HP Data Protector
Integration with Autonomy LiveVault

Introducing cloud backup for HP Data Protector environments

Technical white paper

Table of contents

Summary

This technical white paper describes the integration of HP Data Protector (**Data Protector**) with Autonomy LiveVault® (**LiveVault**), which introduces cloud backup for enterprise environments where Data Protector is used as the data protection application. The white paper includes information which, together with information in the Data Protector end-user documentation and the LiveVault end-user documentation, guides you through all usage aspects of the Data Protector LiveVault integration (**integration**): installation and configuration, backup policy management, cloud backup, restore of data from the LiveVault cloud to a system in the Data Protector cell using the integration (cloud restore), and troubleshooting. Where needed, cross-references point to Data Protector and LiveVault documentation items. The white paper ends with a glossary, which explains some of the frequently used terms, and references to relevant resources on the web.

Introduction

The Data Protector LiveVault integration offers an additional level of protection for data stored on systems in the Data Protector cell. Besides the on-premise backup solution that has been offered by Data Protector until recently, this integration together with the LiveVault service and the LiveVault cloud storage adds a back-up-to-the-cloud solution to Data Protector environments. Apart from other requirements, the main use case in which such a combined data protection solution can effectively address customers needs are disaster recovery scenarios. For higher backup and restore speeds, the LiveVault service offers TurboRestore Appliances which can be used with the integration as well.

Integration concepts

When using this integration, cloud backup and cloud restore sessions are driven exclusively by LiveVault. Data Protector is used for initial configuration of the integration and for management of LiveVault **backup policies**, LiveVault's counterparts of Data Protector backup specifications. Backup policies can coexist with the latter, thus providing extra protection for the already protected systems.

Cloud backup (and consequently cloud restore) must be enabled for each system in the Data Protector cell separately. Once the Data Protector Disk Agent and the LiveVault Agent are installed on it, such a system becomes a **source client**. Backup policies can only protect source clients.

Licensing

For data which you are going to back up using this integration, licensing must be covered for both products: you need to purchase appropriate Data Protector and LiveVault licenses. For details on the licensing models, see the following:

- *HP Data Protector Installation and Licensing Guide*
- *LiveVault Quick Start Guide* and other resources on the LiveVault website (see Call to action)

Limitations and considerations

Limitations

The integration has the following limitations:

- The functionality supporting the integration is not available in the Data Protector Java GUI.
- The only supported Data Protector backup object type is *filesystem*.
- When creating or reconfiguring a backup policy in the Data Protector user interface, the two basic policy properties that can be configured are:
  - Which volumes, folders, and files are backed up
  - Whether the policy should be made active or not

  Other backup policy options, including the backup schedule and the retention period of the backed up data, are assigned automatically by the LiveVault subscription to which you subscribe. For more information, see the *LiveVault Web Management Portal Help*.
- When creating a backup policy in the Data Protector user interface, you cannot define filesystem object exclusions: subfolders of an already selected folder or files contained in it cannot be excluded from cloud backup. This constraint is imposed by the current design of the Data Protector-LiveVault communication protocol.
- LiveVault omits specific filesystem objects from being backed up. As a rule, these objects do not contain viable user data.

CAUTION:
Although the Data Protector user interface enables you to select such objects, and, when selected, they appear included in the Data Protector backup specification, they are skipped by the LiveVault backup process.

This is due to inability of Data Protector to present LiveVault automatic backup exclusions in its graphical user interface. The constraint is imposed by the current design of the Data Protector-LiveVault communication protocol.

For a list of the objects that are not backed up by LiveVault, see the following *LiveVault Web Management Portal Help* topics:

- *Objects that Cannot Be Backed Up*
- *Automatic and Recommended Backup Exclusions*

- Instead of protecting the same data with multiple backup policies, LiveVault uses other means of assuring safety of the protected data. It does not allow the same filesystem object to be covered by more than one backup policy. For example, the following two paths cannot be specified in two backup policies for the same source client, in this order:

  ```
  C:\Folder\Subfolder
  C:\Folder
  ```

  The second policy contains a path that includes all filesystem objects covered by a path defined in the first, already existing policy.

  For this reason, Data Protector disallows creating backup policies that overlap in this sense. An error is reported in the Data Protector GUI while attempting to save a policy which includes rules that overlap with the ones defined in an already existing policy.

  To configure multiple backup policies for the same source client, it is recommended to use paths that differ either in the drive letter or in the folder as close to the volume root as possible, for example:

  ```
  C:\Folder1
  ```

`C:\Folder2`

For detailed information on the LiveVault backup policy rules interpretation, see the following *LiveVault Web Management Portal Help* topics:

- *Interpreting File Selection Rules*
- *Understanding File Selection Rules*

- Volumes which are mounted to a mount point folder and which have no drive letter assigned cannot be backed up using this integration. To include such a volume in cloud backups, assign it to a drive letter and select the drive letter as the filesystem objects when creating or updating the corresponding backup policy.

Considerations

Consider the following when planning your integration-related activities:

- In Data Protector Manager-of-Managers environments, the integration must be separately configured in each Data Protector cell where cloud backup is required.
- The only supported Data Protector backup type is *incremental* backup (Incr).

  This constraint is imposed by the architectural design of LiveVault. For more information about the Data Protector backup types, see the *HP Data Protector Help*.
- Each backup policy can be configured to back up data from a single system only.

  This constraint is also imposed by the architectural design of LiveVault.
- For performance reasons, the total amount of data backed up using a single backup policy should not exceed 1 TB. If the size of your cloud backup requirement on a particular system exceeds this amount, use multiple backup policies to back the data up.
- Backup policies that you create from the Data Protector graphical user interface (GUI) cannot be further managed from the LiveVault Web Management Portal, but only by Data Protector.

  This means the only two aspects that you can change on a backup policy level, after the policy is created, are the list of filesystem objects that are backed up and the policy state (active, inactive). Other policy options are enforced by LiveVault.

Installing the integration

Operating system requirements

The integration supports the following operating systems on the source client:

- Windows Server 2008 R2 (64-bit):
  - Full installation
  - Server Core installation
- Windows Server 2008 – x64 (64-bit):
  - Full installation
  - Server Core installation
- Windows Server 2008 – x86 (32-bit)
  - Full installation
  - Server Core installation
- Windows Server 2003 – x64 (64-bit)

- Windows Server 2003 – x86 (32-bit)

For operating system requirements for systems with other roles in the Data Protector cell, see the *HP Data Protector Platform and Integration Support Matrix*.

Required applications

The following application software versions are required by the integration:

- HP Data Protector 7.00
- Autonomy LiveVault 7.52

Prerequisites for installation

The following are prerequisites for installation of the integration:

- A Data Protector cell is correctly set up for backup and restore purposes, with the Data Protector Cell Manager and the Installation Server installed on the appropriate systems.

  For more information, see the *HP Data Protector Concepts Guide*, the *HP Data Protector Installation and Licensing Guide*, and the *HP Data Protector Help*.
- On each system which is to become a source client, the following is installed and configured appropriately:
  - LiveVault Agent

    To be able to install the agent, a computer subscription must already exist in LiveVault.

    For installation and configuration instructions, see the *LiveVault Agent Distribution Guide*, the *LiveVault Environment Configuration Guide*, and the *LiveVault Quick Start Guide*.
- On an arbitrary system in the Data Protector cell, the following is installed:
  - Data Protector User Interface

    This component is mandatory. It includes the Data Protector graphical user interface (GUI).

    For installation instructions, see the *HP Data Protector Concepts Guide* and the *HP Data Protector Installation and Licensing Guide*.
  - Data Protector English Documentation (Guides, Help)

    This component is optional. It must be installed on the same system as the User Interface component if you want to access the context-sensitive Help that explains integration specifics in the Data Protector GUI.

Installation procedure

On each system which is to become a source client, install the Data Protector Disk Agent component locally or remotely. For installation instructions, see the *HP Data Protector Installation and Licensing Guide* and the *HP Data Protector Help*.

Configuring the integration

Before you can start creating backup policies, you need to configure the integration. Assumption and a prerequisite at this point is that a partner and a customer are already registered in LiveVault environment, and that a custom LiveVault Web Service address is already assigned. For a guidance on these actions, see the *LiveVault Environment Configuration Guide*.

The configuration process involves creation of identification strings, which needs to be done in LiveVault, and their provisioning to Data Protector. The strings are used for inter-process communication between Data Protector and LiveVault. LiveVault-specific steps must be followed first, with the Data Protector-related ones following afterwards.

Configuring the LiveVault side

To configure the integration on the LiveVault side, you need to create the two identification strings. They are the Access Id and the Secret Key; both form the LiveVault API Key. Once crated, write them down as you will need them for configuration of the Data Protector side.

You have to perform this action in the LiveVault Web Management Portal. For instructions, see the *LiveVault Technical Notes: LiveVault-Data Protector Integration*.

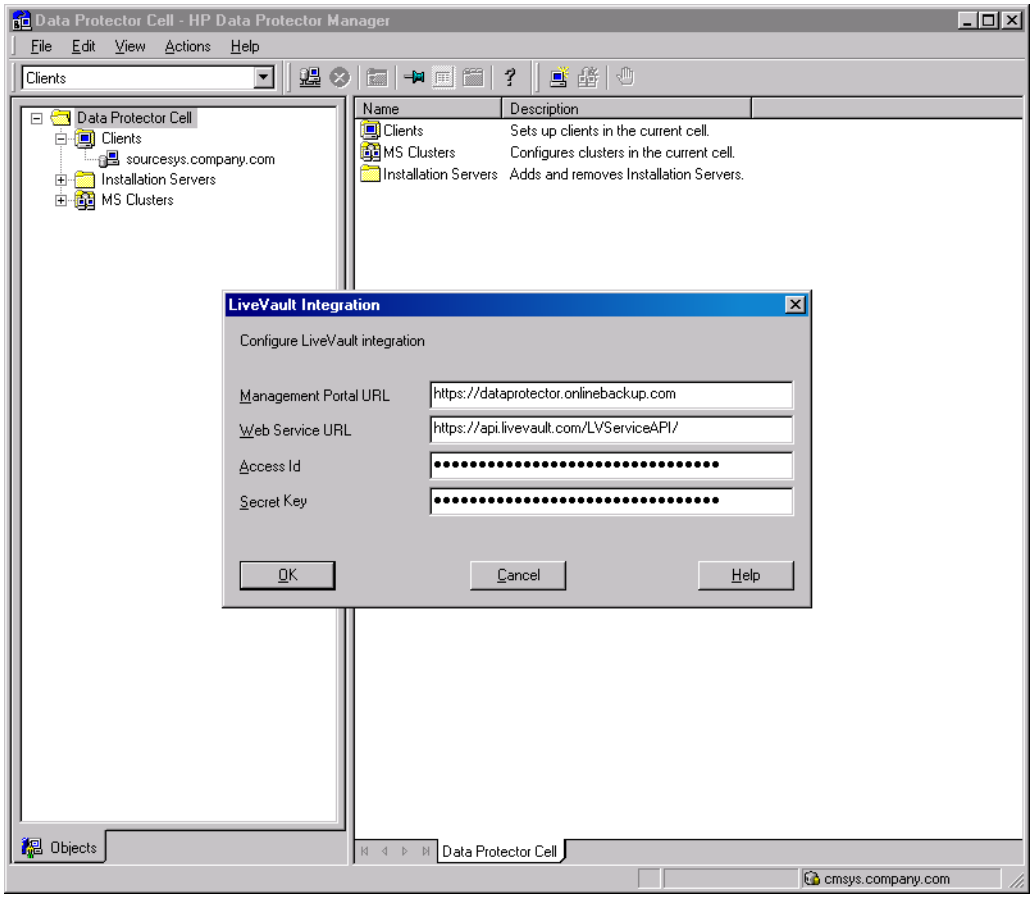
Configuring the Data Protector side

To successfully configure the integration on the Data Protector side, you need web addresses of the LiveVault Web Management Portal and the LiveVault Web Service, and the two identification strings acquired during the LiveVault configuration.

Follow the steps:

1. Launch the Data Protector graphical user interface.
2. In the Context List, click **Clients**.
3. In the Scoping Pane, expand **Data Protector Cell** and then right-click **Clients**.
4. From the context menu, select **Configure LiveVault Integration**.

Figure 1: Configuring the integration on the Data Protector side



5. In the LiveVault Integration dialog box, specify the option values as follows:

   Management Portal URL: The web address of the LiveVault Web Management Portal. The Data Protector GUI uses this address to open the portal in the embedded web browser pane when LiveVault Restore is selected in the Restore context.

   Web Service URL: The web address of the LiveVault Web Service. This address is used for inter-process communication between Data Protector and LiveVault.

   Access Id and **Secret Key**: Customer-specific alphanumeric strings that you acquire during the integration configuration procedure from the LiveVault Web Management Portal. They are used for inter-process communication between Data Protector and LiveVault. In the Data Protector GUI, they are hidden by bullet characters. Ensure that the secret key does not get disclosed by accident.

6. Click **OK** to save your changes and close the dialog box.
7. If the Data Protector Cell Manager uses a web proxy server for Internet access, perform the following in addition:
   a. On the Cell Manager system, add a *system* environment variable `all_proxy` with the following value (replace placeholders with actual values, square brackets denote optional parts):

      `[<Protocol>://][<Username>:<Password>@]<SystemName>[:<PortNumber>]`

b. On the same system, restart the Data Protector processes by invoking the following commands in sequence:

```
omnisv –stop
omnisv -start
```

IMPORTANT:
The Access Id and Secret Key values are encrypted using the Data Protector's certificate for encrypted control communication for increased security. If the certificate is changed, the integration must be reconfigured on the Data Protector side in order to function properly.

Managing LiveVault backup policies

This section explains how LiveVault backup policies are created, modified, and deleted from the Data Protector graphical user interface (GUI).

NOTE:
Cloud backups in the Data Protector cell run according to the backup policies configured in LiveVault. However, Data Protector also stores local Data Protector backup specifications (backup policy counterparts) to its Internal Database (IDB) when backup policies are created or modified. These backup specifications are only used as a base for subsequent backup policy management in the Data Protector GUI, and do not directly influence the cloud backup process and schedule.

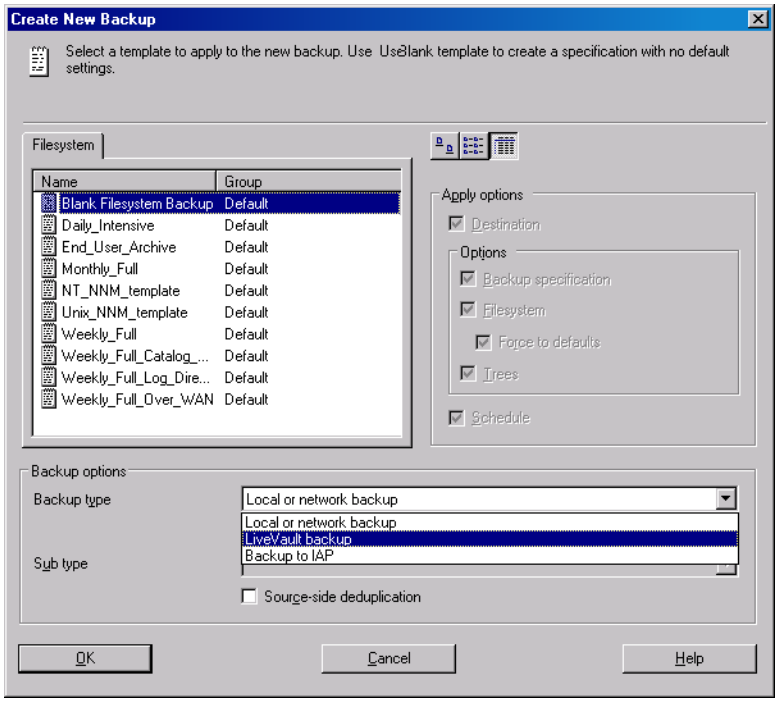
Before managing your backup policies, consider topics discussed in Limitations and Considerations.

Creating backup policies

To create a backup policy, perform the steps:

1. Launch the Data Protector graphical user interface.
2. In the Context List, click **Backup**.
3. In the Scoping Pane, expand **Backup** and **Backup Specifications**.
4. Right-click **Filesystem** and select **Add Backup** from the context menu. The Create New Backup dialog box appears.

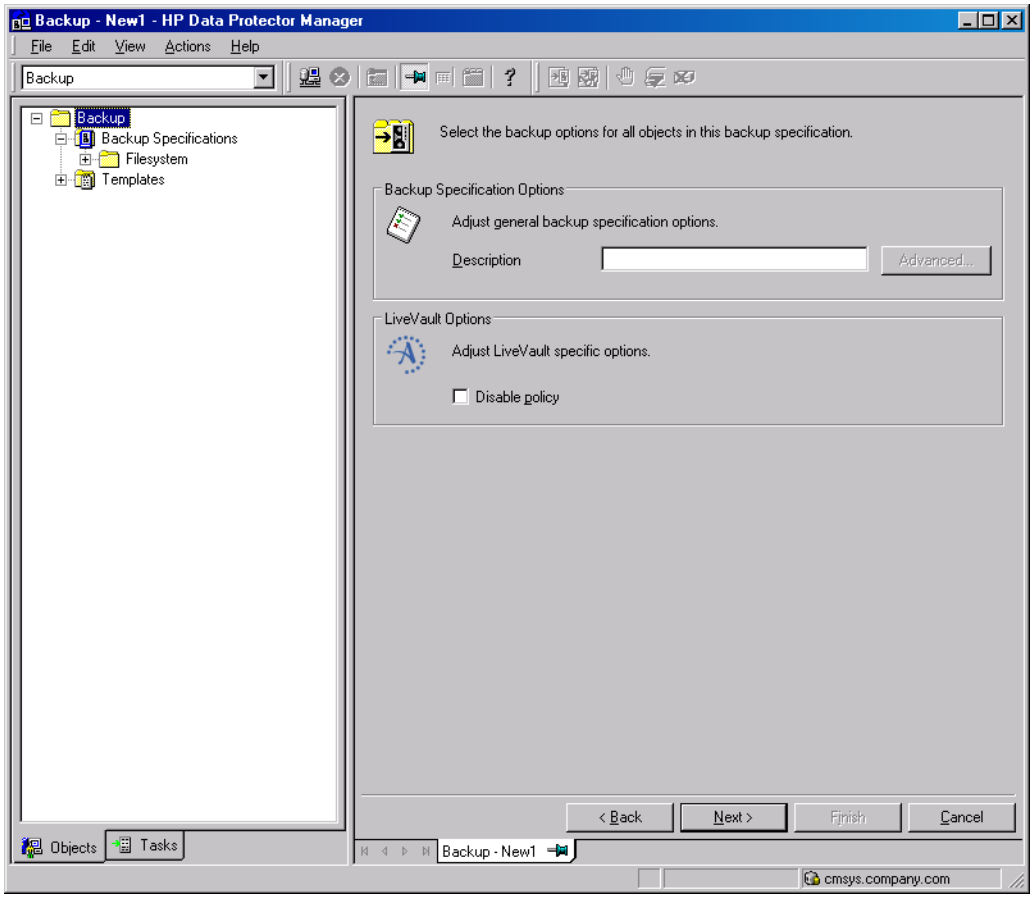
Figure 2: Creating a new backup policy in the Data Protector GUI



5. From the drop-down menu Backup type, select **LiveVault backup**.
6. Click **OK** to confirm the selection and close the dialog box.

   In the Results Pane, fully qualified domain names of the source clients are displayed.
7. Expand the fully qualified domain name of the desired source client, and select the volumes, folders, or files which you want to back up. Click **Next**.

Figure 3: Specifying the backup policy options



8. Under Backup Specification Options, in the **Description** field, enter an arbitrary description.

   The description will not be used in LiveVault, but will only be saved to the Data Protector Internal Database (IDB).

9. Under LiveVault Options, select the **Disable policy** option if needed.

   If selected, this option causes the backup policy to be inactive in LiveVault and prevents triggering cloud backups based on it. You can activate it later when modifying the policy from the Data Protector GUI.

10. Click **Next** and then **Save as**.

11. In the dialog box Save Backup As, in the Name text box, enter a backup policy name and click **OK**.

    In LiveVault, the backup policy is created and saved with the specified name.

Modifying backup policies

Similarly as when creating backup policies, the only two backup policy aspects that can be reconfigured are the list of volumes, folders, and files that are backed up, and the policy status (disabled or enabled).

To create a backup policy, perform the steps:

1. Launch the Data Protector graphical user interface.
2. In the Context List, click **Backup**.
3. In the Scoping Pane, expand **Backup**, **Backup Specifications**, and finally **Filesystem**.
4. Right-click the chosen backup policy and select **Properties** from the context menu.
5. In the Results Pane, expand the fully qualified domain name of the source client, and revise the filesystem object selection.

   Click the **Options** tab.
6. Revise the **Description** and **Disable policy** options.
7. Click **Apply**.

   In LiveVault, the backup policy is updated accordingly.

Deleting backup policies

In the Data Protector GUI, when you delete a backup policy, two things happen:

- The corresponding Data Protector backup specification is removed from the Data Protector Internal Database (IDB).
- In LiveVault, the backup policy is scheduled for deletion. It remains configured for restore purposes until the retention period for the covered data expires. Only at that moment the policy is actually automatically deleted.

To delete a backup policy, perform the steps:

1. Launch the Data Protector graphical user interface.
2. In the Context List, click **Backup**.
3. In the Scoping Pane, expand **Backup**, **Backup Specifications**, and finally **Filesystem**.
4. Right-click the chosen backup policy and select **Delete** from the context menu.
5. In the dialog box, confirm the deletion by clicking **Yes**.

Restoring data from the LiveVault cloud

Restore of the backed up data is preformed through the LiveVault agent that is installed on the source client, without Data Protector involvement. For more information, see the following *LiveVault Web Management Portal Help* topics:

- *Restoring Your Data: An Overview*
- *Restoring a standard policy*

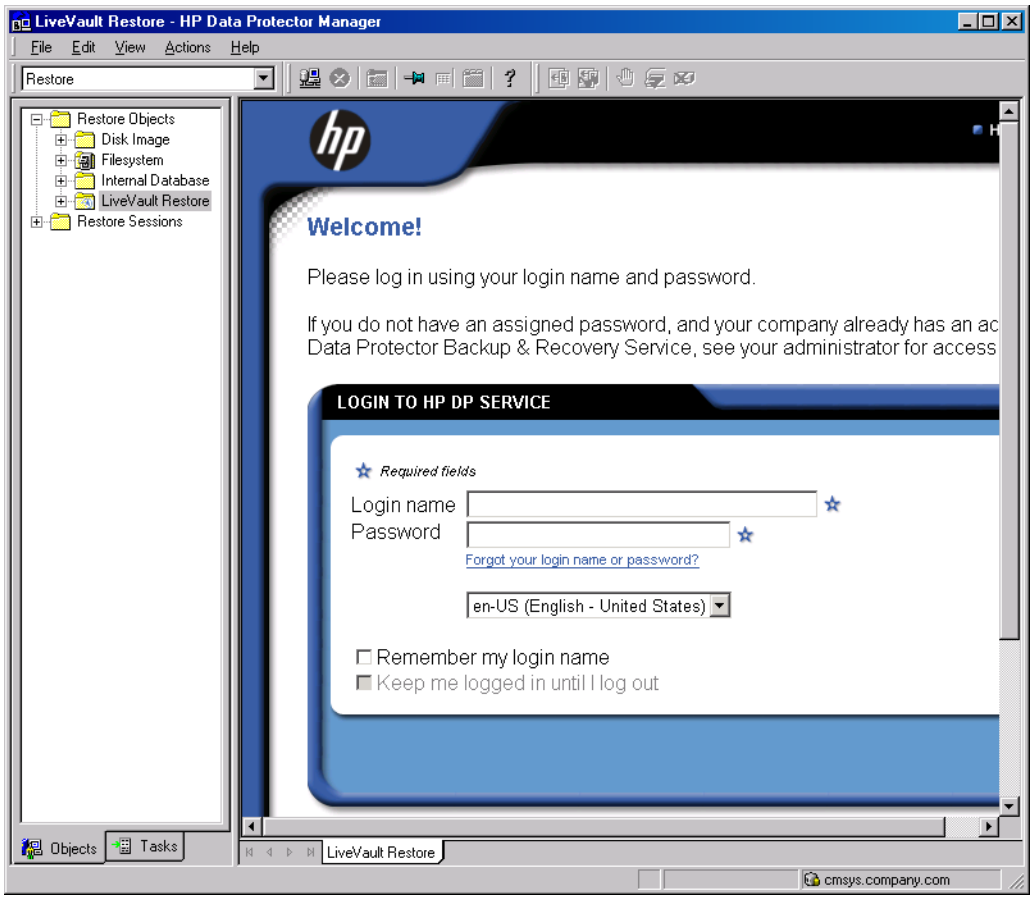
You can trigger cloud restore as well as define the restore scope and select other restore options in the Restore Wizard of the LiveVault Web Management Portal. You can access the portal from an arbitrary system using a supported web browser, or you can use the Data Protector GUI for this purpose. Restore context of the Data Protector GUI embeds a web browser pane and provides the same level of user experience. It uses the web address specified for the integration configuration option Management Portal URL to display the portal.

To access the LiveVault Web Management Portal from the Data Protector GUI, proceed as follows:

1. Launch the Data Protector graphical user interface.

2. In the Context List, click **Restore**.
3. In the Scoping Pane, expand **Restore Objects** and then select **LiveVault Restore**.
   The LiveVault Web Management Portal displays in the Results Area.

Figure 4: Accessing the LiveVault Web Management Portal from the Data Protector GUI



Troubleshooting

This section provides problem-solving information when using the Data Protector LiveVault integration.

For general Data Protector troubleshooting information, such as log and event reporting, warnings, and diagnostics, see the *HP Data Protector Troubleshooting Guide* or the *HP Data Protector Help*. For the LiveVault troubleshooting information, see the *LiveVault Web Management Portal Help*.

Before you begin

Before you start determining the root cause of your problem:

- Ensure that the latest official patch bundles or patches for your Data Protector version are installed. On how to verify this, see the *HP Data Protector Help* index: "patches".

- Get familiar with general Data Protector limitations as well as recognized issues and workarounds. For more information, see the *HP Data Protector Product Announcements, Software Notes, and References*.

Glossary

The following table explains some of the terms used in this document.

Term or acronym	**Description**
backup policy	A policy in the LiveVault environment that defines which, how, and when the data is backed up to the LiveVault cloud.
cloud backup	A backup process during which data is backed up from a system in the Data Protector cell to the LiveVault cloud using the Data Protector LiveVault integration.
source client	A system in the Data Protector cell which stores original data that is backed up to the LiveVault cloud. The Data Protector Disk Agent and the LiveVault Agent are installed on it.

For more information

Visit the following HP Data Protector online resources to get more information:

www.hp.com/go/dataprotector

www.hp.com/go/imhub

www.hp.com/go/software

Call to action

To read more about HP Data Protector, visit www.hp.com/go/dataprotector.

To read more about Autonomy LiveVault, visit http://backup.autonomy.com/connectedbackup/products/alv.page?.

4AA4-0282ENA, Created March 2012