Hewlett Packard Enterprise

HPE Data Protector Integration with Autonomy LiveVault

Introducing cloud backup for HPE Data Protector Environments

Table of contents

Summary

This technical white paper describes the integration of HPE Data Protector (**Data Protector**) with Autonomy LiveVault® (**LiveVault**). This integration introduces the concept of cloud backup for enterprise environments where Data Protector is used as the data protection application. The white paper includes information that, when examined together with Data Protector and LiveVault user documentation, guides you through all the user scenarios from a 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 appropriate, you will find cross-references to Data Protector and LiveVault documentation topics. The white paper concludes with a glossary, which explains some of the frequently used terms, and also provides 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. In addition to the on-premise backup solution that Data Protector provides, the Data Protector LiveVault integration, when used together with the LiveVault service and the LiveVault cloud storage, adds a backup-to-cloud solution to Data Protector environments. Among the many requirements and use cases, the primary scenarios in which the integrated data protection solution most effectively addresses customer needs are in the area of disaster recovery. For faster backup and restore speeds, the LiveVault service offers TurboRestore Appliances, which can be used with the integration as well.

Integration concepts

When using a Data Protector LiveVault 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**, which are LiveVault counterparts to Data Protector backup specifications. Backup policies can coexist with backup specifications, thus providing extra protection for already-protected systems.

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

Licensing

If using the Data Protector LiveVault integration for creation of backup images, you must have a license for both products: Data Protector and LiveVault. For details on the licensing models, see the following:

- *HPE 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 Data Protector LiveVault integration has the following limitations:

- The only supported Data Protector backup object type is *filesystem*.
- When creating or reconfiguring a backup policy in Data Protector, the two basic policy properties you can configure are:
  - Which volumes, folders, and files are backed up
  - Whether or not the policy should be made active

  Other backup policy options, including backup schedules and retention periods, are assigned automatically by the LiveVault subscription. For more information, see the *LiveVault Web Management Portal Help*.
- When creating a backup policy in Data Protector, you cannot define filesystem object exclusions: subfolders of an already-selected folder or files contained in a subfolder cannot be excluded from cloud backup.
- LiveVault omits specific filesystem objects from being backed up. These objects do not contain essential user data.

CAUTION: Although Data Protector enables you to such filesystem objects, and, when selected, they appear to be included in the Data Protector backup specification, they are not included in the LiveVault backup process.

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*

- LiveVault does not allow for the application of multiple backup policies to the same filesystem object data. 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. This is why Data Protector does not allow multiple backup policies to apply to the same filesystem object.

  To configure multiple backup policies for the same source client, you should use paths that differ (either in the drive letter or in a folder as close to the volume root as possible). For example:

  `C:\Folder1`

  `C:\Folder2`

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

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

- Volumes that are mounted to a mount point folder and have no assigned drive letter 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 object 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).
- For more information about the Data Protector backup types, see the *HPE Data Protector Help*.
- Each backup policy can be configured to back up data from a single system only.
- For performance reasons, the total amount of backup data created using a single backup policy should not exceed 1 TB. If the size of your cloud backup requirement on a particular system exceeds 1 TB, use multiple backup policies for backing up the data.
- Backup policies that you create from the Data Protector graphical user interface (GUI) can only be managed using Data Protector; backup policies created within Data Protector cannot be managed from the LiveVault Web Management Portal.

  The only two items you can change on a backup policy level after the backup policy has been created are the:

  - List of filesystem objects that are backed up
  - 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 *HPE Data Protector Platform and Integration Support Matrix*.

Required applications

The following application software versions are required by the integration:

- HPE Data Protector 8.00
- HPE Data Protector 8.10
- Autonomy LiveVault 7.52

Prerequisites for installation

The following are prerequisites for installation of the integration:

- A Data Protector cell must be 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 *HPE Data Protector Concepts Guide*, the *HPE Data Protector Installation and Licensing Guide*, and the *HPE Data Protector Help*.
- On each system that is to become a source client, the following must be installed and configured appropriately:
  - LiveVault Agent

    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 must be installed:
  - Data Protector User Interface

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

    For installation instructions, see the *HPE Data Protector Concepts Guide* and the *HPE 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 that is to become a source client, install the Data Protector Disk Agent component locally or remotely. For installation instructions, see the *HPE Data Protector Installation and Licensing Guide* and the *HPE Data Protector Help*.

Configuring the integration

Before creating backup policies, you need to configure the integration. An assumption here (which is also a prerequisite) is that a partner and a customer are already defined and registered in LiveVault, and that a custom LiveVault Web Service address has already been assigned. For additional information about these actions, see the *LiveVault Environment Configuration Guide*.

The configuration process involves the creation of identification strings, which are used for inter-process communications between Data Protector and LiveVault. You must perform the configuration process from within LiveVault first, and then within Data Protector.

Configuring LiveVault

To configure the LiveVault side of the integration, you must create two identification strings: Access Id and Secret Key. These strings form the LiveVault API Key. After creating these required strings, write the information down, as you will need it for the Data Protector side of the configuration as well.

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

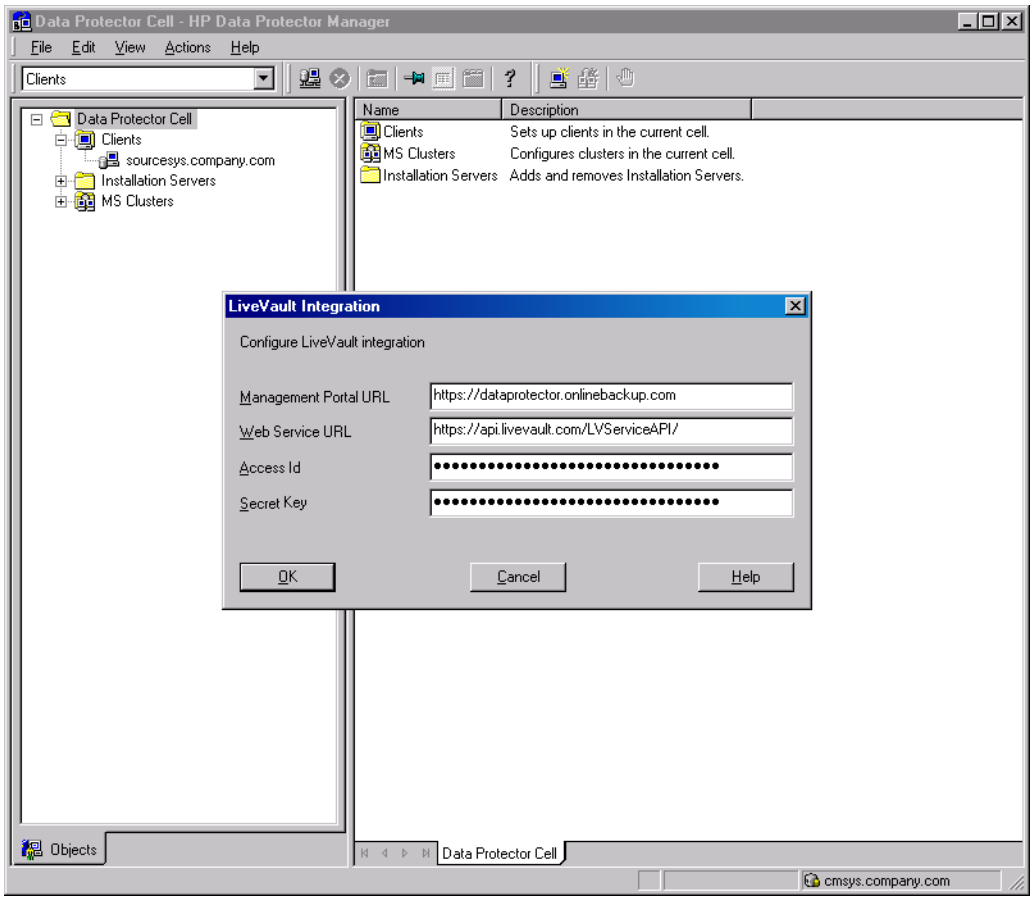
Configuring Data Protector

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

To configure Data Protector for the integration:

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 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 define 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 is not 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:

a. On the Cell Manager system, add a *system* environment variable `all_proxy` with the following values (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 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 to create, modify, and delete LiveVault backup policies 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) in 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.

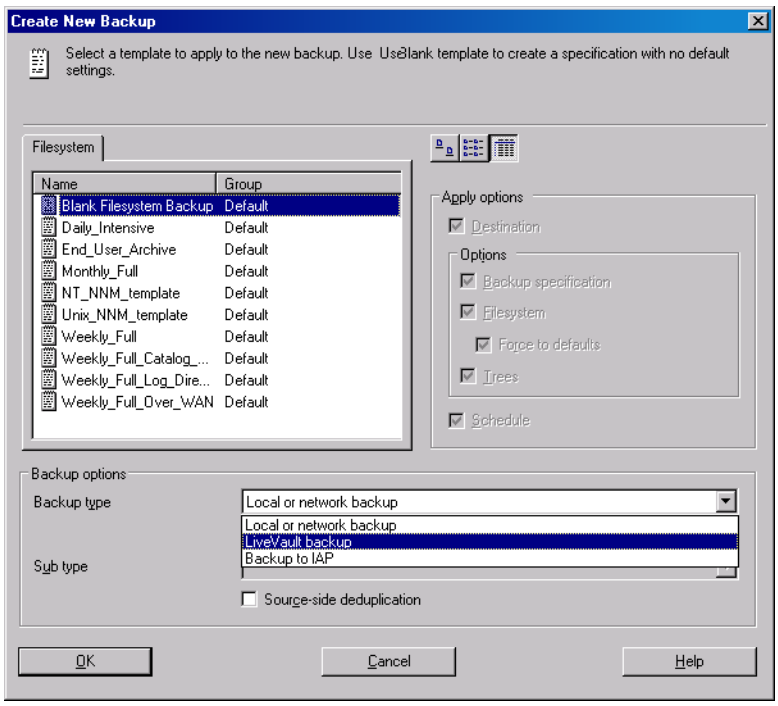
Before managing your backup policies, review the topics discussed in Limitations and Considerations.

Creating backup policies

To create a backup policy:

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.

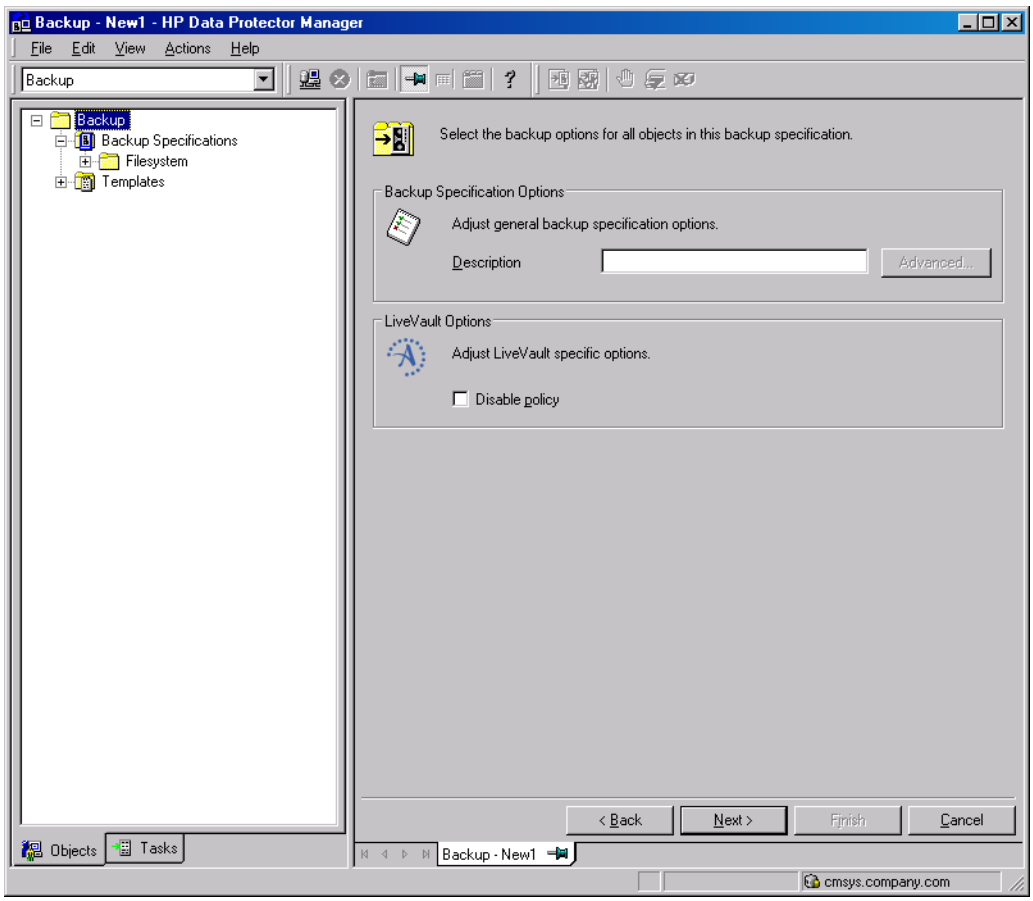
Figure 2: Creating a new backup policy in the Data Protector GUI



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 that you want to back up. Click **Next**.

Figure 3: Specifying the backup policy options



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

   The description will not be used in LiveVault; rather, it will be saved in the Data Protector Internal Database (IDB).
9. Under LiveVault Options, select the **Disable policy** option if needed.

   When selected, this option ensures that the backup policy will be inactive in LiveVault and prevents triggering cloud backups based upon it. You can also activate it later when modifying the policy from the Data Protector GUI.
10. Click **Next** and then **Save as**.
11. Enter a backup policy name in the Name text box of the dialog box and click **OK**.
12. In LiveVault, the backup policy is created and saved with the specified name.

Modifying backup policies

The only two aspects of the backup policy that you can modify are the list of volumes, folders, and files that are backed up, and the policy status (disabled or enabled).

To modify a backup policy:

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 then **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**.

   The backup policy is updated accordingly within LiveVault.

Deleting backup policies

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

- 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 is the policy actually deleted.

To delete a backup policy:

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 then **Filesystem**.
4. Right-click the chosen backup policy and select **Delete** from the context menu.
5. In the dialog box, click **Yes** to confirm the deletion.

Restoring data from the LiveVault cloud

Restores of backed up data are performed using the LiveVault agent installed on the source client, with no Data Protector involvement. For more information, see the following *LiveVault Web Management Portal Help* topics:

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

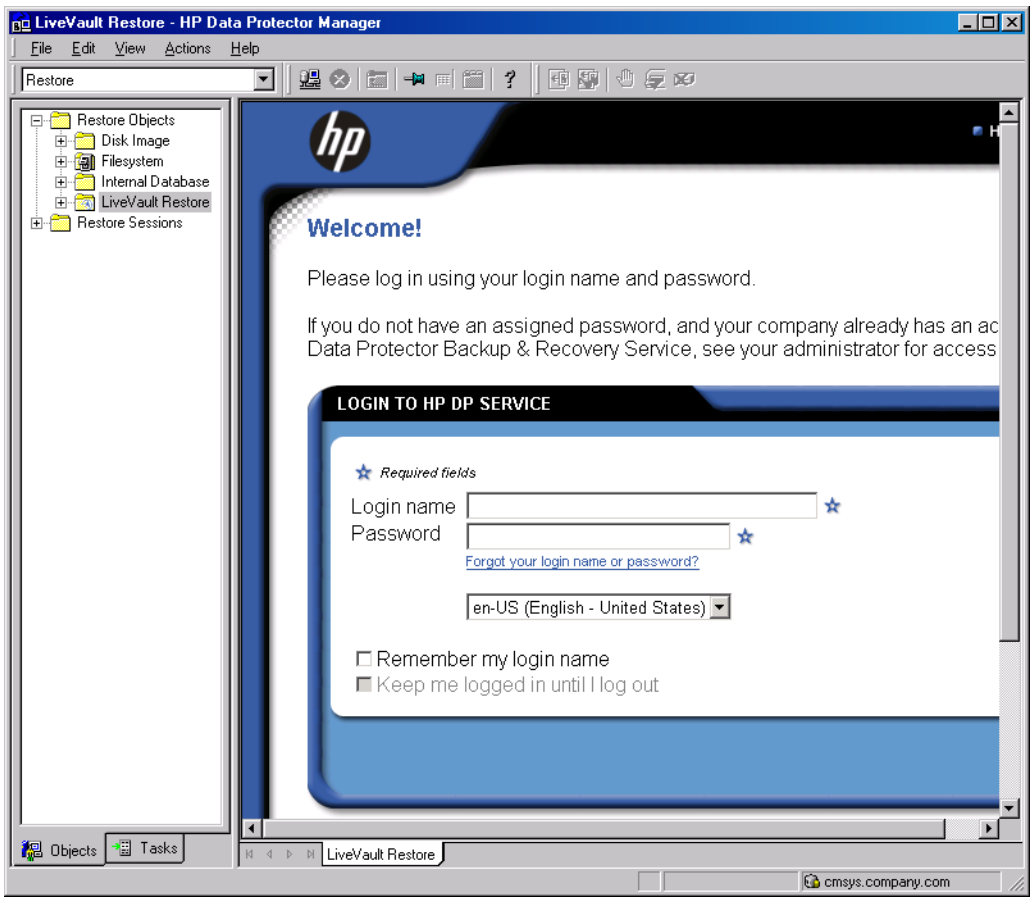
You can trigger a cloud restore as well as define the restore scope and select other restore options in the Restore Wizard of the LiveVault Web Management Portal. You can access the portal from a system using a supported web browser, or you can use the Data Protector GUI. The Restore context of the Data 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:

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 for the Data Protector LiveVault integration.

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

Before you begin

Before you start working to identify the root cause of your problem:

- Ensure that the latest official patch bundles or patches for your Data Protector version are installed. To check what is installed, see the *HPE Data Protector Help* index: "patches".
- Familiarize yourself with general Data Protector limitations as well as recognized issues and workarounds. For more information, see the *HPE 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 what, 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 that stores original data that is backed up to the LiveVault cloud. The Data Protector Disk Agent and the LiveVault Agent are installed here.

For more information

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

http://www.hpe.com/software/dataprotector

www.hp.com/go/imhub

www.hp.com/go/software

Call to action

To read more about HPE Data Protector, visit http://www.hpe.com/software/dataprotector.

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

Get connected

hp.com/go/getconnected

Current HPE driver, support, and security alerts
delivered directly to your desktop

4AA4-0282ENA, Created June 2014

Hewlett Packard Enterprise