VAST + COHESITY

VAST DATA UNIVERSAL STORAGE WITH COHESITY DATAPROTECT

Configuration Guide

TABLE OF CONTENTS

REVISION HISTORY

Revision Number	Description	Date
1.0	Initial Release	April 2022

INTRODUCTION

VAST Data's Universal Storage redefines the economics of flash storage, making flash affordable for all applications, from the highest performance databases to the largest data archives, for the first time. The Universal Storage concept blends game-changing storage innovations to lower the acquisition cost of flash with an exabyte-scale file and object storage architecture breaking decades of storage tradeoffs.

With the advantage of new, enabling technologies that were not available before 2018, this new Universal Storage concept can achieve a previously impossible architecture design point. The system combines low-cost hyperscale flash Drives and Storage Class Memory with stateless, containerized storage services all connected over new low-latency NVMe over Fabrics networks to create VAST's Disaggregated Shared Everything (DASE) scale-out architecture. Next-generation global algorithms are applied to this DASE architecture to deliver new levels of storage efficiency, resilience, and scale.

Cohesity DataProtect is a high-performance, software-defined backup and recovery solution designed for the cloud era. Designed for hyperscale, it offers the most comprehensive policy-based protection for both traditional and modern data sources. DataProtect converges multiple-point products into a single software that can be deployed as on-premises or consumed as a service.

Both products offer unprecedented horizontal scale out without creating storage islands or requiring exorbitant upfront costs. With VAST Data, a customer can grow their data storage performance independent of their capacity needs and vice versa. With Cohesity DataProtect, backup capacity and performance can grow asynchronously with their storage needs allowing maximum flexibility in an organization's data center and budget.

SOLUTION OVERVIEW

This document will look at using a VAST Data Universal Storage cluster with Cohesity DataProtect in two different scenarios:

- **As a source** – Cohesity is backing up the data on the VAST system and
- **As a target** – VAST is used to backup data from another source

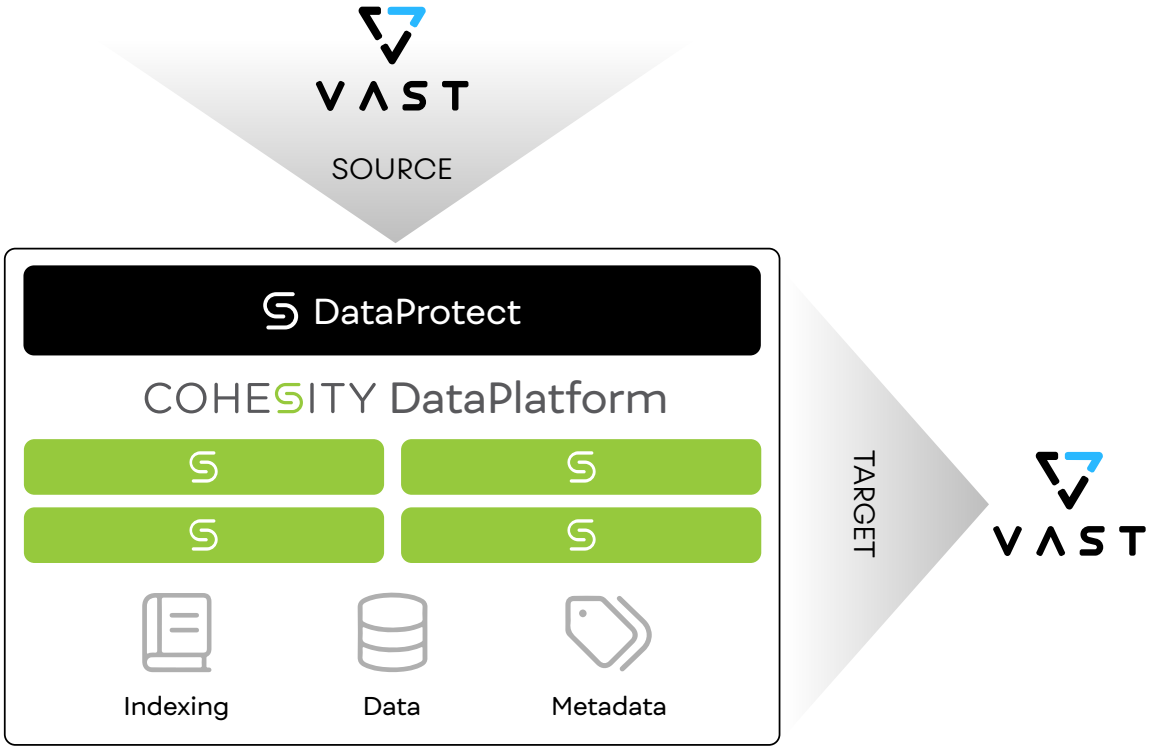

Figure 1 – Cohesity Integration with VAST

VAST AS A DATA SOURCE

Let's start by looking at the scenario where it is desired to back up data residing on a VAST cluster. There are several ways that Cohesity can communicate with third party storage. The two methods to communicate with the VAST cluster are as an NFS mount or an SMB share.

When a mount point is registered on the Cohesity system there is no granularity below that mount point for creating a backup policy. It will be a grab-all policy that will back up that entire directory, however, upon recovery or restore Cohesity DataProtect does allow for directory browsing.

Depending on how the data is organized within the VAST cluster, various sources (mount points) can be registered to allow for multiple backup policies based on differing backup frequencies and requirements. The following sections will highlight the connection method using NFS with the following workflow:

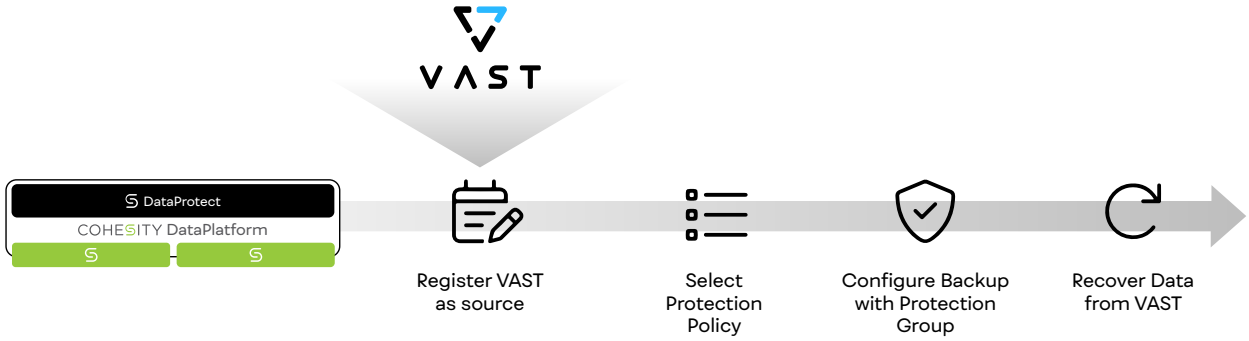

Figure 2 - Workflow for adding VAST Cluster as a source

REGISTER VAST AS COHESITY DATAPROTECT SOURCE

Following the steps in the next few figures shows how easy it is to register a mount point from the VAST cluster using NFS v3. On the Cohesity UI open the **Data Protection** menu on the left pane and select **Sources** (Figure 3).

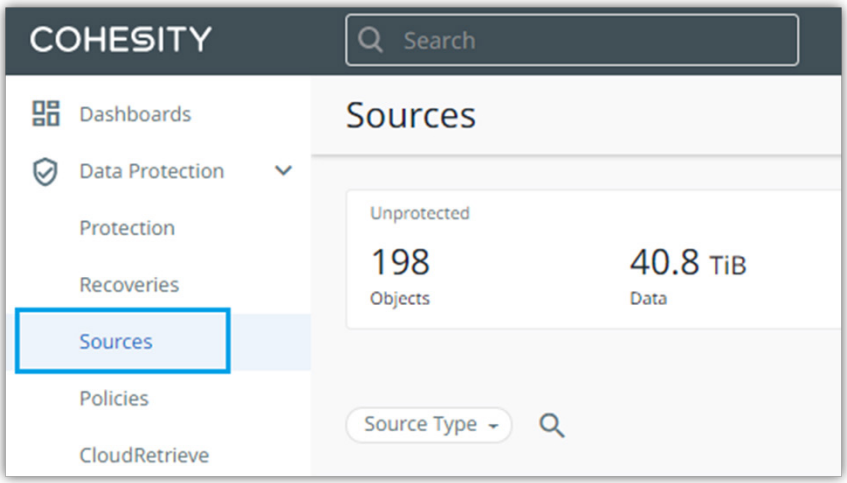

Figure 3 - Adding a VAST cluster mount point as a Source

On the Sources page click on the Register button in the upper right (Figure 4) and then select NAS in the menu list that appears.

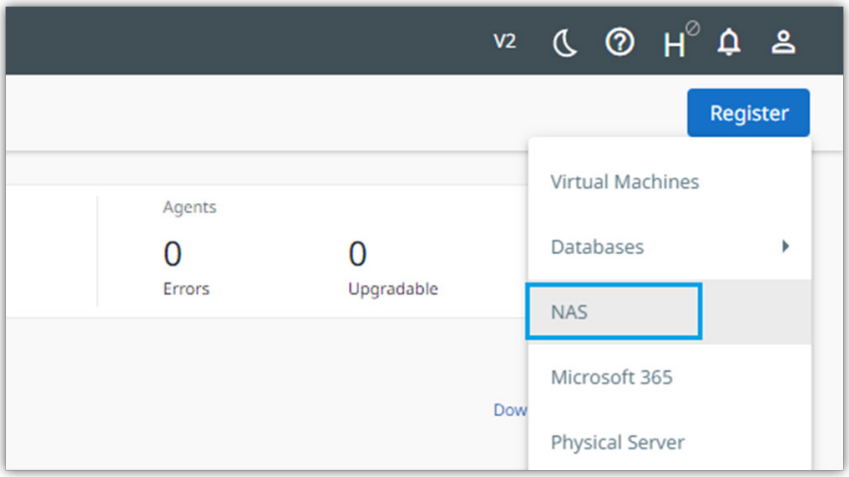

Figure 4 - Select NAS to enter VAST cluster mount point

On the **Register NAS** page (Figure 5) select **Mount Point** from the pull-down menu and then enter the fully qualified domain or IP address and mount point. Then click register.

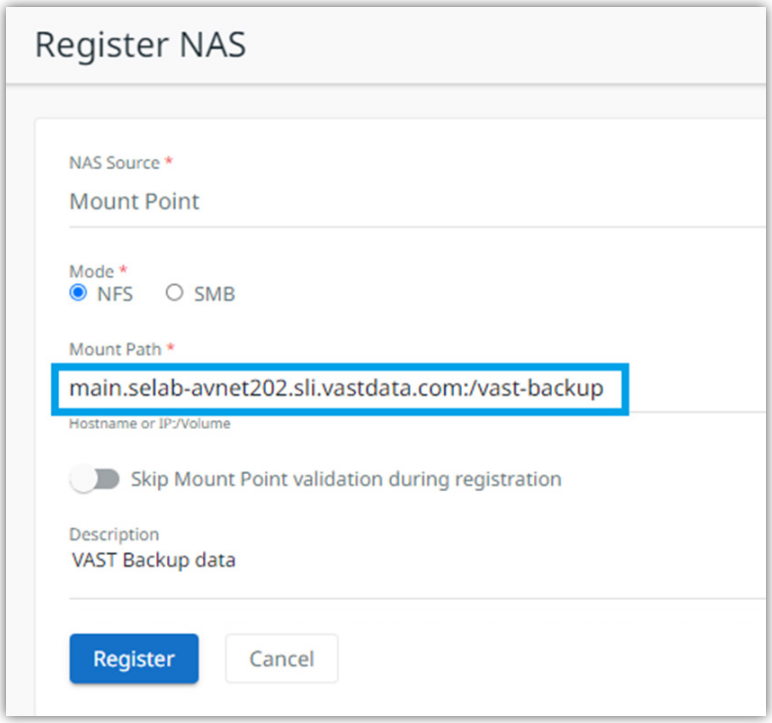

Figure 5 - Registering VAST cluster mount point

When the mount point has been registered it will appear in the Sources page as shown in Figure 6.

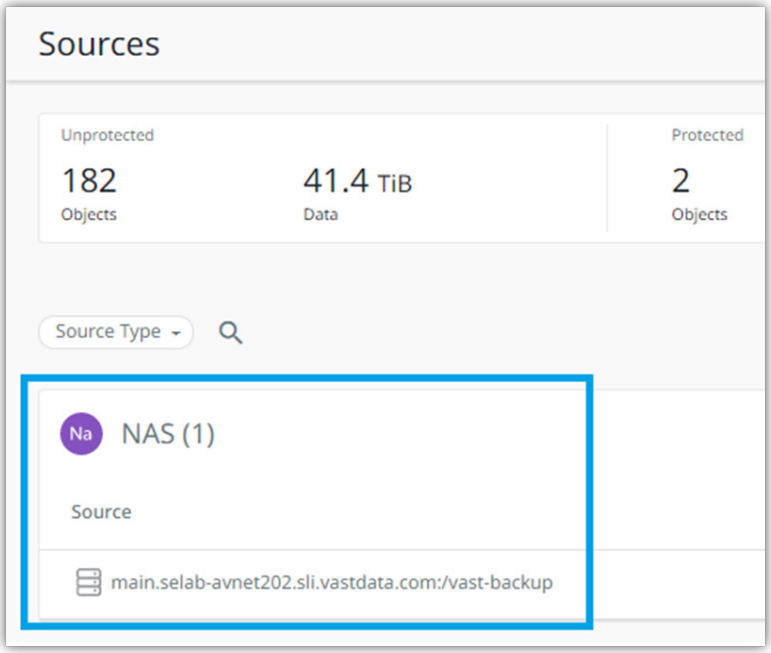

Figure 6 - Successfully added VAST cluster mount point as a source

CREATE PROTECTION GROUP

By default, Cohesity provides four protection policies – **Bronze, Silver, Gold and Protect Once**. Since backup requirements can vary greatly (and is outside the scope of this paper), we will simply use the **Gold** policy for illustration purposes. Policy selection will play a larger role when using the VAST cluster as a target and will be discussed later.

A protection group combines a mount point, backup policy and storage domain (compression/dedupe settings). To create one, from the left pane under **Data Protection** click on **Protection** and then click on **Protect** in the upper right (Figure 7) and then select **NAS**.

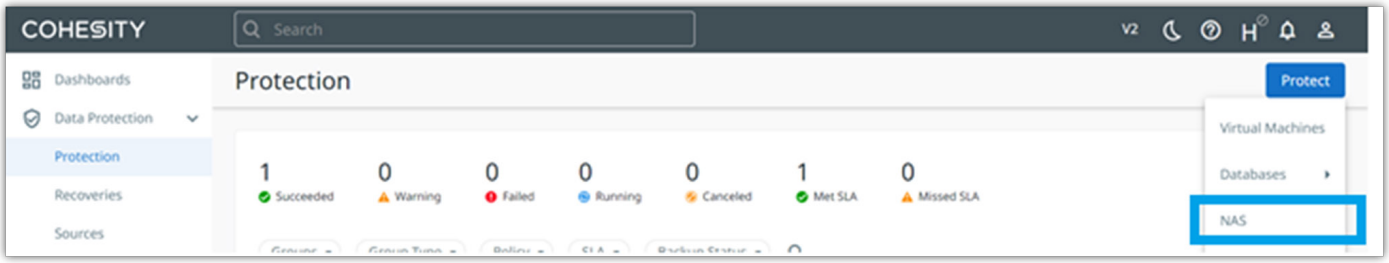

Figure 7 - Create Protection Group

When the NAS window appears select the Source pull down menu and choose NAS Mounts Points (Figure 8). This will then present an Objects section where you will see the available VAST cluster mount point that was registered.

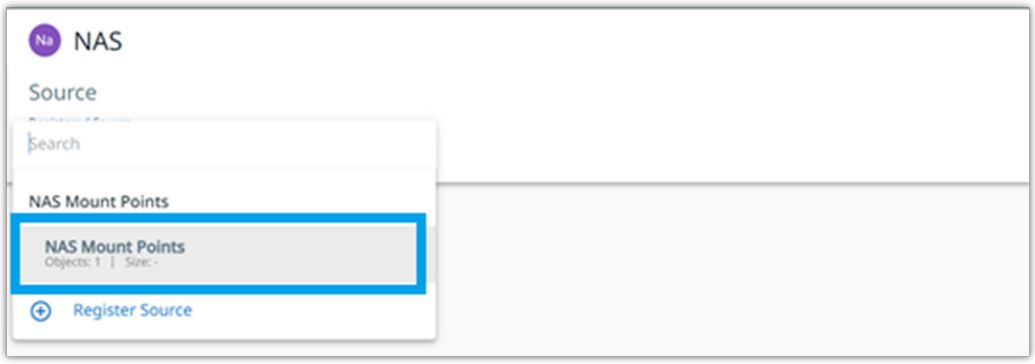

Figure 8 - Select NAS Mount Points to find the source

Select the VAST mount point and then click Save Selection (Figure 9).

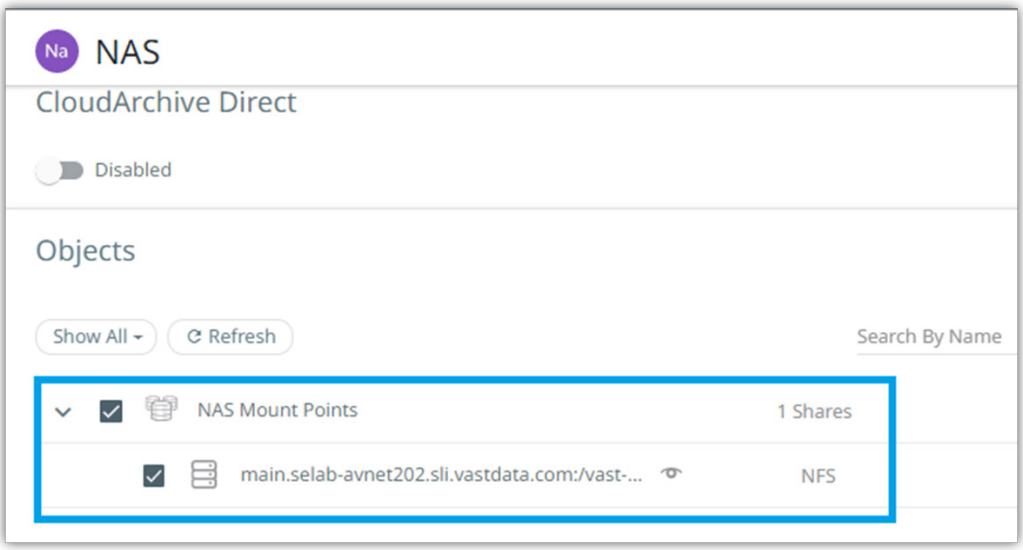

Figure 9 - Select the VAST cluster mount point

After saving, the **Objects** section is minimized, and the remaining fields of Protection Group need to be filled out. Figure 10 shows the entire form filled out with a protection group name and a **Gold** policy is chosen for specific frequency of backups and retry options.

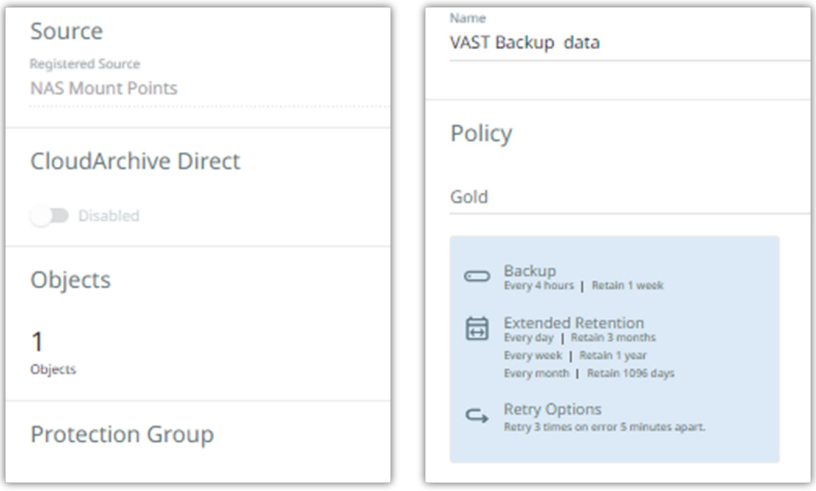

Figure 10 - Protection Group summary (split)

Upon creating the protection policy, it will be initiated, and a backup will begin as can be seen in Figure 11.

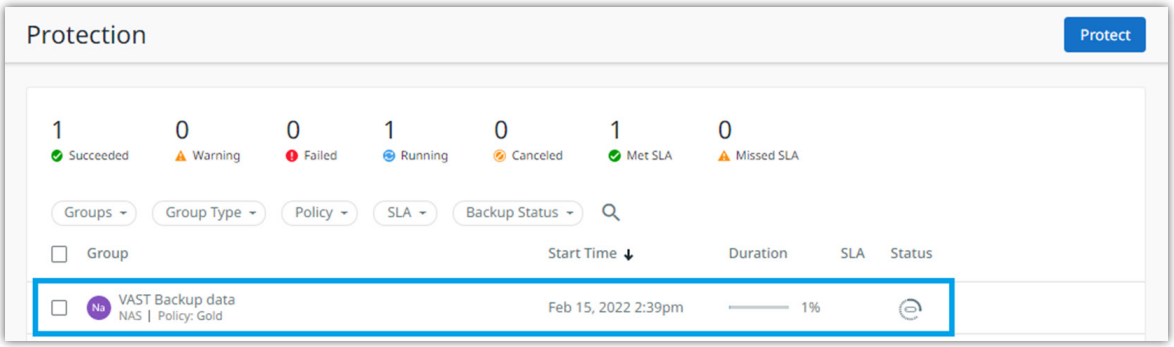

Figure 11 - Protection Group created and backup initiated

RECOVER DATA FROM BACKUP

Recovering data is quite simple from any of the full or incremental backup points.

On the left windowpane under **Data Protection** select **Recoveries**. In the upper right click on **Recover** and maneuver to select **Files or Folders** under **NAS** (Figure 12).

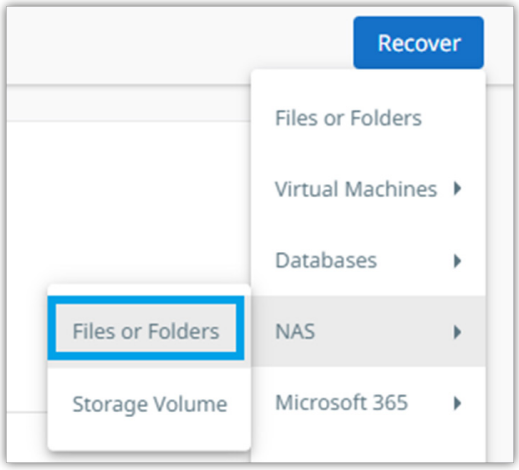

Figure 12 - Select Folder to recover data

This will bring up a window that allows the user to search for the desired files and folders to recover. Glancing at Figure 13 there are two choices to look for the data. If a specific file or folder is known, it is easy to find it by using the Files and Folders option and searching with appropriate characters. If the data is in a known directory, then perhaps selecting the Browse method will be more appropriate.

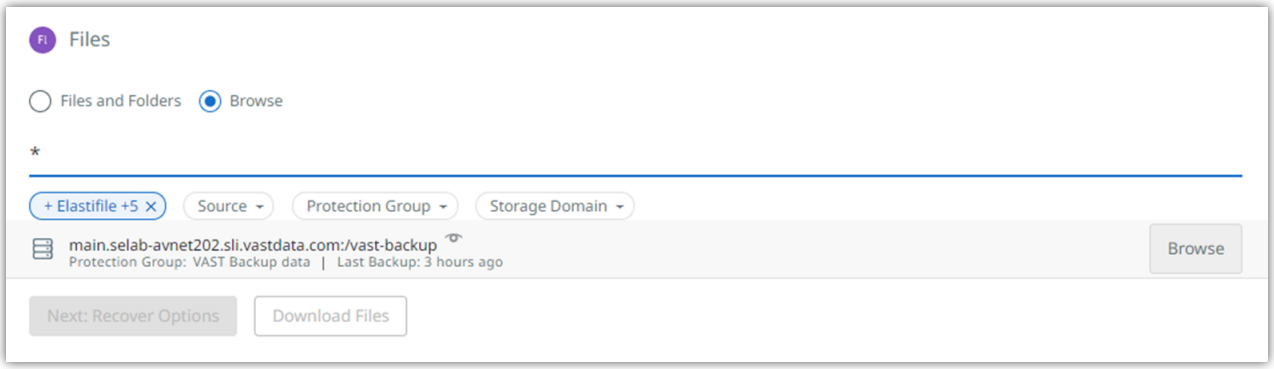

Figure 13 - Browse for file or folder to restore

Once the item(s) have been selected there are several recovery options to choose from, but one easy way is just to download the files and folders directly. If it is more than one file Cohesity DataProtect will zip up the files and allow for download when complete.

With the current integration of the VAST cluster being a simple mount point it would be useful for recoveries if some organization was planned for and established within the directory that would allow for more efficient searching and hence restores.

VAST AS A DATA TARGET

There are two ways to use a VAST cluster as a target:

1. As an archive target as part of an existing policy for cold level storage.

2. As a CloudArchive Direct target where source data from an NFS mount (VAST or third-party) goes directly to the VAST cluster without being backed up on the Cohesity DataProtect cluster.

Both will be looked at in the following sections.

ADDING VAST AS AN EXTERNAL TARGET

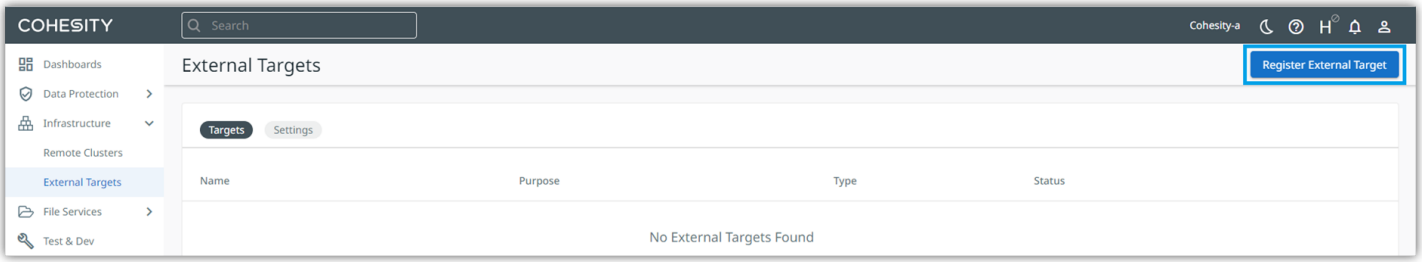

Figure 14 - Register External Target

In the upper right corner click on **Register External Target**. This will bring up a **New Target** window (Figure 15).

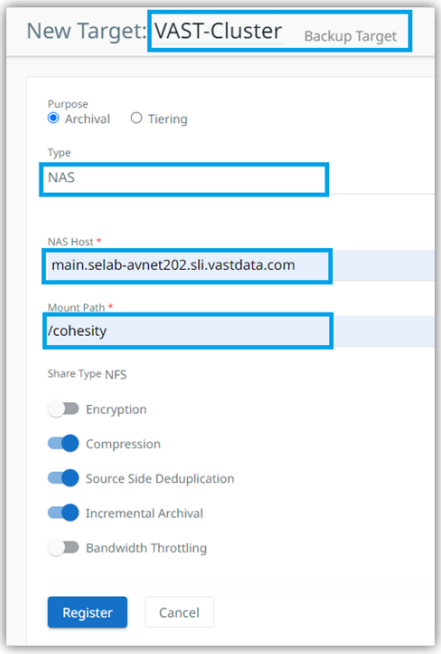

Figure 15 - Enter VAST Cluster details to register

Enter in a name and use the pull-down menu to select NAS for the Type. Enter in the appropriate host and mount path. Refer to Cohesity documentation for more information on the remaining settings to determine what is appropriate. Click Register to finish. After the VAST cluster has been registered as an external target it can now be added to a Protection Policy which differs slightly in each of the target cases. Let's explore each one of them now.

USING VAST AS A TARGET WITH CLOUDARCHIVE DIRECT

In this example, using the Cohesity DataProtect feature, CloudArchive Direct, we will perform a backup from one VAST cluster (or anything other Cohesity supported storage) to a different VAST cluster. Here Cohesity plays middleman and just performs an archive without any backup on the local DataProtect cluster. Only the metadata and indexes are stored on the DataProtect cluster to improve searching and restores. The data, metadata and indexes are all stored on the VAST external target.

Creating Protection Policy for CloudArchive Direct

To be able to backup data to the VAST external target created previously it needs to be a part of a **Protection Policy.** The process is similar to creating a typical archive policy (See section Creating an Archive Protection Policy and Figure 26) except after creation one default setting, Retry Options, needs to be set to zero. This is achieved by editing the protection policy and selecting Customize Retries (Figure 16).

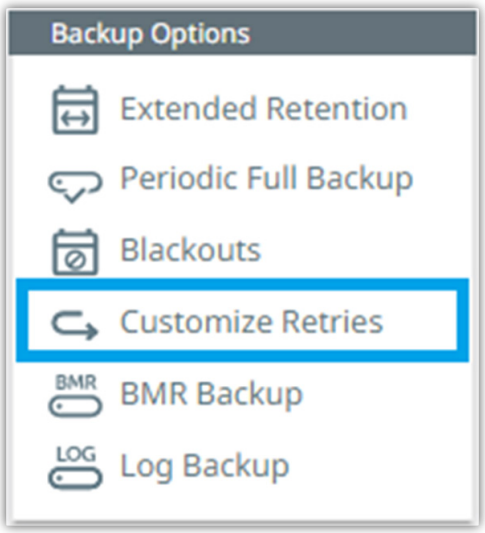

Figure 16 - Backup Options - Customize Retries

Clicking on that option inserts the additional setting beneath **Backup**. Ensure **Retries** is set to zero (Figure 17) and click **Save**.

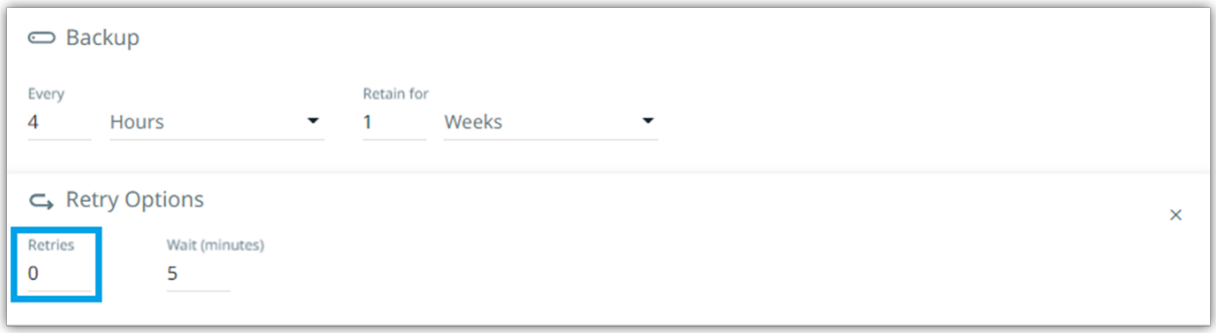

Figure 17 – Setting Customize Retries to Zero

Executing CloudArchive Direct Backup

With the VAST target registered and now a part of a backup policy, it is time to tie it all together with a Protection Group. There are a couple of ways to do this within the DataProtect UI. In this example we will configure the protection starting from the NAS source itself under **Sources** in the **Data Protection** category. Simply right click on the three dots next to the VAST source and select **Protect** (Figure 18).

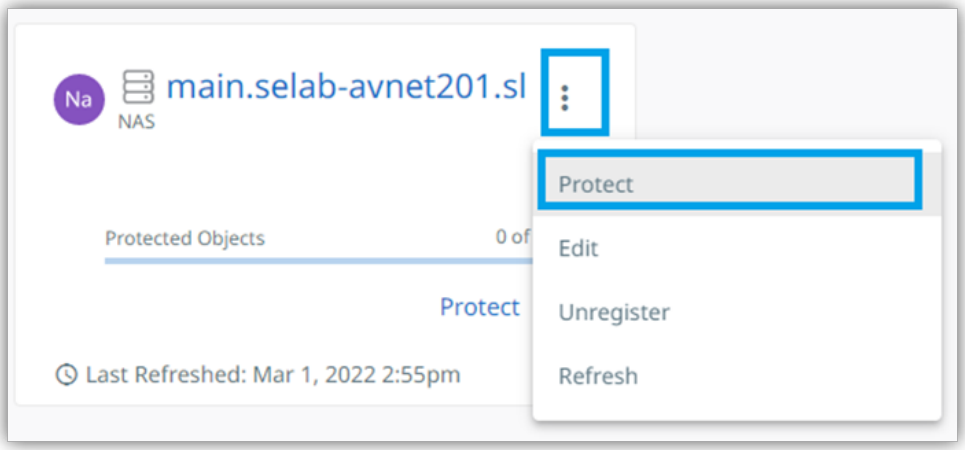

Figure 18 – Selecting NAS Source to Protect

This brings up another window for configuration of the policy. Start by selecting the Registered Source as **NAS Mount Points** (for VAST sources) and then toggle the CloudArchive Direct on (Figure 19). The **Objects** sections lets you select the mount point on the VAST target.

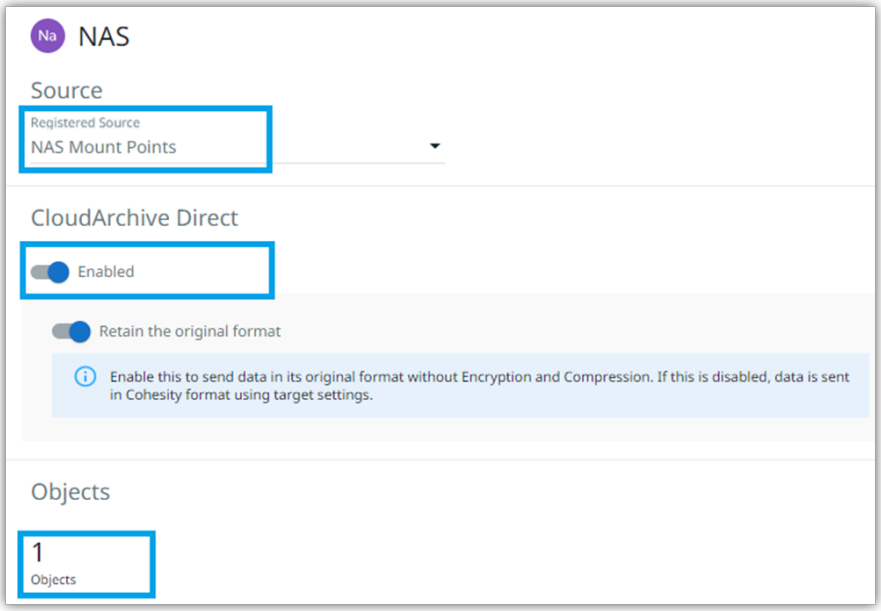

Figure 19 - Configuring CloudArchive Direct (top)

Give the protection group a name and then select the policy that was created in the previous section (Figure 20). If there are no policies that have the retry options set to zero, then nothing will show up in the pull-down menu, but a new policy can be created here.

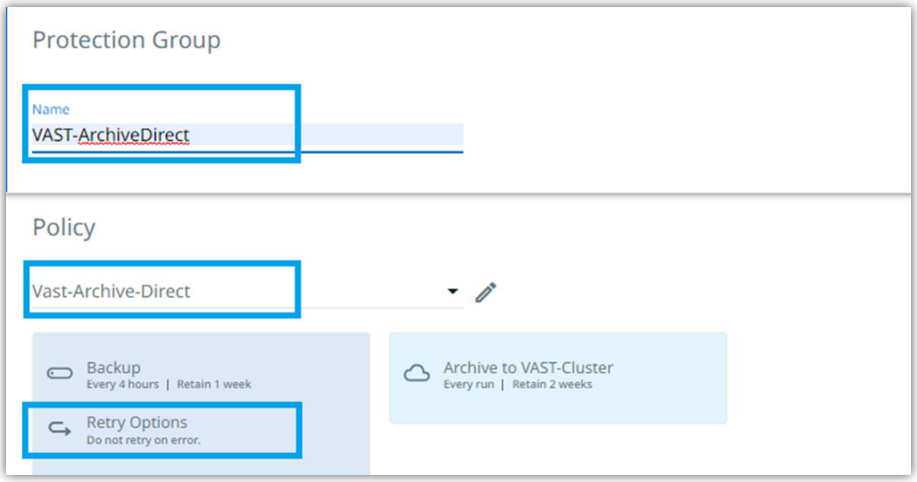

Figure 20 - Configuring CloudArchive Direct (bottom)

Once finished with the form click **Protect** and the protection group will be created and depending on the scheduling may begin immediately.

Restoring Data From CloudArchive Direct

Restoring data from Cohesity DataProtect is quite simple and there are numerous options to recover the desired data into the desired location. The following example shows a simple method of recovering a couple of files from the NAS mount that was protected in the previous section.

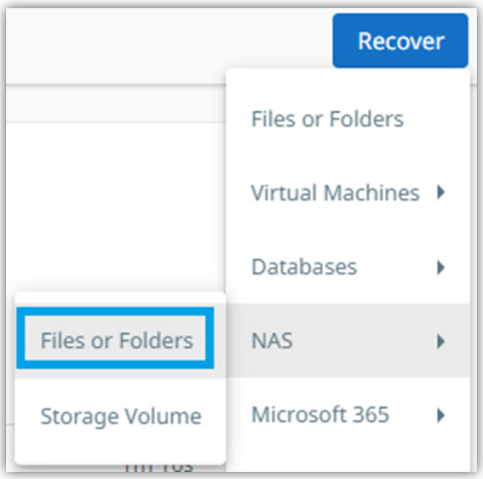

Figure 21 - Recover Files or Folders

Start off by going to the left windowpane and selecting **Recoveries** under **Data Protection**. On the right side of the window click on **Recover** and select **Files or Folders** under **NAS** as shown in Figure 21.

This brings up a **Files** window where the search type for the data can be chosen as shown in Figure 22. Here, the Browse method is selected along with a wild card filter which brings up all available NAS sources. Since there is only one configured simply click **Browse**

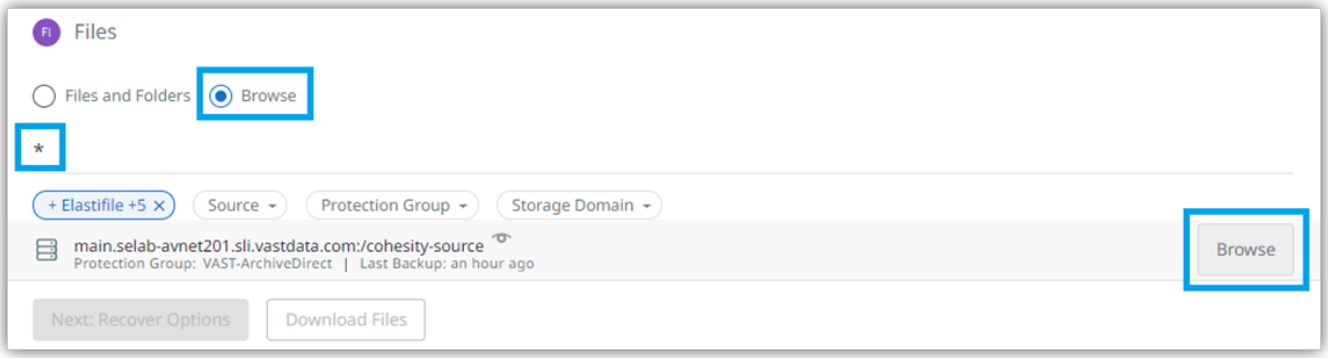

Figure 22 - Recover Files by Browsing

After a couple of intuitive clicks into the directory structure of the backed-up data – two files are selected for recovery as in Figure 23. Once all the desired files are selected simply click **Save** to continue.

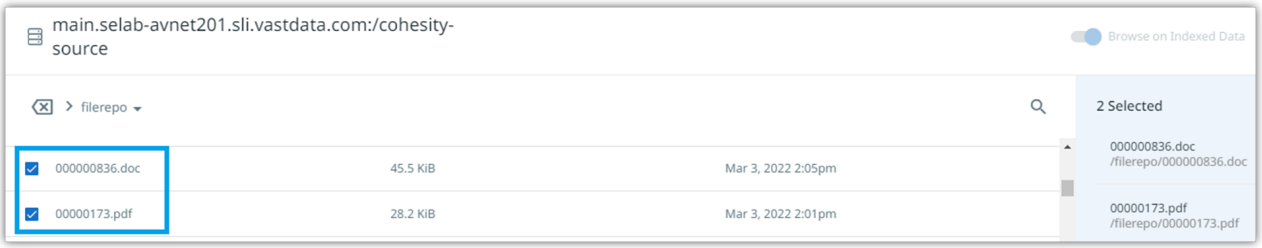

Figure 23 - Selecting Files to Recover

After selecting files and saving, a similar screen to figure 20 appears where additional files can be added to the recovery. At the bottom of that window now appears two recovery choices (Figure 24).

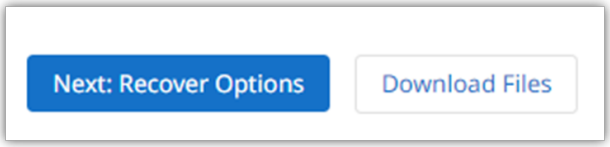

Figure 24 - Recover Options

If selecting **Download Files** and there is only one file, it will simply download straight to the user's desktop. If there is more than one file, then a task is created, and the files will be downloaded within DataProtect. Once the task is completed the user can download the files from within the completed task.

Selecting **Recover Options** offers up more ways to recover the data to different destinations including the original location, new location, and alternative path. To see more information on these options, see the Cohesity user guide.

USING VAST AS AN ARCHIVE TARGET

In the following example VAST will be used as archive target where there is a backup on Cohesity DataProtect and an offline archive on VAST.

Creating an Archive Protection Policy

A new policy can be created, or an existing policy can be copied and edited or simply edited. In the following example a policy was created from scratch.

To do this go to the left windowpane and open **Data Protection** and click on **Policies**. On the upper right click on Create Policy and this will bring up a Create Protection Policy window (Figure 25).

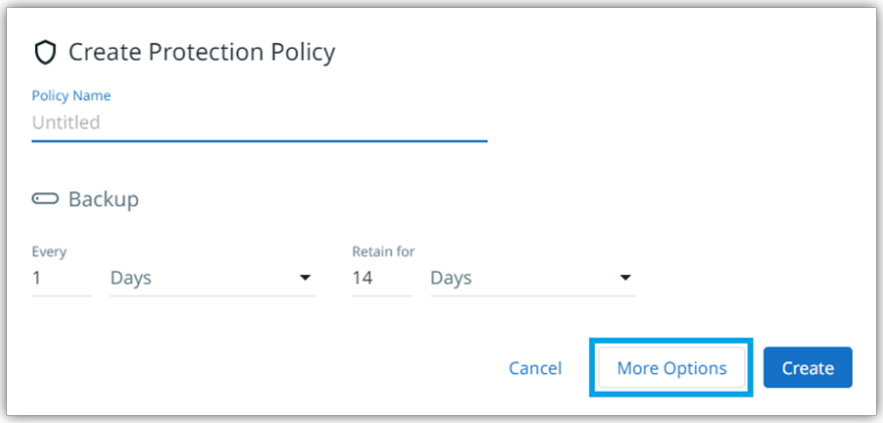

Figure 25 - Create Policy window - simple form

Simply click **More Options** right away as the long form of policy creation is needed to add the VAST target. Fill out the **Policy Name and Backup** frequency and then click on **Add Archive** with the little cloud icon (Figure 26).

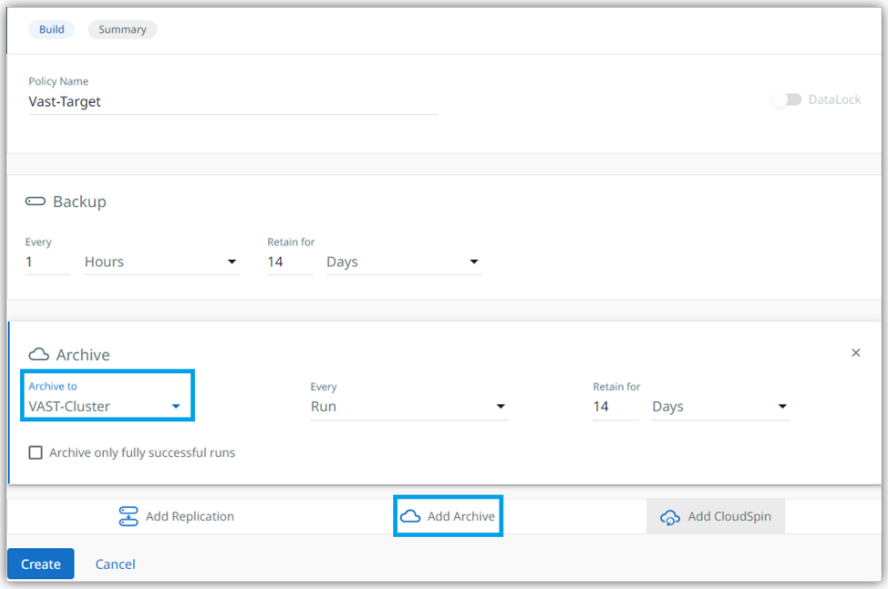

Figure 26 - Creating a Policy - adding archive

An Archive section now appears below the **Backup** section. In that new section under **Archive to**, use the pull-down menu to select the VAST target that was previously registered (Multiple archive locations can be added). When finished click **Create.**

The newly created policy should be listed as in Figure 27 with the term **Archive** and the little cloud icon.

Figure 27 - Newly created policy with VAST archive target

Protection Group Creation with Archive Target

This policy will protect virtual machines where the user chose Virtual Machines from the menu when selecting what to protect (Figure 28).

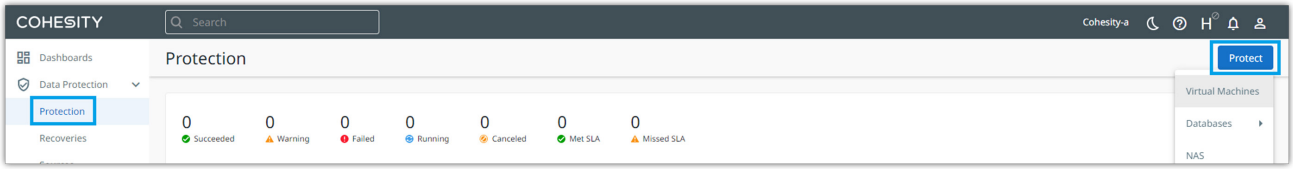

Figure 28 - Creating Protection Group for VMs

A New Protection window (Figure 29) appears and starting at the top select **Add Objects.**

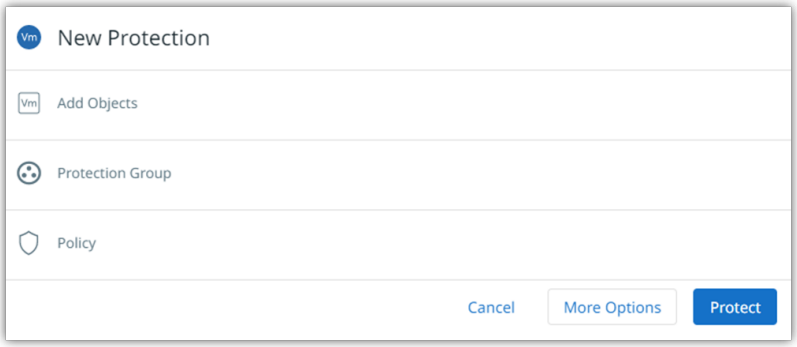

Figure 29 - New Protection Group Window

A new, ***Add Objects***, window appears (Figure 30) and starting at the top select the Registered Source. In this example a vCenter Server has already been added as a source so that one is chosen. Using the browsing capabilities 10 VMs have been selected for protection.

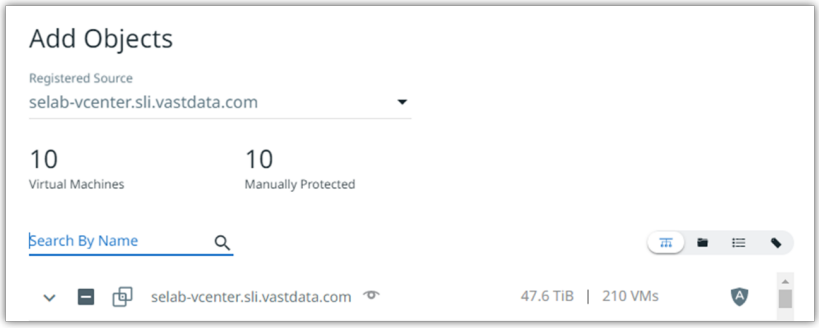

Figure 30 - Adding VMs to Protect

When finished selecting the VMs click **Continue** and then enter in a **Protection Group** name (Figure 29). Lastly under **Policy** use the pulldown menu to select the VAST external target that was configured previously. The final filled out form should look something like in Figure 31. Click **Protect** to finish.

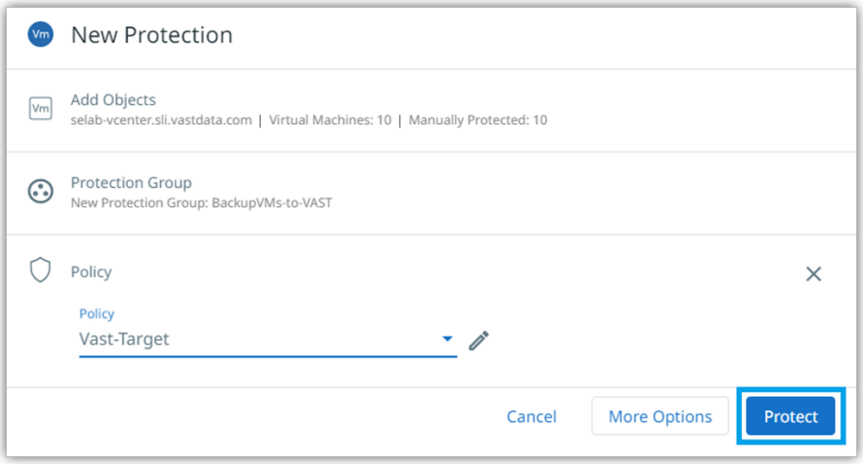

Figure 31 - New Protection Window Filled Out

Just as in Figure 11 a backup will begin and based on the archive frequency both backups (local to DataProtect and to the VAST archive) may be happening simultaneously.

Restoring Data from Archive

Similar to recovering the data from a NAS mount, recovering VMs is just as simple. Again, starting off with the pane on the left select **Protection** under **Recoveries**. On the right side of the window select **Recover** but this time select **VMs** (Figure 32). A Virtual Machines window will appear and in this recovery the search will again be done with the asterisk wild card (Figure 33). Select the VM(s) to be recovered and then click on **Recover Options** (not shown).

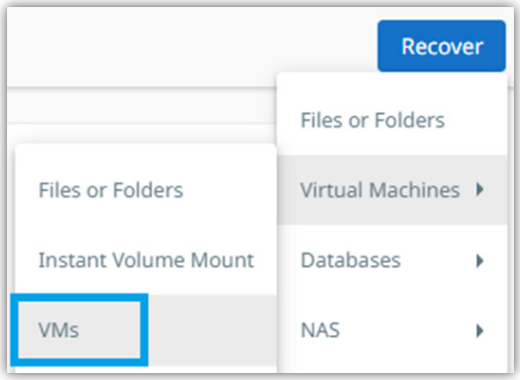

Figure 32 - Selecting VMs to Recover

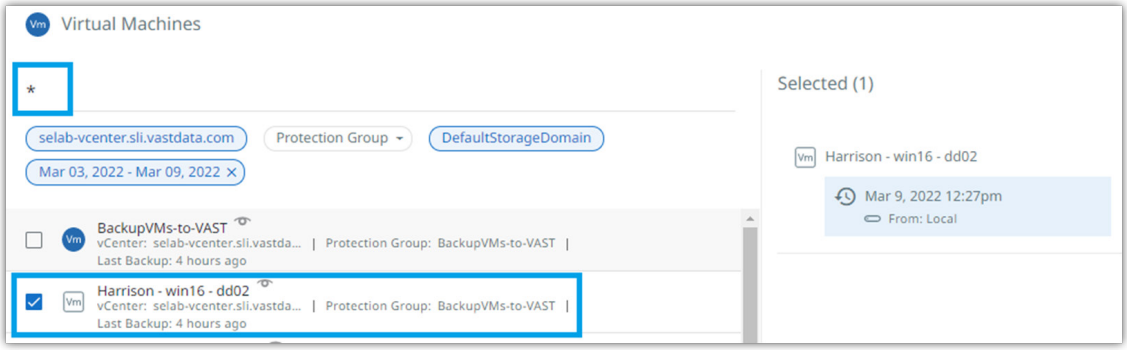

Figure 33 - Searching and Selecting VMs

A Virtual Machines window now appear with further details on how and where to restore the VM (Figure 34).

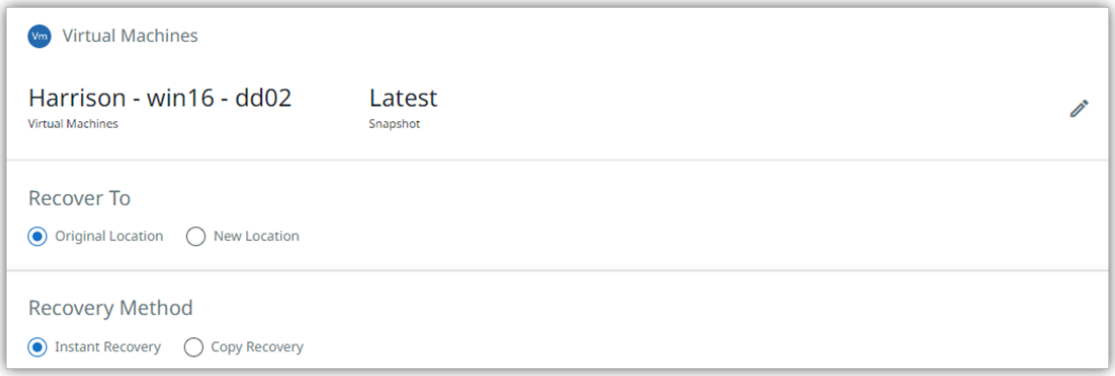

Figure 34 - Virtual Machine Recover Method

For further information on specific VM recovery options see the user guide.

SUMMARY

With the VAST Cluster combined with Cohesity DataProtect, admins can achieve a multitude of back up scenarios. The VAST Cluster can house primary data and have it backed up to DataProtect for sound sleep at night with easy restores in case of data loss. Just as easy, the VAST Cluster can be used as a cold storage archive target either through existing backup policies or directly from another VAST or third-party storage using ArchiveDirect.