Plann...			No
ci	Config...			No
closure...	Closur...			No
impact	Impact	None		No
informa...	Inform...			No
descrip...	Descri...			No
event_id	Sourc...		Unique k...	No
	Actual...			No
	Actual...			No
	Appro...			No

Customization

Every customer has unique needs in IT Service Management functions. You should customize the configuration to suit your needs. Before starting, you need to have a clear understanding of your IT infrastructure and the dependency relations between the various services involved.

This section shows how to customize the configuration through a simple example.

Example

Example:

- The managed nodes include a Data Protector server named `DP001` and an OVO server named `OV001`.
- There are three backup specifications defined in Data Protector server:
  - — backTop: highest importance (within 1 hour)
  - — backHigh: high importance (within 4 hours)
  - — backLow:low importance (within 16 hours)
- These backup sessions are to receive a Gold level (24x7) service.

On the Service Desk Application Server

1. Create a service:
   - name = Backup Service
   - status = supported

   Relate all three backup sessions (backupTo, backupHigh, backLow) as its related configuration items.

2. Create the following configuration items:

Table 5-2 Configuration Items

Search code	status	Name 1	Name 2	Category
DP001	installed	Data Protector node	DP001	server
OV001	installed	OVO node	OV001	server
DATAPROTECTOR	installed	DP Mgmt Server	DATAPROTECTOR	Operational level service
OVOSERVER	installed	OVO Mgmt Server	OVOSERVER	Operational level service
backTop	installed	Top impact backup	backTop	Operational level service
backHigh	installed	High impact backup	backHigh	Operational level service
backLow	installed	Low impact backup	backLow	Operational level service

NOTE You should define the dependency among these configuration items based on your IT infrastructure.

3. Create an SLA:

- name = Backup SLA
- status = active
- service = Backup Service
- Service Level = Gold

4. Add the following closure codes for incidents:

- Successful
- Failed
- Aborted

On your OVO Server Running on UNIX:

An event forwarding script, `sd_eventins.pl`, with default attributes/values is provided for the OVO integration. You may need to modify the attribute/value mapping to better match your infrastructure.

For detailed information on modifying or creating a new import mapping, refer to the *HP OpenView Service Desk: Data Exchange Administrator's Guide*. In general, the interface for forwarding event messages to Service Desk uses the OVO API to get message details. This provides access to 48 message attributes in OVO, such as (on UNIX) message ID, message text, instructions, and annotations. To view all attributes for a message, type:

```
/opt/OV/sd/ovo/get_ovo_attributes SD sd
```

```
/opt/OV/bin/OpC/extern_intf/get_vp_attributes SD sd
3f99cf84-3066-71d6-1b41-0f005d9b0000
```

(Replace 3f99cf84-3066-71d6-1b41-0f005d9b0000 with your OVO event id.)

The output of this command lists all available attributes in square brackets ([ ]) followed by their respective values. The output looks like this:

Table 5-3 **Message Attribute Example**

[SEVERITY]	[AACTION_STATUS]
critical	undefined
[CREATION_DATE]	[OPACTION_ACK]
03/05/2002	No
[CREATION_TIME]	[OPACTION_ANNOTATE]
10:24:36	No
[RECEIVE_DATE]	[OPACTION_STATUS]
03/05/2002	undefined
[RECEIVE_TIME]	[NOTIFICATION]
10:24:36	No

Table 5-3 **Message Attribute Example (Continued)**

[AACTION_ACK]	....
No	
[AACTION_ANNOTATE]	....
No	

You decide which OVO message attributes should be inserted into which fields of an incident in Service Desk, then modify the `sd_eventins.pl` accordingly. For example:

```
#!/usr/bin/perl
#-- sd_eventins.pl
#------------------
#  Use a structure script DP_conf.pl to define mapping between OVO
# backup event and Service Desk incident.
#------------------
require "/opt/OV/bin/OpC/extern_intf/DP_conf.pl";
$previous_keyword = '';
while ($input = <STDIN>) {
  if ($input =~ /^\[/ && $input =~ /\]$/) {
    ($keyword) = ($input =~ /\[(.*)\]/);
    if ($previous_keyword ne '') {
      chop $value;
      $value =~ s/\\/\\\\\\\\/g;
      $value =~ s/\n/\\\\n/g;
      $value =~ s/"/\\"/g;
      $vp_params{$previous_keyword}=$value;
    }
    $previous_keyword = $keyword;
    $value = "";
  }
  else {
    $value = $value . $input;
  }
}
#..............................................................
# node is equal to the message service if not empty and otherwise the
# node name service information is stored in the MAP_COLORING field
$node=$vp_params{MAP_COLORING};
if ($node eq '') {
  $node=$vp_params{NODENAME};
}
#------------------
# Retrieve variable $6 string from original OVO message [ORIGMSGEXT];
# will be part of the information field for Service Desk’s incident.
#------------------
$info = substr($vp_params{ORIGMSGTEXT}, rindex
($vp_params{ORIGMSGTEXT}, "[6]"));
$exec_string = "perl /opt/OV/SD/bin/sd_event -f
/opt/OV/SD/bin/sd_event.ini -v ";
$exec_string .= "event_id=$vp_params{MSGID} ";
$exec_string .= "start=\"$vp_params{CREATION_DATE}
$vp_params{CREATION_TIME}\" ";
$exec_string .= "solution=\"$vp_params{INSTRUCTIONS}\" ";
```

```
#--- information section
$exec_string .= "information=\"Original message: $info\\n";
$exec_string .= "Detected by application: $vp_params{APPLICATION}\\n";
$exec_string .= "Object in question: $vp_params{OBJECT}\\n";
$exec_string .= "Annotations: $vp_params{ANNOTATIONS}\" ";
#--- information section
#-----
#-- Special handling for backup session
#-----
#------------------
# Set default description to the first 19 characters of OVO message
# text
[MSGTEXT].
#------------------
$desc = substr($vp_params{MSGTEXT}, 0, 19);
#------------------
# For each monitored event defined in the structure script DP_conf.pl,
# get its description and impact mappings.
# More mappings can be defined and retrieved.
#------------------
foreach $name (@process) {
    if ($node =~ /$name/) {
        $desc = "$node_info->{$name}->{'description'}";
        $severity = "$node_info->{$name}->{'impact'}->{'default'}";
        foreach $code (@impact_codes) {
            $lookup = "$node_info->{$name}->{'impact'}->{$code}";
            if ($lookup ne "") {
                if ($vp_params{ORIGMSGTEXT} =~ /$lookup/) {
                    $severity = $code;
                    last;
                }
            }
        }
        last;
    }
}
$exec_string .= "ci=\"$node\" ";
$exec_string .= "description=\"$desc\" ";
# supposed to flush output, because "exec" does not
$| = 1;
exec "$exec_string";
```

DP_conf.pl

```
#!/usr/bin/perl
#------------------
# To enable Service Desk to determine the resolution
# deadline, the impact field has to be set.
# Impact codes can be customized thru Service Desk Admin
# Console. Make sure the codes specified here are
# defined in Service Desk.
#
# The time allowed to solve an incident, depends on the
# priority (impact) given to the incident. The default:
# Top (1 hr), High (4hrs), Medium (8 hrs), Low (16 hrs),
# None (1 day 16 hrs).
# To change the time allowed to solve incidents, you map
# a solution duration to a priority code in Service Desk
# thru Admin Console.
#------------------
@impact_codes = ( 'Top', 'High', 'Medium', 'Low' );
#------------------
# Define the events to be monitored.
#------------------
@process = (
        '.BackupSessions.Running',  #-- backup event
        '[138:704]',#-- DP space low event
        '[138:706]',#-- DP corrupted event
        '[138:712]',#-- DP purge needed event
        '[138:702]'#-- mount request event
);
#------------------
# For each monitored event, define its mapping of
# “description” and “impact”fields.
# More mappings can be defined.
#------------------
$node_info = {
 '.BackupSessions.Running' => {
'description' => 'Backup: ',
 'impact' => {
 'default' => 'Medium',#-- default impact
 'Top' => 'backTop',
 #-- backTop session has highest impact
'High' => 'backHigh',
#-- backHigh session has high impact
'Low' => 'backLow'
#-- backLow session has low impact
                }
        },
        '[138:704]' => {
                'description' => 'DB Space Low',
                'impact' => {
                        'default' => 'Medium'
                }
        },
        '[138:706]' => {
                'description' => 'DB Corrupted',
                'impact' => {
                        'default' => 'Medium'
                }
        },
        '[138:712]' => {
                'description' => 'DB Purge Needed',
                'impact' => {
                        'default' => 'Medium'
                }
        },
        '[138:702]' => {
                'description' => 'Mount Request',
                'impact' => {
                        'default' => 'Medium'
                }
        },
};
```

sd_backupins.pl

This script, a variation of sd_eventins.pl, is invoked by EndOfSession events to modify the original StartOfSession incident.

```
#!/usr/bin/perl
$numArgs = $#ARGV + 1;
$ovoEventID = $ARGV[0];
$ovoStatus = $ARGV[1];
$ovoTime = $ARGV[2];
#------------------
# Set closure code for backup session ended with status:
# Completed -> Successful
# Aborted -> Aborted
# Failed -> Failed
# The closure codes can be customized thru Service Desk
# Admin Console. Make sure the codes specified here are
# defined in Service Desk.
#------------------
if ($ovoStatus =~ /Completed/) {
   $closurecode = 'Successful';
} elsif ($ovoStatus =~ /Aborted/) {
   $closurecode = 'Aborted';
} else {
   $closurecode = 'Failed';
}
$exec_string = "perl /opt/OV/SD/bin/sd_event -f
/opt/OV/SD/bin/sd_event.ini -m update -v ";
$exec_string .= "event_id=$ovoEventID ";#--
StartOfSession event id
$exec_string .= "endtime=\"$ovoTime\" ";#-- mapped to
“actual finish” field
$exec_string .= "status=\"Completed\" ";#-- mapped to
“status” field
$exec_string .= "closurecode=\"$closurecode\" ";#--
mapped to “closure code” field
#--- print "$exec_string\n";
# supposed to flush output, because "exec" does not
$| = 1;
exec "$exec_string";
```

Testing

You can test the setup by starting (in Data Protector) a backup session for any of the three backup specifications defined above. You should see an incident (StartOfSession event) being created with the right deadline calculated and the right service (and so the right SLA) related. The same event is then modified (EndOfSession event) for the following fields:

- status (from registered to completed)
- actual finish (completion time)
- actual duration (automatically calculated based on actual start/finish)
- closure code (successful, failed, aborted)

Index

A

All Hosts Backup Statistics Report, 46

B

Backup groups, 33
Backup Health
  criteria, 51
  status, 51
Backup Health Module, 50

C

Cell request server, 22, 23
Client Host Backup Report, 47
conventions, 11
Custom reports, 86
Customer models, 38
  importing, 39
Customization
  Data Protector-SIP, 33

D

Data Protector
  error messages, 42
  Integration for OVO/UNIX, 78
  reports, 52
    understanding, 52
Data Protector Integration for OVO/UNIX, 80
Data Protector Integration module, 23
Data Protector-SIP
  cell manager, 36
  customer models, 38
  filter level, 34
  gauge settings, 35
  logging, 34
  management data filter, 40
  portal views, 38
  refresh rate, 34
  troubleshooting, 56
Data Protector-SIP deployments, 25
Deployments
  Data Protector-SIP, 25

E

Error messages
  module, 42
    adding, 43
    editing, 44
  understanding, 42

G

Gauges
  protection status, 45

H

Hosts Statistics Report, 48

J

Java Developer's Kit, 21, 82

L

Logging, 34

M

Management data filter, 40
Messages, 87
  format, 90
  parameters, 90

N

Netscape Navigator, 21, 82

O

OpenView
  Operations, 78, 80, 82
  Reporter, 78, 80
  Service Information Portal, 20, 22
OpenView Operations, 18
Oracle, 78, 82
OVO, 78, 80, 82

P

Portal view
  services, 41
Portal views, 38
Protection status
  gauge, 45
  module, 45

R

Reporter, 78, 80
Reports, 52
  All Hosts Backup Statistics, 46
  Client Host Backup, 47
  custom, 82, 86
  Data List Trees, 52
  global settings, 55

Host Statistics, 48
module, 52
editing, 54
Object Last Backup Up, 53
understanding, 52

S

SIP, 20, 22
Status gauges, 23

T

Troubleshooting
Data Protector-SIP, 56
typographical conventions, 11