HP OpenView Storage Data Protector Integration Guide

for

HP OpenView SIP and Reporter

Version: A.06.00

HP-UX, Solaris and Windows

Manufacturing Part Number: B6960–96014
July 2006

Legal Notices

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

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

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

UNIX® is a registered trademark of The Open Group.

Contents

1. Introduction

Overview 14
HP OvenView SIP Integration 15
HP OvenView Reporter (OVR) Integration 15

2. Data Protector-SIP Integration

Introduction 18
Component List 18
Product Capabilities and Integration Benefits 18
How Data Protector Integrates with SIP 19
Planning the Integration 22
Installing the Integration 24
Prerequisites 24
Dependencies 25
Installing on the Data Protector Server 25
Establishing Data Protector/SIP Communication 26
Installing on a Windows SIP Server 26
Installing on an HP-UX SIP Server 26
Installing on an Solaris SIP Server 27
Installing on a Web Server 28
Installing on a Windows Web Server 28
Installing on an HP-UX Web Server 29
Installing on a Solaris Web Server 30
Customizing the Integration 32
Setting Up Backup Groups on Data Protector 32
Editing ConfigSpec.xml 32
Log Location, Log Level 33
Filter Level 33
Refresh Rate 33
Gauge Settings 34
Cell Manager Setting 35
Creating Customer Models and Portal Views 36
Customer Models 36
Importing the Customer Model 37
Management Data Filter 37
Adding and Removing Services in a Portal View 38
Modules 39
Data Protector Protection Status Module 39

Contents

Data Protector Protection Status Gauge . . . 39
Host Statistics Report . . . 41
Editing the Data Protector Protection Status Module . . . 42
Data Protector Reports Module . . . 43
Data List Trees . . . 44
Object Last Backup . . . 44
Editing the Data Protector Reports Module . . . 44
Establishing Global Settings for Reports . . . 45
Data Protector Backup Session List Report Module . . . 46
Editing the Data Protector Backup Session List Report Module . . . 46
Editing PortalView.xml Directly . . . 46
Establishing Global Settings for Reports . . . 47
Data Protector Error Messages Module . . . 47
Adding a Data Protector Error Message Module to your Portal View - GUI . . . 48
Editing the Data Protector Message Module . . . 48
Editing PortalView.xml Directly . . . 49
Establishing Global Settings for Reports . . . 49
Troubleshooting . . . 50
Error Messages . . . 50
Data Unavailable . . . 50
Parse Rest of Config . . . 50

3. Data Protector-OVR Integration

Introduction . . . 52
Prerequisites . . . 52
Product Capabilities and Integration Benefits . . . 52
Component List . . . 53
How Data Protector Integrates with OVR . . . 54
Dependencies . . . 55
Data Protector/OVR Integration . . . 57
Installing the Integration . . . 58
Prerequisites . . . 58
Installation . . . 58
Configuration . . . 58
Using the Reporter Integration with Data Protector . . . 60
Registering a Data Protector Cell Manager with the Module . . . 60
Troubleshooting . . . 60
Gathering Data from Data Protector . . . 62

Contents

Generating Reports 62
Viewing Reports 62
Creating Custom Reports 63
Creating Data Protector Custom Reports 63
Data Source 63
Message Format 66
Troubleshooting 69

Contents

Printing History

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

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

Table 1 **Edition History**

Part Number	Manual Edition	Product
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
B6960–90015	July 2006	HP OpenView Storage Data Protector A.06.00

Contact Information

General Information

General information about Data Protector can be found at

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

Technical Support

Technical support information and information about the latest Data Protector can be found at the HP Electronic Support Centers at

http://www.itrc.hp.com

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. Send feedback to

storagedocs.feedback@hp.com

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 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 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 13.

Chapter 2 “Data Protector-SIP Integration” on page 17.

Chapter 3 “Data Protector-OVR Integration” on page 51.

1 Introduction

Overview

This guide describes the integration of Data Protector with two other OpenView products: Service Information Portal and Reporter.

- **HP OpenView Storage Data Protector** is a backup and recovery solution designed specifically for enterprise-wide and distributed environments.

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

- **HP OpenView Service Information Portal (SIP)** creates a "portal" view into a customer's services for a service provider. It allows you present data from your internal applications such as Data Protector, OVIS, OVR, and OVO as reports on custom web pages for each of your clients.

- **HP OpenView Reporter (OVR)** is a management reporting tool that transforms data captured by OpenView agents into management information, including real-time and historical availability and performance reports. Reporter can also generate reports on systems managed by HP OpenView Operations (OVO).

  After collecting information based on pre-defined and user-specified lists of metrics, Reporter formats the collected data into Web page reports.

The integrations allow information from Data Protector to be used by OV SIP and OVR for their portal and reporting capabilities. With SIP, you can monitor and control Data Protector backup and recovery processes. More details are given in the following sections.

Data Protector also integrates with **HP OpenView Operations**, an operations management solution that gives you control over the IT infrastructure. It monitors, controls and reports on network, systems, storage, databases and applications. The integration is covered in two guides:

- *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations—HP-UX*

- *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations—Windows*

HP OvenView SIP Integration

The integration of Data Protector and OpenView Service Information Portal (SIP) assists Service Level Management (SLM) to help you achieve a specific, consistent and measurable level of service. It provides a simple, effective way for the following:

- 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 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.

OV SIP portal components and modules include Service Browser, Service Graph, and Service Cards.

HP OvenView Reporter (OVR) Integration

The integration of OpenView Reporter with Data Protector, via OpenView Operations, provides detailed and in-depth information concerning the health and status of Data Protector's data protection services.

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

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

- Additional reports can be generated, customized, or modified using Crystal Reports. This product is not included with OVO, OVR, or Data Protector. Refer to the Crystal Reports documentation for template and configuration information.
- The reports provide a high-level view of the data protection services for the whole enterprise.

2 Data Protector-SIP Integration

Introduction

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

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.

Product Capabilities and Integration Benefits

The integration of Data Protector and OpenView Service Information Portal (SIP) assists Service Level Management (SLM) to help you achieve a specific, consistent and measurable level of service. It provides a simple, effective way for the following:

- 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 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.

The integration consists of two main elements:

- The *Data Protector Integration module*, installed on the SIP server or a separate web server.

  The module's components are automatically installed with SIP, and are on your SIP web server or on a separate web server, depending on your deployment.

  The module consists of two primary elements:

  — SIP components, including SIP XML, XSL, and module definitions.

  — SIP-Data Protector servlets, including the following Java servlets, as well as the Configuration Specifications, `ConfigSpec.xml`:

    — `CustomerGroup` servlet: provides the customer model to the SIP Management Data Filter.

    — `Reporter` servlet: generates and creates XML reports, and includes a configurable threading option.

    — `StatusGauge` servlet: generates status gauges.

- The *Cell Request Server (CRS) process*, installed on the Data Protector cell manager, which sends reports to SIP via the socket. For information on configuring this module, see "Installing the Integration" on page 24.

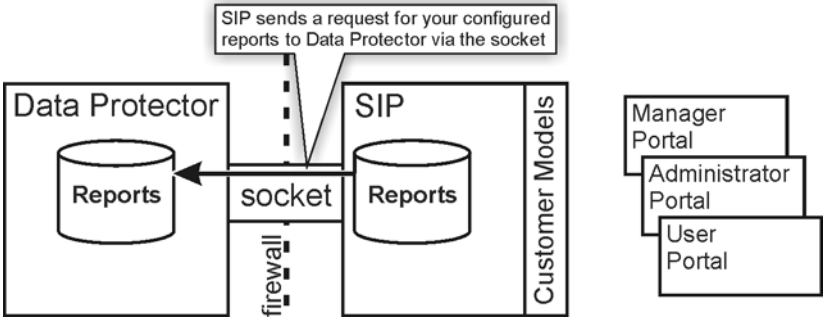
How Data Protector Integrates with SIP

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

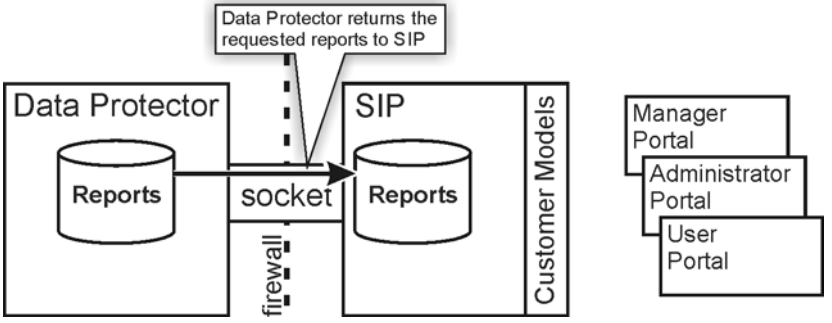
1. You, a user, request a report.
2. The request goes to the Customer Group servlet, which:

   a. maps you to the groups in your customer profile,

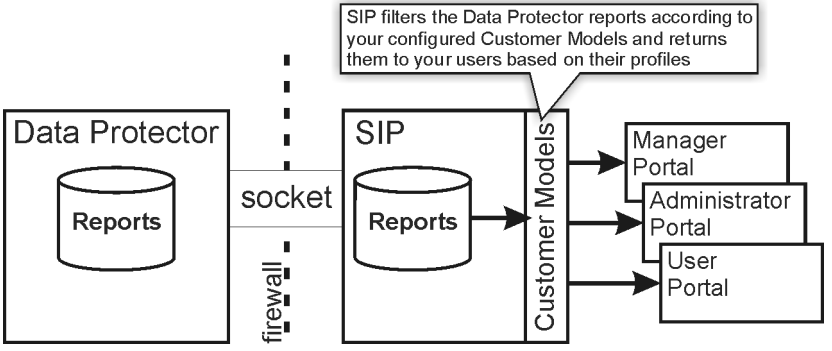
b. sends the request to Data Protector's report database via the socket connection between the SIP portal and Data Protector.



3. Data Protector sends report data via the socket connection to the Docs servlet and/or the Gauges servlet to be formatted.



4. The information is formatted. The final reports and gauges pass through the security filter, and are returned to you.



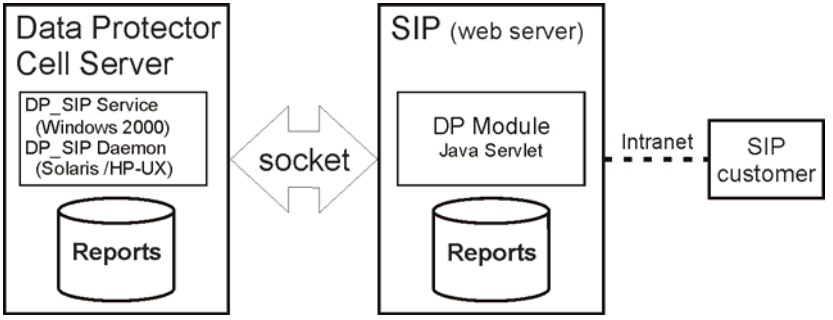
See “Planning the Integration” on page 22 for detailed information about how SIP and Data Protector work together.

Planning the Integration

Before setting up your Data Protector cell manager with SIP, you need to determine which deployment model to use. There are three basic models:

- **Deployment A:** 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.

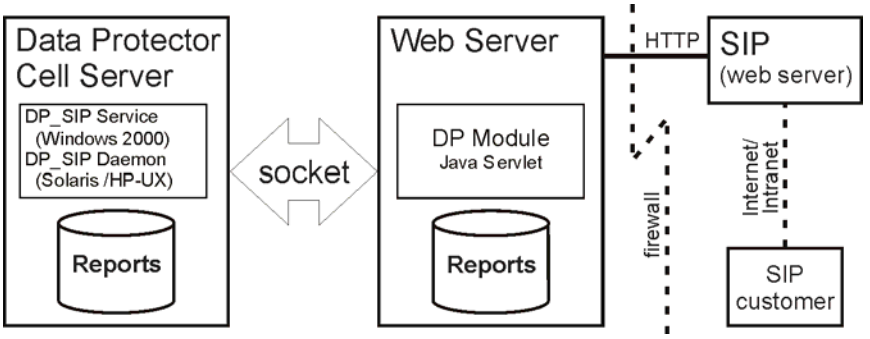
  This option is for cases in which all customers are internal. It can be implemented either completely behind a firewall or with access to SIP via port 8080 to a user portal outside the firewall.



  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 (8080) and accessed by an external customer.

- **Deployment B:** The Data Protector integration module resides on a web server that communicates with SIP via HTTP through the firewall.

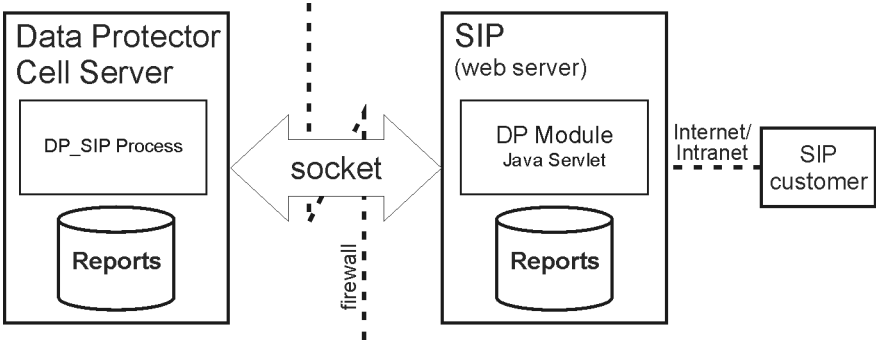
The Data Protector module for SIP is run on a web server within the firewall. This module communicates with SIP remotely through the firewall via HTTP, and communicates with the Data Protector cell manager through sockets completely contained within the firewall.



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:** Data Protector and SIP communicate through a socket completely contained within the firewall.

  The Data Protector module for SIP runs on the SIP server outside the corporate firewall. It communicates with the Data Protector cell manager via socket on port 5555 through the firewall.



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

Installing the Integration

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

Prerequisites

SIP and Data Protector must already be installed:

- To install SIP, see the *Service Information Portal Installation Guide*.
- To install Data Protector, see the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Table 2-1 Software Requirements—Data Protector

Operating System	Data Protector Version			
	5.0	5.1	5.5	6.0
HP-UX 11.0	✔	✔	✔	✔
HP-UX 11.11	✔	✔	✔	✔
HP-UX 11.23			✔	✔
Solaris 7	✔	✔	✔	✔
Solaris 8	✔	✔	✔	✔
Solaris 9		✔	✔	✔
Solaris 10				✔
Microsoft Windows XP Professional (32-bit)	✔	✔	✔	✔
Microsoft Windows 2000	✔	✔	✔	✔
Microsoft Windows Server 2003		✔	✔	✔
SUSE Linux Enterprise Server 9 (x64)				✔

Table 2-2 Software Requirements—SIP

Operating System	Version
HP-UX 11.10, 11.11 Solaris 7 and 8 Windows 2000, 2003	3.1, 3.2

Before installing the integration (on any platform or server), ensure 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

Dependencies

- Sun's Java Developer's Kit 1.3 is required for SIP 3.1.
  Java Developer's Kit 1.4.2 is required for SIP 3.2.
- Some OpenView components require Netscape Navigator 4.7 to be installed. This is unnecessary as long as alternative means of browsing HTML pages is available (such as a web browser on a separate machine, or an alternative compatible web browser).
- The environment must be properly set and configured before installing the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about specific requirements, see the installation guides for those components.
- This integration uses Data Protector backup specification groups. See the Data Protector online Help index: "backup specification groups" for more information and how to configure them.

Installing 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, associate the Data Protector organizations (imported via the customer model) with Roles. See the *SIP Deployment and Integration Guide* for more information.

Installing on a Windows SIP Server

1. Insert the Data Protector Windows installation DVD.
2. Change directory to `OV_Integrations`.
3. Run `DP-SIP-WIN_A.06.00.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 36
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize `ConfigSpec.xml` as described in “Editing ConfigSpec.xml” on page 32.

Installing on an HP-UX SIP Server

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

   `DP-SIP-HPUX_A.06.00.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 36
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.

7. Customize `ConfigSpec.xml` as described in “Customizing the Integration” on page 32.
8. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) as follows:
   a. Edit the file `APACHE_HOME/apache/conf/jk.conf`
   b. *For SIP 3.1:* Find the line:

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

   c. *For SIP 3.1:* Add the following lines:

      ```
      JkMount /dpreporter/* ajp12
      JkMount /dpreporter ajp12
      ```

   d. Stop and restart Apache and TOMCAT.

Installing on an Solaris SIP Server

1. Insert the Data Protector Solaris installation DVD.
2. As root, use `pkgadd` to install the following depot:

   ```
   DP-SIP-SUN_A.06.00.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 36
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize `ConfigSpec.xml` as described in “Customizing the Integration” on page 32.
8. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) as follows:
   a. Edit the file `/opt/OV/SIP/apache/conf/jk.conf`
   b. *For SIP 3.1:* Find the line:

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

c. *For SIP 3.1:* 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 in this section appropriate for 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.

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 web server and application server. This is not covered in the steps below. Refer to your application server and web server documentation.

Installing on a Windows Web Server

1. Insert the Data Protector Windows installation DVD.
2. Change directory to `OV_Integrations`.
3. Run `DP-SIP-WIN_A.06.00.exe`.
4. Follow the steps in the Setup Wizard, selecting `SIP Servlet Only`.

On the SIP portal machine, insert the Data Protector Windows installation DVD:

1. Change directory to `OV_Integrations`.

2. Run `DP-SIP-WIN_A.06.00.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 36
5. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
6. Customize `ConfigSpec.xml` as described in "Editing ConfigSpec.xml" on page 32.

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

   `DP-SIP-HPUX_A.06.00.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 "Editing ConfigSpec.xml" on page 32.
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. *For SIP 3.1:* Find the line:

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

   c. *For SIP 3.1:* 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 DVD:

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 36
4. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.

Installing on a Solaris Web Server

To install the integration on a Solaris web server:

1. Insert the Data Protector Solaris installation DVD.
2. As root, use `pkgadd` to install the following depot:

   `DP-SIP-SUN_A.06.00.pkg`

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 "Editing ConfigSpec.xml" on page 32.
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. *For SIP 3.1:* Find the line:

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

   c. *For SIP 3.1:* 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 Solaris DVD:

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

   `DP-SIP-SUN_A.06.00.pkg`

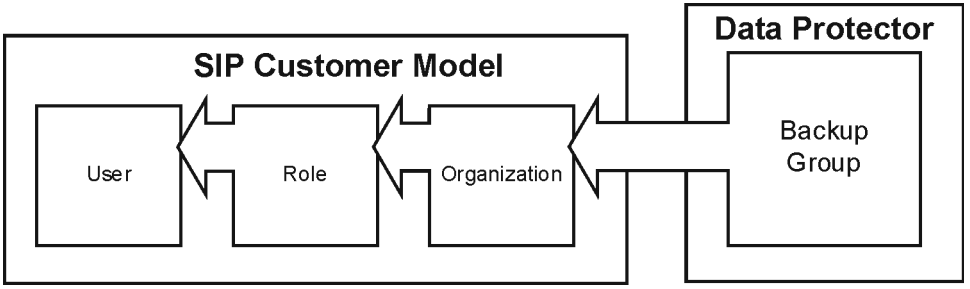
2. Select and install the `Solaris SIP` component.
3. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 36
4. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.

Customizing the Integration

Setting Up Backup Groups on Data Protector

To receive reports via SIP, 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 2-1. For more information about configuring groups, see the Data Protector online Help index: “backup specification groups”.

Figure 2-1 Backup Group Mappings



IMPORTANT

Backup specification group names must *not* include periods (.) or question marks (?).

If you define a role containing overlapping backup groups, users with that role will see redundant data in their reports.

Editing ConfigSpec.xml

There are several options for customizing your integration in the file `ConfigSpec.xml`, 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 following sections describe these options.

Log Location, Log Level

Log Level determines the level at which events will be logged (1 - 5).

Log Location specifies the name and location of your log file. You must specify an existing directory.

Syntax:

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

Example: The log level is 3, so events with a severity of 3, 2, or 1 will be logged. The log file `msgtxt` is located in the directory `d:/tmp/logging/`:

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

Filter Level

Determines which types of messages are delivered. Set each message type as true (delivered) or false (not delivered).

Example: Messages tagged Major and Critical are delivered; those tagged Minor and Warning are not:

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

NOTE Message filters in `ConfigSpec.xml` apply at system level. Any message levels filtered out here will not be logged to your SIP or web server.

Refresh Rate

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

To set the refresh rate, edit the line:

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

- **update_rate** is the refresh rate in minutes. Avoid values <10.
- **archive_rate** is the rate at which archived reports expire from the system, that is, the time in minutes that a recently accessed report will be maintained on the system. The recommended minimum is five minutes. `Archive_rate` should be greater than `update_rate`.
- **file_loc** is the location of the files gathered and archived to support `RefreshRate`. Enter a valid, existing directory. This repository may need to be very large if you expect many users to log on at the same time.

Example: 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 Data Protector system health graphically using a gauge with three ranges: green, yellow, and red, indicating the protection status.

You can change the default settings to reflect the sensitivity of your data or the critical nature of systems you are backing up.

To set the gauges, edit the line:

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

Example:

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

Do not allow color bands to overlap. If you change green to 0-70, you must also change the lower value of yellow to 70.

NOTE Gauge settings in `ConfigSpec.xml` are applied to your entire system. If you want some settings to be specific to a given module view, see “Editing the Data Protector Protection Status Module” on page 42. You can 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 language, port number, and Java user password. If the Data Protector Administrator has changed either the Data Protector port or added a password for a Java user, edit this variable so that the integration servlets can communicate with Data Protector.

To identify a cell manager, edit the line:

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

where:

- *locale*: the language of the cell manager. Required.
- *port*: the port the integration uses to communicate with the cell manager. *Default:* 5555
- *password*: optional. Only needed if the Data Protector Administrator wants to create a Java user account. *Default:* none
- *host_name*: identifies the cell manager using a fully qualified host name or IP address. Required.

NOTE

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

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

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

This section discusses:

- Customer Models: the concept and how they are used within Data Protector and SIP.
- Management Data Filter: how it is used to serve appropriate information to users.
- Adding and Removing Services in a Portal View: how to configure Data Protector services for display within a SIP portal view.

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

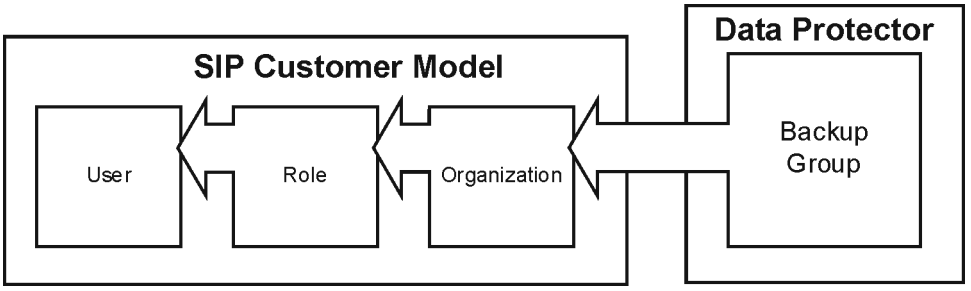
Customer Models

To help you present the correct information to your users, SIP employs an expandable concept of customer models. With these, you can create and fine-tune different portals for users according to the department they work in, their job functions, security considerations, and so on.

To generate reports properly, each cell manager is used to create a basic organization named `group@cellserver` where the host is specified. Detailed instructions for segmenting data and creating customer models are in the *SIP Deployment and Integration Guide*.

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

Figure 2-2 Customer Model



Importing the Customer Model

Import the customer model from the SIP servlet as follows:

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:

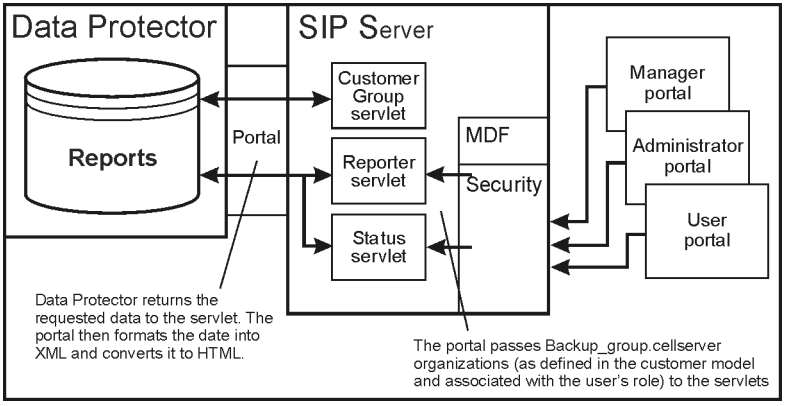
   `http://`*`servlet_host.com`*`/dpreporter/customer`

   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 2-3 Management Data Filter Overview



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, and can include multiple organizations.

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

For more details 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 a role 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 is inserted into your `PortalView.xml` file and displayed in the portal view. To edit the modules, see "Data Protector Error Messages Module" on page 47, "Data Protector Protection Status Module" on page 39, or "Data Protector Reports Module" on page 43.

Modules

Data Protector Protection Status Module

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

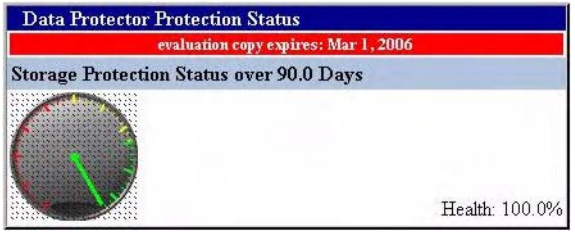
The Data Protector Protection Status module displays a visual representation of the success rates of your backups.

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

Gauges appear when the tab first displays in your portal. They indicate the overall health rating for services monitored by each gauge. View details by clicking on a gauge or a health title link.

Data Protector Protection Status Gauge

The Data Protector Protection Status gauge shows the status of the backup statistics for all organizations associated with the current role. This is calculated by averaging information from all the organizations.



All Hosts Backup Statistics Report Click a Protection Status Gauge on the main portal window to see the `All Hosts Backup Statistics` report, a detailed listing of information about your system's protection status.

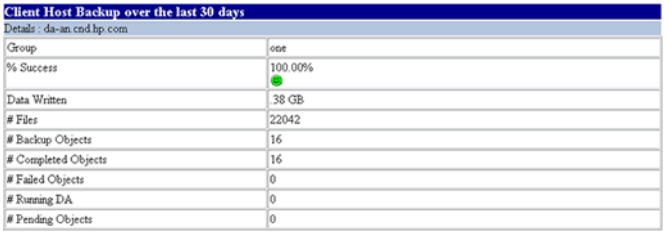
All Hosts Backup Statistics over the last 30 days

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

Client Host	Name of the cell manager

User Group	Name of the customer group
% Success	Percentage of successful backup requests. The number in this field is expandable. See page 41 for details.
Data Written	Amount of backup data written (gigabytes)
# Completed Objects	Number of completed backup jobs
# Failed Objects	Number of failed backup jobs
# Running DA	Number of disk agents currently running
# Pending Objects	Number of pending backup jobs

Client Host Backup Report Click on the `% Success` field in the `All Hosts Backup Statistics` page to see the `Client Host Backup Report`, an expanded detail view of the protection status for the selected customer group on the cell manager.



Client Host Backup over the last 30 days

Details : da-an.cnd.hp.com

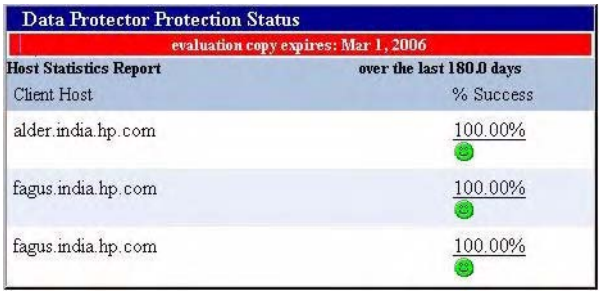
Group	one
% Success	100.00%
Data Written	38 GB
# Files	22042
# Backup Objects	16
# Completed Objects	16
# Failed Objects	0
# Running DA	0
# Pending Objects	0

Details:	Name of the cell manager to which the report applies
Group	Name of the customer group
% Success	Percentage of successful backup requests. The number in this field is expandable. See page 41 for details.
Data Written	Amount of backup data written
# Files	Number of files backed up
# Backup Objects	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.

# Completed Jobs	Number of completed backup jobs
# Failed Objects	Number of failed backup jobs
# Running DA	Number of disk agents currently running
# Pending Objects	Number of pending backup jobs

Host Statistics Report

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



Time Frame	Time frame for which data is collected/displayed (“`over the last 30 days`” in the example above)
Client Host	Qualified host name of the cell manager
% Success	Percentage of successful backup requests. The number in this field is expandable. See the following section for details.

Detail View Click on a percentage in the main portal window to see the `All Hosts Backup Statistics` report, a detailed listing of information about your system’s protection status. See “All Hosts Backup Statistics Report” on page 39 for more information.

Click on a percentage in the `All Hosts Backup Statistics` report to display the `Client Host Backup Report` and a further level of detail. See “Client Host Backup Report” on page 40 for more information.

Editing the Data Protector Protection Status Module

The Protection Status 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. Use the Edit page to customize the module.

Using the Protection Status - Edit page To customize the Protection Status module, click on the `Edit` button in the title bar. The `Data Protector Protection Status – Edit` pane is displayed.

Data Protector Servlet host:	Fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Module	Select the version of the module to display: `Status Gauge` or `Host Status`.
Over the last:	Time frame from which to display results.
Warning % At and Below:	Success percentage above which the protection status is considered normal/successful. Status at or below are considered warning.
Critical % At and Below:	Success percentage at or below which the protection status is considered to be critical.

Protection Status Criteria Criteria for gauging protection status are pre-configured in this system, so you do not need to configure these gauges. You can, however, configure thresholds for the general protection status, or severity.

Protection status are generally defined as follows:

Normal	Safe health range; 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 probably imminent; the situation should be resolved immediately.

You can change thresholds for these statuses globally based on factors within your unique environment. See “Editing ConfigSpec.xml” on page 32 for details.

Editing PortalView.xml Directly You can edit `PortalView.xml` file directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP Deployment and Integration Guide* for details.

Data Protector Reports Module

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

The following 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. One report is generated per group; customers with multiple groups get multiple reports.

Data Protector Reports

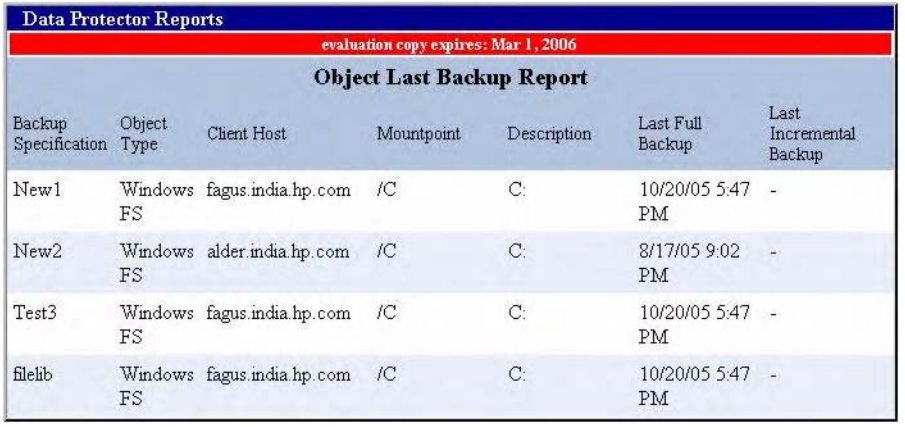
evaluation copy expires: Mar 1, 2006

Data List Tree Report

Backup Specification	Object Type	Client Host	Mountpoint	Tree
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/Backup.4BP
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BK
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BR
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB006.4BK
New2	Windows FS	alder.india.hp.com	/C	C:/BuildsNPatches
Test3	Windows FS	fagus.india.hp.com	/C	C:/j2sdk1.4.1_03

Object Last Backup

This basic report shows all objects owned by a group and the data of the last full and partial backup for that group. One report is generated per group; customers with multiple groups get multiple reports.



Data Protector Reports

evaluation copy expires: Mar 1, 2006

Object Last Backup Report

Backup Specification	Object Type	Client Host	Mountpoint	Description	Last Full Backup	Last Incremental Backup
New1	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-
New2	Windows FS	alder.india.hp.com	/C	C:	8/17/05 9:02 PM	-
Test3	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-
filelib	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-

Editing the Data Protector Reports Module

Use the Edit page to customize the Reports module:

Click on the `Edit` button  in the title bar. The `Data Protector Reports - Edit` pane is displayed.

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	Select which report to display, `Data List Trees` or `Object Last Backup`.

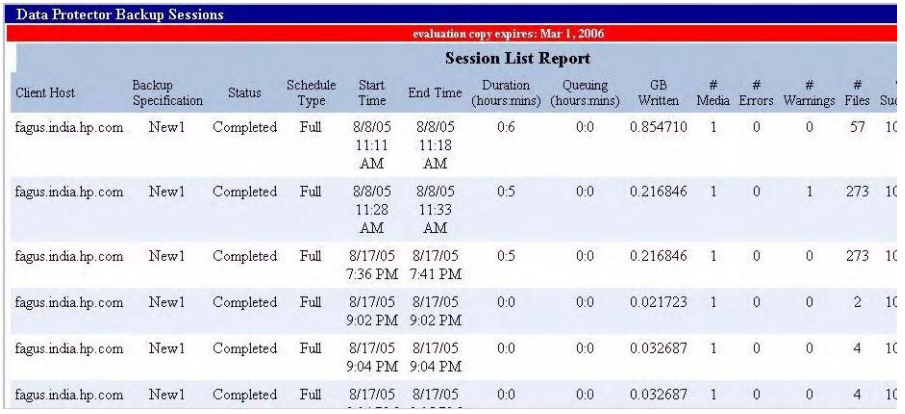
Editing PortalView.xml Directly You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP Deployment and Integration Guide* for details.

Establishing Global Settings for Reports

For more information about establishing global settings for reports, see “Editing ConfigSpec.xml” on page 32.

Data Protector Backup Session List Report Module

The Backup Session List Report module provides backup session information over a period from Data Protector on one or more cell managers in your management domain. This basic report details all backup sessions associated with backup specifications of groups associated with the SIP customer.



Data Protector Backup Sessions

evaluation copy expires: Mar 1, 2006

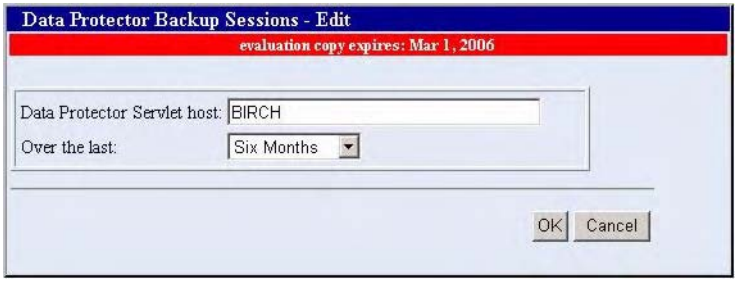
Session List Report

Client Host	Backup Specification	Status	Schedule Type	Start Time	End Time	Duration (hours:mins)	Queuing (hours:mins)	GB Written	# Media	# Errors	# Warnings	# Files	Su
fagus.india.hp.com	New1	Completed	Full	8/8/05 11:11 AM	8/8/05 11:18 AM	0:6	0:0	0.854710	1	0	0	57	1(
fagus.india.hp.com	New1	Completed	Full	8/8/05 11:28 AM	8/8/05 11:33 AM	0:5	0:0	0.216846	1	0	1	273	1(
fagus.india.hp.com	New1	Completed	Full	8/17/05 7:36 PM	8/17/05 7:41 PM	0:5	0:0	0.216846	1	0	0	273	1(
fagus.india.hp.com	New1	Completed	Full	8/17/05 9:02 PM	8/17/05 9:02 PM	0:0	0:0	0.021723	1	0	0	2	1(
fagus.india.hp.com	New1	Completed	Full	8/17/05 9:04 PM	8/17/05 9:04 PM	0:0	0:0	0.032687	1	0	0	4	1(
fagus.india.hp.com	New1	Completed	Full	8/17/05	8/17/05	0:0	0:0	0.032687	1	0	0	4	1(

Editing the Data Protector Backup Session List Report Module

Use the Edit page to customize the Backup Session List Report module:

Click on the Edit button  in the title bar. The Data Protector Backup Sessions - Edit pane is displayed.



Editing PortalView.xml Directly

You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP Deployment and Integration Guide* for details.

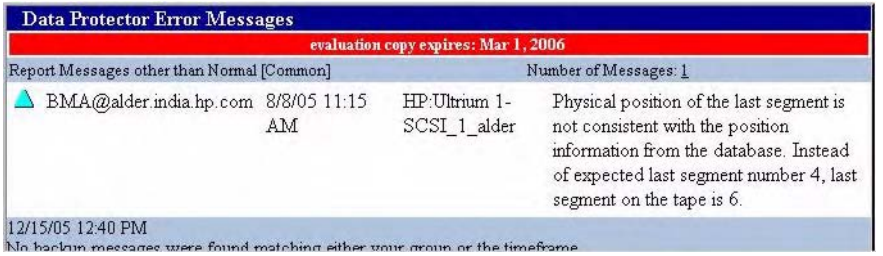
Establishing Global Settings for Reports

For more information about establishing global settings for reports, see “Editing ConfigSpec.xml” on page 32.

Data Protector Error Messages Module

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

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



The 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 Data Protector online Help index: “notifications/types”.

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

To add a Data Protector message module to a SIP portal:

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 one with ViewAdmin editing permissions.
2. Navigate to the `Storage` tab.
3. At the bottom of the right column, either:
   - Select `Data Protector 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 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.

Editing the Data Protector Message Module

To modify the Message module in your SIP portal:

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 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  in the title bar. The Data Protector Error Messages - Edit pane is displayed.

   - From the `Over the last:` menu, choose a timeframe.
   - In the `Data Protector Servlet host:` field, enter the qualified host name and port of the appropriate servlet.

5. Click `OK` to apply the changes and return to the main portal view.

Editing PortalView.xml Directly

You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP Deployment and Integration Guide* for details.

Establishing Global Settings for Reports

For more information about establishing global settings for reports, see “Editing ConfigSpec.xml” on page 32.

Troubleshooting

Error Messages

Data Unavailable

If this message appears after adding a module while viewing reports, 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 large enough to be likely to contain data.

Parse Rest of Config

If you receive 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-OVR Integration

Introduction

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

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

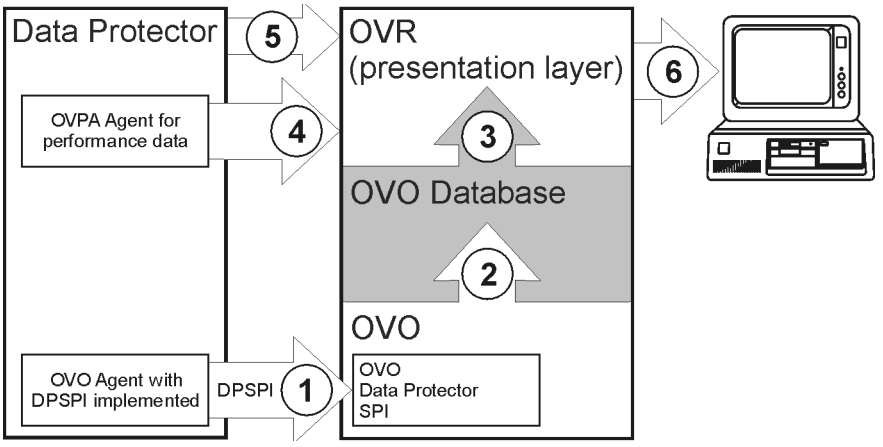
This integration maximizes the potential of OVO, OVR, and Data Protector, providing all of the following benefits:

- Enterprise-level data is presented in easy to read charts, tables, and graphs, making it simpler to review and analyze.
- Critical information concerning Data Protector services is available through any compatible web browser on your network, so administrators are not tied to a single location for accessing the Data Protector or Operations machines.
- Additional reports can be generated, customized, or modified using Crystal Reports. This product is not included with OVO, OVR, or Data Protector. Refer to the Crystal Reports documentation for template and configuration information.
- The reports provide a high-level view of the data protection services for the whole enterprise.

Component List

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 forwarding messages to other services.
OpenView Reporter	A reporting service that further analyzes, inspects, and collects data gathered by OVO and formats it into a web-based presentation.
Data Protector Integration for OVO/UNIX	Helps you 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 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. See 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 is available on another machine.
- The correct environment is required before installing the components of the integration. This may include installing various patches, software, and changing settings. Please refer to the corresponding installation guides for more information.

Table 3-1 Software Requirements

Application	Version	Platform
OVO UNIX	7.x, 8.x	HP-UX 11.00, 11.11 and 11.23 Solaris 8, 9
Data Protector	5.0	HP-UX 11.00, 11.11 Solaris 7, 8 Windows 2000, XP
	5.1	HP-UX 11.00, 11.11 Solaris 7, 8, 9 Windows 2000, XP, 2003
	5.5	HP-UX 11.00, 11.11, 11.23 Solaris 7, 8, 9 Windows 2000, XP, 2003
	6.0	HP-UX 11.00, 11.11, 11.23 Solaris 7, 8, 9, 10 Windows 2000, XP, 2003 SUSE Linux Enterprise Server 9 (x64)
OVO Agent	7.10, 8.10	HP-UX 11.00, 11.11, 11.23 Solaris 8, 9
OVO DB	Oracle 8i/9i	HP-UX 11.00, 11.11

Table 3-1 Software Requirements

Application	Version	Platform
OVR	3.5	Windows 2000
	3.6	Windows 2000, 2003

Table 3-2 Supported Platforms

Application	Supported Version	Supported OS Platform
OVR 3.5 and OVO/Unix 7.x on separate systems (OVR is Windows, OVO Management Server is Unix)	Reporter 3.5	Windows 2000
OVR 3.6 and OVO/Unix 7.x/8.x on separate systems (OVR is Windows, OVO Management Server is Unix)	Reporter 3.6	Windows 2000, Windows 2003

Data Protector/OVR Integration

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

- *DP/OVO/OVR integration*
  Populates Data Protector specific data into the OVO database. To produce Data Protector specific reports, OVR reads the OVO database to retrieve data. An Oracle 8i/9i client should be installed on the OVR server.
- *DP/VPPA/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 port other than 5555 is used, this part of integration will not work. The password for the user `Java` must be the default password.

Installing the Integration

Prerequisites

- A working Data Protector-OVO integration
- A working OVO-OVR installation

See the *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations* or the OVR installation documents for more information.

Installation

To install the Data Protector-OVO-OVR integration:

1. On the OVR system, insert the Data Protector Windows DVD.
2. Change to the `OV_Integrations` directory.
3. Run: `Data Protector-Reporter Integration.exe`
4. If you are installing the integration package on Reporter version 3.6, you are prompted to select the version of the OVO Management Server (OVO 7.x or OVO 8.x). Select the version of the Management Server available in your environment. Based on the selection, the installer will install the appropriate reports.
5. Follow the on screen instructions to complete the installation.

Configuration

If you have followed the suggested order of installation and the Data Protector-OVO integration has already been installed and configured, you should not need to configure the Data Protector-OVR integration, 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. If the reports do not work, check the integration.

To configure a transaction report manually, you must integrate Data Protector with ARM by linking the `libarm.sl` files in Data Protector and OVPA. For details, see the Data Protector online Help index: “ARM integration”.

In `Database` is present under **Configure** in the File Menu, the default configuration installed by the integration is:

- *For `Database`:* `openview`
- *For `Server or DSN`:* `ov_net8`

Change the value of `Database` according to the database of the OVO UNIX Management Server being used.

If the OVO UNIX Management Server is 8.*x*, leave the `Server or DSN` value at the default of `ov_net8`. If the server is 7.*x*, change it to `ov_net`.

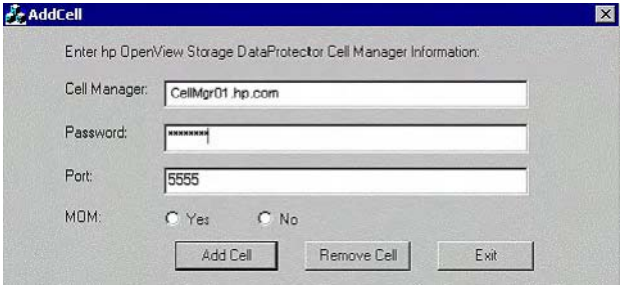
Using the Reporter Integration with Data Protector

Registering a Data Protector Cell Manager with the Module

To use the Reporter Integration, you must register the Data Protector Cell Manager with this module. Use the executable utility `AddCell.exe` in `<INSTALL_DIR>\bin` to register the Data Protector Management System.

You are asked to provide the following:

- The hostname of the Data Protector Cell Manager
- Java user password (*default:* no password)
- The port number of the `omniInet` process (*default:* `5555`)
- Whether the Data Protector Cell Manager is a manager of managers system



Add Cell Window

Use this to register as many Data Protector Cell Managers as required.

Troubleshooting

Error Message `Not able to load Reporter Database!!`

Description The application cannot access the Reporter database.

Action Ensure that the reporter database is accessible.

Error Message
```
Not able to Resolve the host name!!
This cell information is not updated.
```

Description The application cannot resolve the host name.

Action Ensure the host system exists and is accessible.

Error Message
```
Cell information is not added into database now...!!
Error Code: 42502
```

Description The application cannot find the required database table.

Action Ensure the database table `DPCELLS` is present.

If the tables do not exist, create/recreate them as follows:

```
newdb -xml
<INSTALL_DIR>\newconfig\Packages\DPCELLS.xml
newdb -xml
<INSTALL_DIR>\newconfig\Packages\DPTREND.xml
newdb -xml
<INSTALL_DIR>\newconfig\Packages\DPPool.xml
```

Error Message
```
Cell information already exists in the Reporter
database!!
Error Code: 23000
```

Description A Data Protector Cell Manager is already registered with ReporterLite, and you cannot use this application to update the information.

Action To add the same Data Protector Cell Manager with different information, remove the existing information from the database and then add the new information. To remove (or de-register) a Cell Manager, use the `AddCell.exe` application, enter the relevant details and click **Remove Cell**.

Once the Cell Manager is de-registered, data for reports can no longer be collected from it.

Gathering Data from Data Protector

Once Data Protector Cell Managers are registered to ReporterLite, the utility `DPGather.exe` collects data from them. It is launched automatically when required.

Generating Reports

Reporter utility `Repcrys.exe` generates reports. It is launched automatically when required.

Viewing Reports

Use the following link to view generated reports:

`http://<OVR_SERVER>:PortNumber/HPOV_Reports/Family_Data_Protector_Service_Level_Reports.htm`

Creating Custom Reports

The Data Protector integration with OpenView Reporter includes a predefined set of reports on the general health of the backup system and overall backup statistics. You can modify these by changing the default report settings. However, if you want to report on data from new or modified metric lists, you must create new custom report templates.

You can modify report templates and create new ones with Seagate Crystal Reports. (Crystal Reports Professional 10 was used to develop the default templates.)

For instructions, see:

- 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)

Creating Data Protector Custom Reports

When creating 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

Data Protector-OVO generates messages to help you monitor and manage the health and performance of your Data Protector environment with OVO.

These messages are stored in two sets of OVO message tables: active and history. Although these have the same attributes, the two message types 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 the GUI. The message text and original message text are also stored in separate text tables for performance reasons.

OVO message tables include:

OPC_ANNO_TEXT	Annotation text for messages in OPC_ACT_MESSAGES.
OPC_ACT_MESSAGES	The main entry for messages that are currently in the Message Browser window. It can also contain up to 50 acknowledged messages. When more than 50 messages have the ackn_flag set to Yes, they are moved to the history table.
OPC_ANNOTATION	The main entry of message annotations for messages in OPC_ACT_MESSAGES.
OPC_ESCAL_ASSIGN_M	Message numbers of owned messages and messages escalated to or from another management server.
OPC_FORWARD_MSGS	Messages that have been forwarded to other management servers.
OPC_HIST_ANNO_TEXT	Annotation text for history messages in OPC_HIST_MESSAGES.
OPC_HIST_ANNOTATION	Annotations for a history message in OPC_HIST_MESSAGES.
OPC_HIST_MESSAGES	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	The message text, divided into 254-byte parts, for messages in OPC_HIST_MESSAGES table.
OPC_HIST_ORIG_TEXT	The original message text, divided into 254-byte parts, of a history message in OPC_HIST_MESSAGES.
OPC_INSTR_INTERF	The definition of instruction text interfaces.
OPC_INSTRUCTIONS	The text of normal instructions.

OPC_MSG_TEXT	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	The original (unprocessed) text of messages in OPC_ACT_MESSAGES.

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

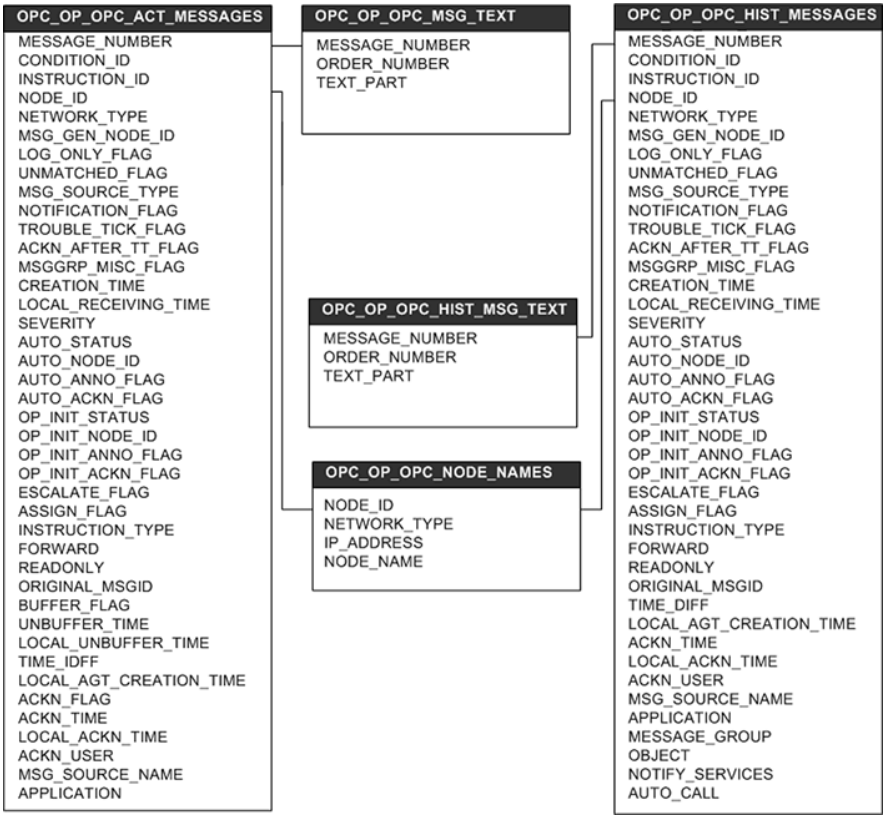
Four OVO message tables are among those most frequently used in the default report templates provided by this integration:

- OPC_ACT_MESSAGES
- OPC_MSG_TEXT
- OPC_HIST_MESSAGES
- 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 find each node's IP address and the identifying name from the table OPC_NODE_NAMES.

The relationship between these tables is illustrated in Figure 3-1:

Figure 3-1 Relationship Diagram



Message Format

The DP-OVO integration installs six message groups 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:

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 normally displayed only in the Data Protector interface. This message group is disabled by default. Enable the group if you want to receive the most detail about Data Protector's operation.

An OVO message includes the following parameters:

Message Group	The following 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	The hostname of the Data Protector system where the event occurred.	
Severity	The impact that the event has on Data Protector. For messages derived from SNMP traps, the severity value of the SNMP trap is used.	
Service Name	Depends on the impact the event has on a service. Must map with a node in Data Protector's service tree.	

Object	Depends on the impact the event has on a service. Must 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. • a monitor set the Object parameter to the name of the monitor.

NOTE

For details of different message formats based on `Message Group`, `Service Name`, and `Object`, see the *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations—HP-UX* or *Windows* as appropriate.

Troubleshooting

Problem	Resolution
While attempting to install the report package, setup was unable to detect HP OpenView Reporter on the machine.	Make sure the machine on which you are installing has HP OpenView Reporter A.03.50 or higher 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.03.50 or higher.
Installed HP OpenView Reporter version is not A.03.50 or higher.	Upgrade or install HP OpenView Reporter A.03.50 or higher 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 5 MB	Free 5 MB or more disk space on the selected drive and continue installing the OpenView Reporter Data Protector report package.

A

All Hosts Backup Statistics report, 39
Apache, 28

B

backup groups, setting up on Data Protector, 32

C

cell manager
  registering with OVR module, 60
cell manager settings, 35
Cell Request Server, 19
Client Host Backup report, 40
ConfigSpec.xml, editing, 32
CRS, 19
custom reports, 63
customer models, 36
  importing, 37
customizing
  Data Protector-SIP integration, 32
  reports module, 44

D

Data List Trees report, 44
Data Protector, 14, 18, 19
  error messages, 47
  integration for OVO/UNIX, 52, 53
  reports, 43
  versions, 24, 55
Data Protector Integration module, 19
Data Protector-OVO integration, 14
  message groups, 66
  message parameters, 67
  messages, 63
Data Protector-OVR integration, 15, 54, 57
  configuring transaction reports manually, 59
  installing, 58
  supported platforms, 56
  troubleshooting, 69
Data Protector-SIP
  backup groups, 32
  cell manager settings, 35
  ConfigSpec.xml, editing, 32
  customizing, 32
  filter level, 33
  gauge settings, 34
  logging, 33
  refresh rate, 33
Data Protector-SIP integration, 15
  customer models, 36
  deployments, 22
  installing, 24
  installing on a Solaris SIP server, 27
  installing on a Solaris web server, 30
  installing on a web server, 28
  installing on a Windows SIP server, 26
  installing on a Windows web server, 28
  installing on an HP-UX SIP server, 26
  installing on an HP-UX web server, 29
  installing on the Data Protector server, 25
  management data filter, 37
  portal view services, 38
  portal views, 36
  protection status gauges, 39
  protection status module, 39
  troubleshooting, 50

E

editing reports module, 44
error messages, 50
  module, 47

F

filter level, 33

G

gauge settings, 34
gauges, protection status, 39

H

Hosts Statistics report, 41

I

IIS, 28
installing Data Protector-OVR integration, 58
installing Data Protector-SIP integration, 24
  on a Solaris SIP server, 27
  on a Solaris web server, 30
  on a web server, 28
  on a Windows SIP server, 26
  on a Windows web server, 28
  on an HP-UX SIP server, 26
  on an HP-UX web server, 29
  on the Data Protector server, 25

Index

integration with SIP, 19

J

Java Developer's Kit, 25, 55

L

logging, 33

M

management data filter, 37
message
  format, 66
  groups, 66
  parameters, 67
  tables, 64

N

Netscape Navigator, 25, 55

O

Object Last Backup report, 44
OpenView Operations *see* OVO
OpenView Reporter *see* OVR
OpenView Service Information Portal *see* SIP
Oracle, 52, 55
OVO, 52, 53
  Agent versions, 55
  database versions, 55
  message tables, 64
  versions, 55
OVR, 14, 52, 53
  gathering data from Data Protector, 62
  registering a DP cell manager, 60
  using with Data Protector, 60
  versions, 56

P

planning Data Protector-SIP integration, 22
portal view services, 38
portal views, 36
PortalView.xml, editing, 45
protection status
  gauges, 39
  module, 39, 42
protection status criteria, 42

R

refresh rate, 33
Reporter *see* OVR
reports, 43
  All Hosts Backup Statistics, 39
  Client Host Backup, 40
  configuring manually, 59
  custom, 55, 63
  customizing reports module, 44
  Data List Trees, 44
  global settings, 45
  Host Statistics, 41
  module, 43
  Object Last Backup Up, 44
requirements, 24

S

Service Level Management, 18
SIP, 14, 18
  versions, 24
SLM, 15, 18
software requirements, 24
status gauges, 19

T

TOMCAT, 28
troubleshooting
  Data Protector-OVR integration, 69
  Data Protector-SIP integration, 50
  registering a DP cell manager with OVR, 60