COHESITY

Protect Generic NAS with Cohesity

Bringing Scalability and Simplicity to Generic NAS Protection

Version 1.1

May 2025

ABSTRACT

Cohesity streamlines the protection of Generic NAS data you manage. Furthermore, it allows you to archive the backups to any public cloud or tape storage for long-term retention, replication, and recovery to a different location for disaster recovery.

Table of Contents

Figures

Tables

Introduction to Generic NAS Protection with Cohesity

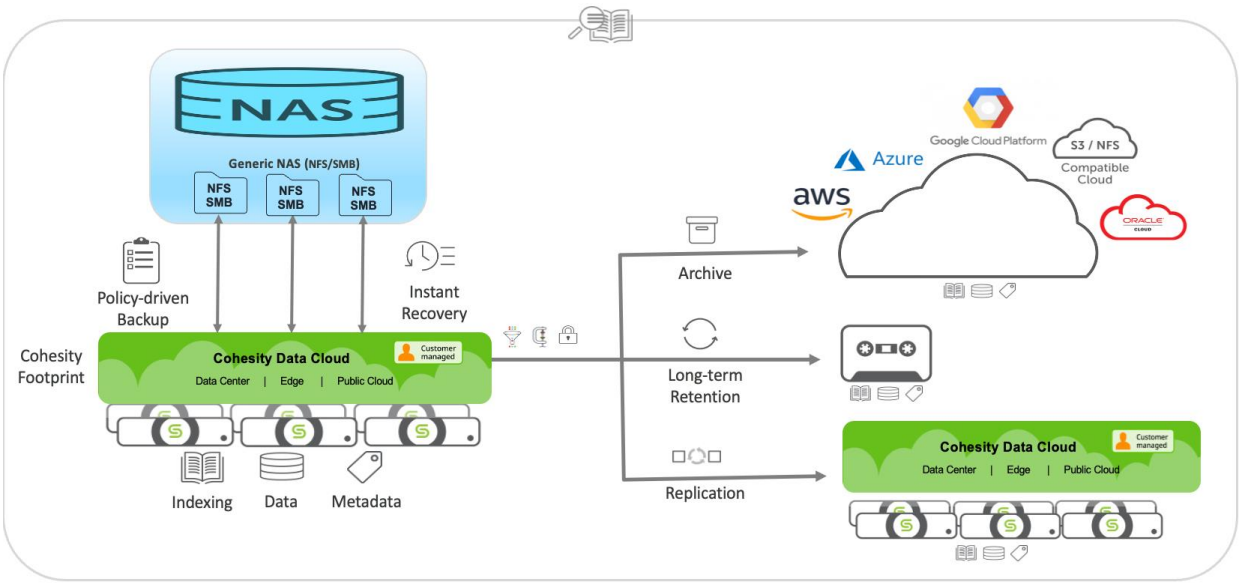
Modern enterprise data centers contain massive amounts of structured and unstructured data in many forms, including log directories, home directories, departmental shares, engineering repositories, and application datasets. This critical data requires a modern data protection and recovery solution that can efficiently protect the ever-growing applications and unstructured data stored via NAS protocols. The solution must adhere to the organizational data protection SLAs and, at the same time, provide better storage efficiency and data reusability.

Cohesity Data Protection Architecture for Generic NAS

Cohesity has API integration with specific NAS vendors such as NetApp and Dell EMC Isilon. These NAS sources are backed up using Cohesity NAS Adapter (API based). All the other NAS vendors where Cohesity does not have API integration are referred to as Generic NAS. Each share in the Generic NAS is registered as an individual Generic NAS source and protected using the NAS protocols. Cohesity provides a fast, powerful, and simple backup and recovery solution that scales well to grow with the ever-growing data.

To meet the needs in a reliable and efficient ecosystem, Cohesity provides a solution that eliminates the complexities and operational inefficiencies of traditional NAS protection solutions by unifying your data protection and recovery infrastructure—including target storage, backup, recovery, replication, archiving, and disaster recovery—on a single platform.

Figure 1: Protect Generic NAS Data with Cohesity



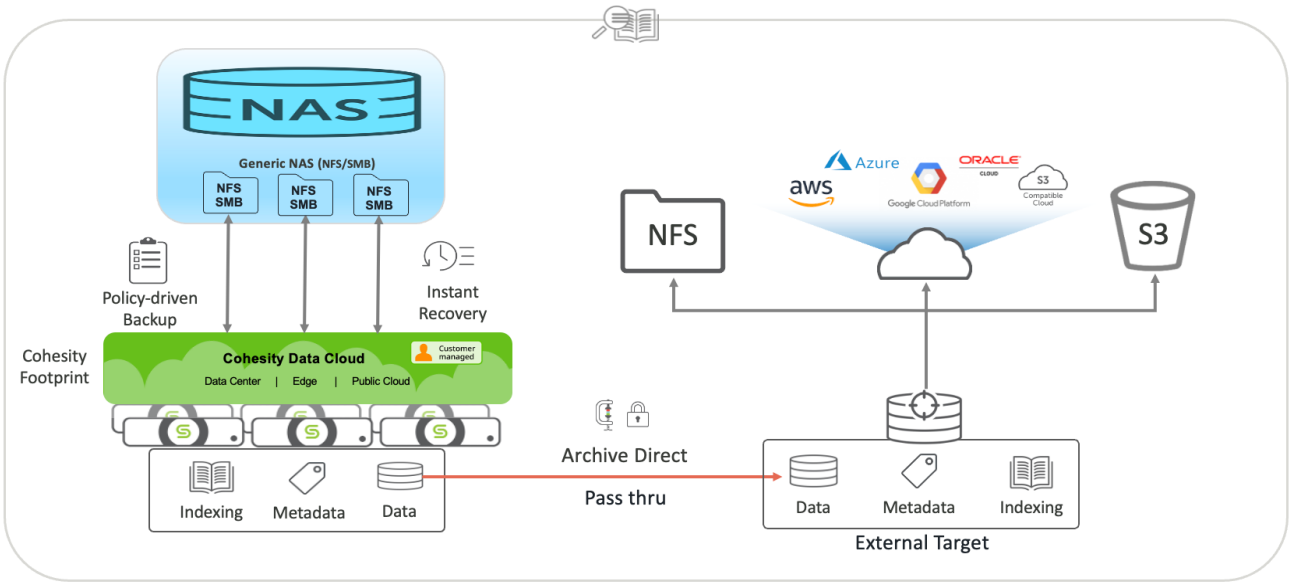
Once you back up your Generic NAS source directories to Cohesity, you can also:

- Recover your data.
- Archive it to lower-cost cloud/NFSv3/S3 storage for long-term retention and disaster recovery.
- Send it to tape for long-term retention.
- Replicate it to another on-premises or cloud Cohesity cluster.

Cohesity CloudArchive Direct Architecture for Generic NAS

Cohesity has built CloudArchive Direct for NAS, a cost-efficient solution that processes and streams the data directly from NAS source to lower-cost storage on External Targets using object storage in the public/private cloud or NFS. By eliminating the need to store a copy locally before archiving, the footprint/capacity requirements of your Cohesity cluster are dramatically reduced. Only the metadata and indexes, which enable quick search and recovery, are stored on the Cohesity cluster. The entire Generic NAS dataset (the data along with metadata and indexes) is stored only on the External Target.

Figure 2: Make Generic NAS Data Archival Cost-effective with Cohesity's CloudArchive Direct



CloudArchive Direct is a policy-driven feature with seamless integration with all major cloud vendors like AWS, Azure, GCP, Oracle, or any S3-compatible object store. It can also be configured with compression and encryption to achieve maximum storage efficiency and security.

NOTE: See Archive Your Data Directly with Cohesity CloudArchive Direct for details.

Features and Benefits

As data grows exponentially, the need for a modern approach to data protection and backup solutions has become critical. Cohesity offers agentless, policy-based data backups, granular file-level restore capabilities, and replication, archiving and cloud tiering.

What's more, Cohesity provides:

- **Incremental Forever**. Taking advantage of native NFS and SMB-based backups, Cohesity offers true 'incremental forever' functionality. Unlike NDMP, it requires performing only one full backup, followed by incremental backups forever. This reduces the time required for backups and recovery and simplifies operations.
- **Multithreaded File Discovery**. Cohesity backups are much faster because they employ high-speed multithreaded file discovery.
- **Distributed and Parallel Ingest**. Cohesity's intelligent data-transfer logic creates an efficient backup plan and assigns backup streams across all nodes, performing distributed and parallel ingest in the cluster, ensuring faster backups.
- **Instant Recovery**. Cohesity enables instant NAS volume to be restored to any point-in-time (PIT) copy. Upon restore, Cohesity creates an instantaneous clone of the snapshot. The NAS volume can be accessed directly from the clone, with storage running directly from the Cohesity cluster. This eliminates the need to move data from secondary to primary systems before initiating a restore.
- **Flexible Restore Targets**. As Cohesity backs up data in its native format, it supports data restoration to different vendor devices, giving you the flexibility to restore data to the original source or a different target.
- **Data Security with Encryption**. Cohesity provides built-in, software-based encryption so that you can securely store and transfer your data. Cohesity keeps your data safe by encrypting data at rest and in transit with AES 256-bit encryption.
- **Incremental Indexing**. Cohesity indexes only the changed data between the last and most recent backup, resulting in faster indexing and reduced resource impact.

NAS Backups—Legacy vs Cohesity

Cohesity's modern platform also offers several advantages over traditional NAS data protection solutions. Table 1 below compares Cohesity's data protection solution against legacy solutions for tackling the key challenges in NAS backup.

Table 1: Legacy vs Cohesity NAS Backup Solutions

KEY CHALLENGES	LEGACY NAS BACKUP	COHESITY NAS BACKUP
Infrastructure Silos	Siloed media servers and targets lead to complex infrastructure with fragmented datasets.	Hyperconverged platform enables the consolidation of infrastructure and datasets, which leads to a better return on investment (ROI).

KEY CHALLENGES	LEGACY NAS BACKUP	COHESITY NAS BACKUP
Management	Multiple interfaces to manage different components are inconvenient and prone to human errors.	Unified management for multiple clusters from a single pane of glass reduces administrative overhead.
Scalability	Requires forklift upgrades to scale up, which is disruptive and time-consuming.	Transparent scale-out with relative ease. With growing business needs, it can incorporate additional resources (capacity, compute, network) without tedious forklift upgrades.
Performance at Scale	Requires periodic, frequent full backups, which is unfeasible with large file systems at a petabyte scale that contain billions of files. This results in increased RPOs.	Faster, more intelligent backups with distributed and parallel ingest. Full support for incremental-forever backups, reducing data traffic, shortening the backup window, and improving RPO.
Storage Efficiency	Does not provide global data reduction across silos, making backups inefficient with storage and costly.	Inline and post-process variable-length deduplication makes efficient use of storage and lowers the total cost of ownership.
Data Mobility	Not storage agnostic. For example, NetApp backups cannot be restored instantaneously to third-party vendor storage.	Backups are taken using native NFS and SMB protocols, making data recovery platform-independent. For example, an Generic NAS backup can be restored to NetApp instantaneously, and vice-versa.
Faster and Granular Restores	Indexes need to be read from a media server. As a result, network bottlenecks can dramatically slow down indexing, making recovery times very lengthy.	The file metadata is indexed to allow Google-like search in your backups, enabling very fast, granular file-level recovery to any point in time across billions of files.
SLA Predictability for Recovery	Recovery times are not predictable and can take weeks at the petabyte scale.	Backup data can be exposed as a Cohesity View for instant restore on Cohesity, delivering predictability and eliminating RTO concerns.
Cloud Integration	Most often, it uses cloud gateway to tier or archive data to the cloud.	Natively integrated with major public cloud providers to enable smooth archival and tiering to the cloud.

Explore Cohesity's Generic NAS Adapter's Capabilities

Cohesity's Generic NAS adapter provides a wide range of Generic NAS data protection capabilities for your Generic NAS backup, including:

- **Encrypt Backup Traffic Between Generic NAS Source and Cohesity**. You can encrypt your backup traffic between Generic NAS source and Cohesity just by enabling "Encryption" in the Protection Group's advanced settings.
  - **For SMB backups**, if encryption is enabled in the Protection Group, then Cohesity starts an encrypted SMB session with Generic NAS source to access the SMB volume data to back up. The encrypted SMB session encrypts all the session traffic between Generic NAS source and Cohesity.

NOTE:

- To use this feature, enable encryption at the share level in your Generic NAS configuration.
- The restore workflow is encrypted.

Table 2: Encryption Behavior Relationship with SMB Encryption Status in Generic NAS

COHESITY VERSION	ENCRYPTION ENABLED IN PROTECTION GROUP?	OPERATION	SMB ENCRYPTION *ENABLED* ON NAS SHARE	SMB ENCRYPTION *DISABLED* ON NAS SHARE
6.8.1, 7.0, 7.0.1, 7.1, 7.1.1, 7.1.2 and 7.2.2	No	Backup	Fail	Pass
		Restore	Fail	Pass
		Backup traffic encryption	N/A, as the backup failed	No
	Yes	Backup	Pass	Fail
		Restore	Pass	Fail
		Backup traffic encryption	Yes	N/A, as backup failed

- **For NFS backups**, if encryption is enabled in a Protection Group's advanced settings, then Cohesity reads the NFS volume data over Kerberos to ensure the backup traffic is encrypted between Cohesity and the Generic NAS source.

  NOTE:

  - Encrypting in-flight data will have a minor impact on the performance.
  - To use the encryption functionality for NFS volumes, you must join the Cohesity cluster to the active directory as the Kerberos server or add the Kerberos provider in the Cohesity cluster Access Management section.
  - To use this feature, enable encryption at the share level in your Generic NAS configuration.

- **Download List of Skipped Files to Local .csv File**. You can download the list of all entities (files and folders) that were skipped during backup, along with the most applicable reason. Log in to Cohesity to download this list to a .csv file on your local machine.
- **File DataLock to Preserve Access Time of SmartLock Directories**. With Cohesity 6.8.x and higher, you can enable **File DataLock** in the Cohesity Protection Group's advanced settings for NAS data protection. If enabled, Cohesity preserves the write once read many (WORM) attributes, along with backed up data, for the files and folders of the protected WORM directories, which provides the access time, lock period of the files/folders, and other information. These attributes are applied to the files and folders when recovered to the Cohesity View, thus making the data immutable in the View. Cohesity also allows you to:
  - Override the lock period of the files/folders while recovering them to the Cohesity View.
  - Set the lock period for the new files/folders that are created in the recovered Cohesity View.

  NOTE:

  - Supports Enterprise or Compliance modes.
  - Preserves the access times of both hard and symbolic links.
  - You cannot enable or disable File DataLock once a Protection Group is created.
  - You can delete Protection Groups and snapshots that have File DataLock enabled. However, once the data is recovered to the Cohesity View, that is, when the preserved WORM properties are applied, the Cohesity View cannot be deleted until the lock period expires.

  See File DataLock in the online Help for details.

SMB DFS Referral

The Cohesity SMB client now follows the Distributed File System (DFS) referral. The Distributed File System has a collection of shares on different machines that serve a file system namespace. If one machine does not have a particular file requested by the client, it is referred to check the other machine.

Users can now backup the entire DFS namespace by simply registering the share with the hostname directly as a Generic NAS SMB mount point.

Before the 6.8 version, registering each share as a Generic NAS source and backing it up in a Protection Group was suggested by Cohesity support as a workaround in some cases. After the upgrade, the Cohesity cluster may end up backing up the same data multiple times causing data bloat and an increase in the run time.

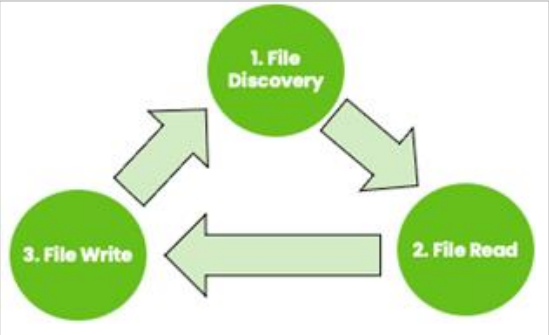
If you are using this method, then you should contact Cohesity Support to transition to the SMB DFS Referral method.

Understand Cohesity's Generic NAS Backup Approach

Cohesity DataProtect uses a simple three-step approach to protecting Generic NAS data. Each step is optimized with modern techniques like adaptive data tasking and distributed parallel data streaming.

To understand how Cohesity Generic NAS data protection works, it's essential to understand exactly what is going on in each phase of the process:

1. **File Discovery**: Discover the files to back up.
2. **File Read**: Read the discovered files over NAS protocols and divide the files into multiple data chunks.
3. **File Write**: Write the data chunks to Cohesity using distributed and parallel streams.



File Discovery

At a high level, for every backup run, the Cohesity file runner discovers the list of files and folders that need to be backed up from the user-selected object in the Cohesity Protection Group. You can also use simple exclusion and inclusion rules to define the objects to be protected.

NOTE:

- To add an inclusion, you must prefix a forward slash ('/') or suffix an asterisk ('*') to the path of a particular file within the protected object. For example, '`/test`' or '`*.txt`'.
- Cohesity does not support regular expressions for inclusions.
- Cohesity supports complex regular expressions for exclusions such as '`/Vol1_Folder2/*.txt`' or '`/Vol1_Folder*/File1.txt`.' Refer to Create a Protection Group for NAS Volumes in the online Help for more on exclusions and inclusions.

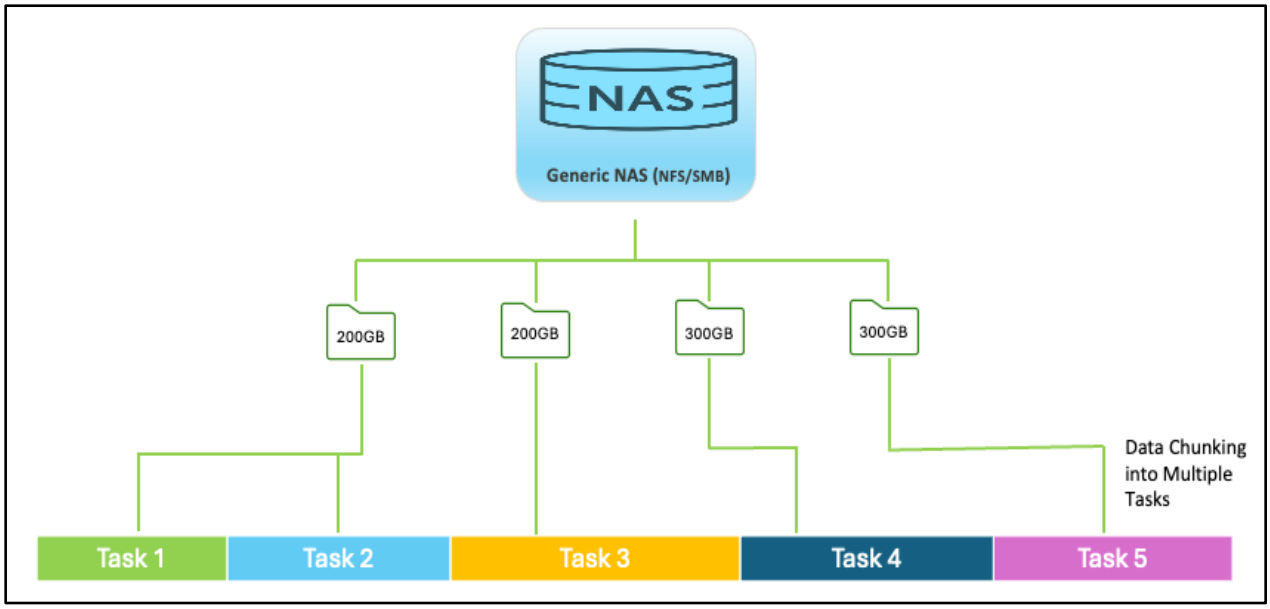
Cohesity performs slightly different file-discovery processes during full and incremental backups. See Cohesity Generic NAS Backup Workflows below for details.

File Read

Cohesity DataProtect uses a parallel and distributed architecture to read the NAS dataset, using native SMB/NFS protocols identified during the File Discovery phase above. It uses an intelligent algorithm to divide the identified dataset into multiple tasks (data chunks) based on data size and the number of files. This adaptive task chunking enables Cohesity DataProtect to back up data more efficiently, reducing the backup window and improving backup SLAs.

In the example below, identified datasets in the File Discovery phase have been divided into five tasks with varying sizes.

Figure 3: File Read

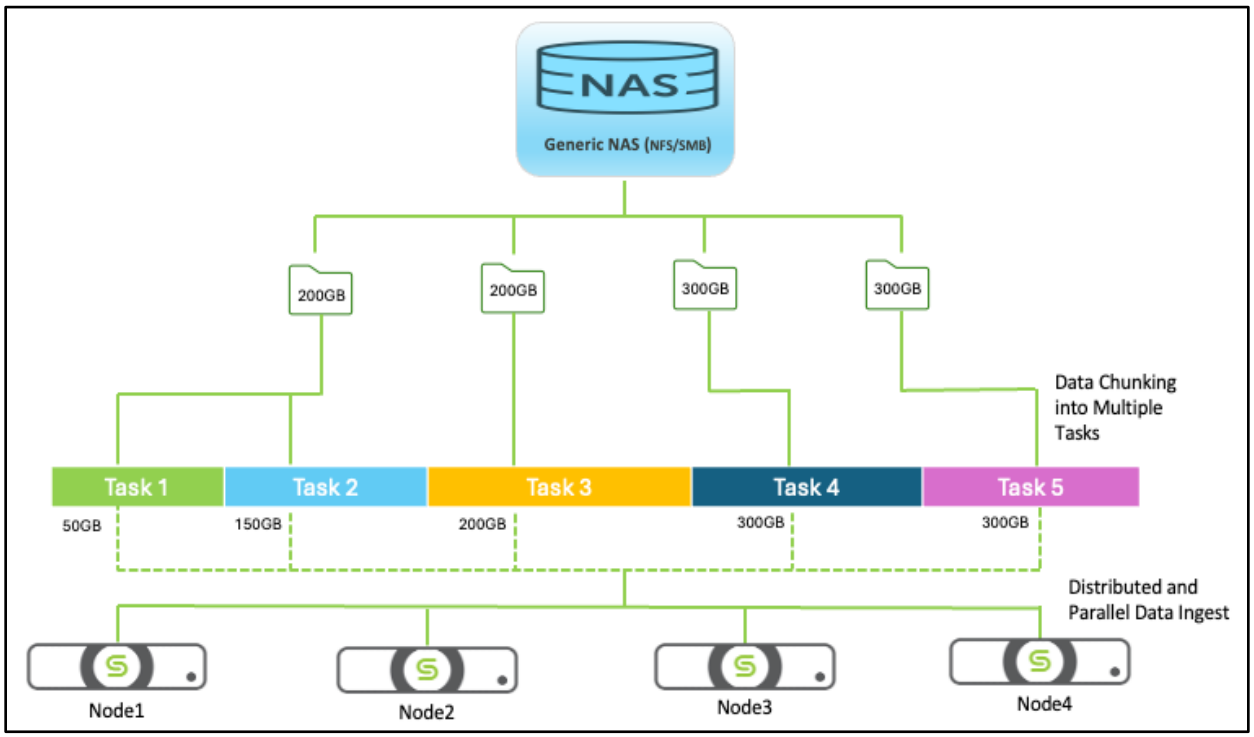


File Write

File Write is the last phase in the backup process. In this phase, files and folders that were divided into multiple tasks during the File Read phase above are written over parallel streams to different Cohesity cluster nodes or, with CloudArchive Direct, streamed directly to an archive storage target in the public cloud. As all the nodes are involved in writing the data, backup throughput is greatly improved.

In the example below, tasks created in the File Read phase are ingested in a parallel, distributed fashion to all Cohesity nodes

Figure 4: File Write



Cohesity intelligently selects the node for data placement based on multiple factors such as capacity, performance, the Quality of Service (QoS) policy, and the system state of the node, which helps improve RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives). The ingest engine also ensures that data is optimally placed onto the SSD or spinning disk tier that best suits the profile of the incoming data stream.

Cohesity also provides encryption of the data, both at rest and in flight, with AES 256-bit encryption.

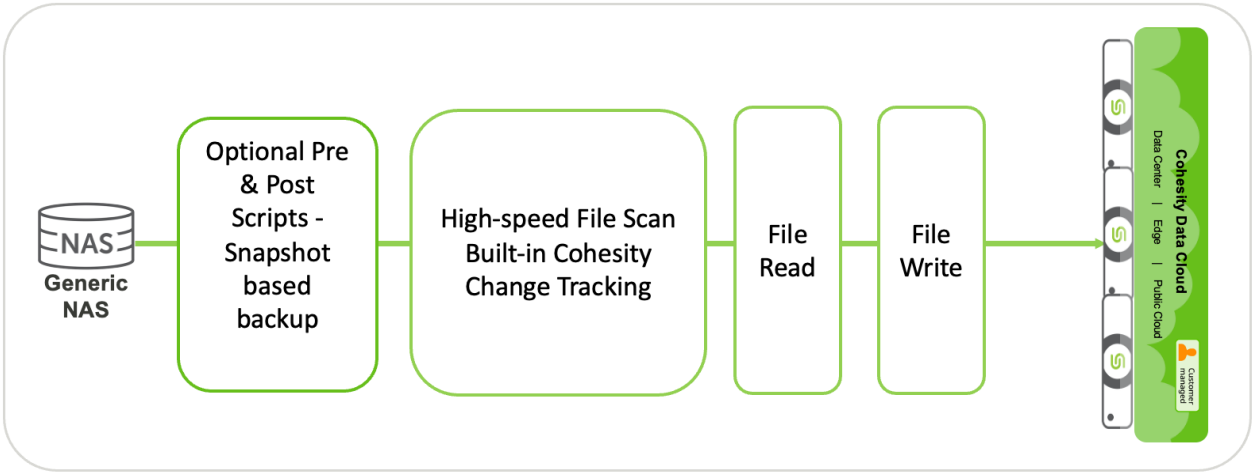
After a Protection Run is completed, all files are indexed by Cohesity to enable global search and rapid recovery.

Cohesity Generic NAS Backup Workflows

As you prepare to protect your NAS data, it helps to understand the various workflows and choices available in Cohesity's solution. With our approach of taking a full backup once and following it with incremental forever backups, each phase involves slightly different operations:

- **Full backups**: In this case, Cohesity executes high-speed file discovery using a file runner.
- **Incremental backups**: After the full backup, Cohesity employs its Built-in CFT (Cohesity streaming diff technology.)

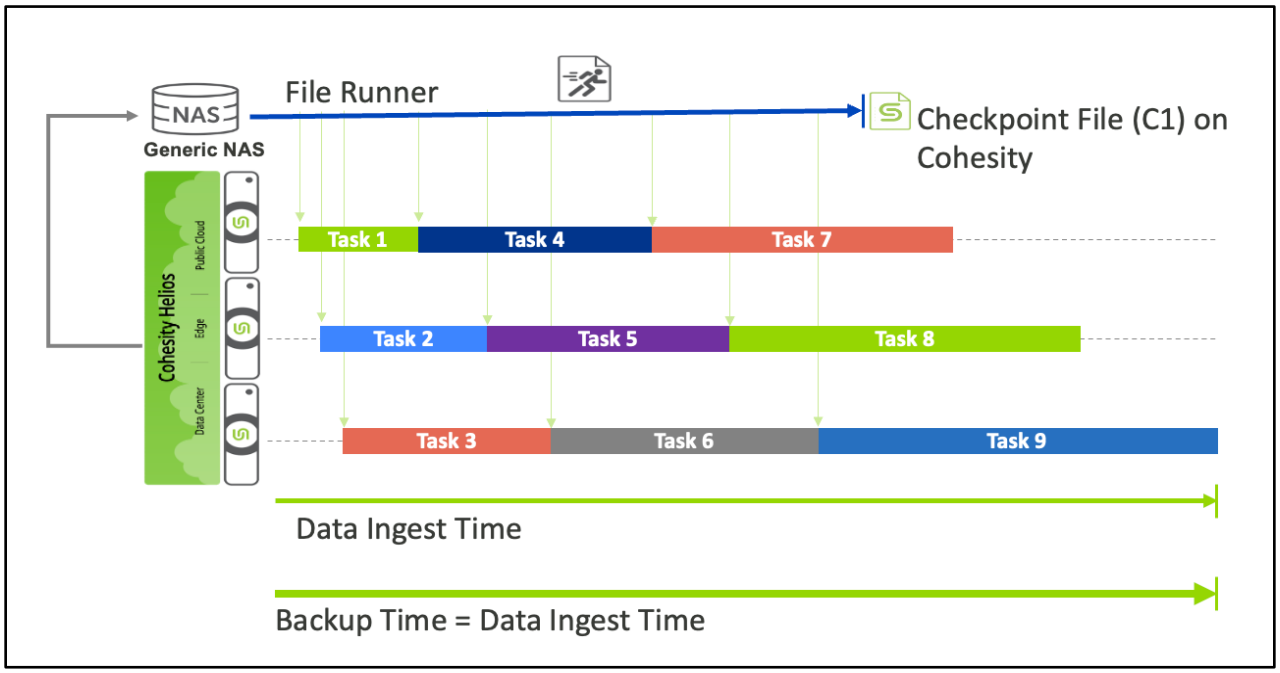
Figure 5: Cohesity's Approach to Protecting Generic NAS Data



Full Backup with High-speed File Discovery

To start the protection, the initial backup is always a full data backup. Cohesity's Generic NAS data protection is a mount-based backup and can be used to back up any NAS device. Generic NAS data protection is not a point-in-time (PiT) backup and Cohesity DataProtect scans through the live file system during backup. Hence, the open or locked files may be excluded during backup. You could however configure custom Pre/Post scripts that can be used to take snapshot-based backups.

Figure 6: Cohesity's Initial, Full Generic NAS Backup Process



During the initial, full backup, Cohesity DataProtect scans the Generic NAS live filesystem and performs the following operations in parallel, thereby dramatically reducing backup times:

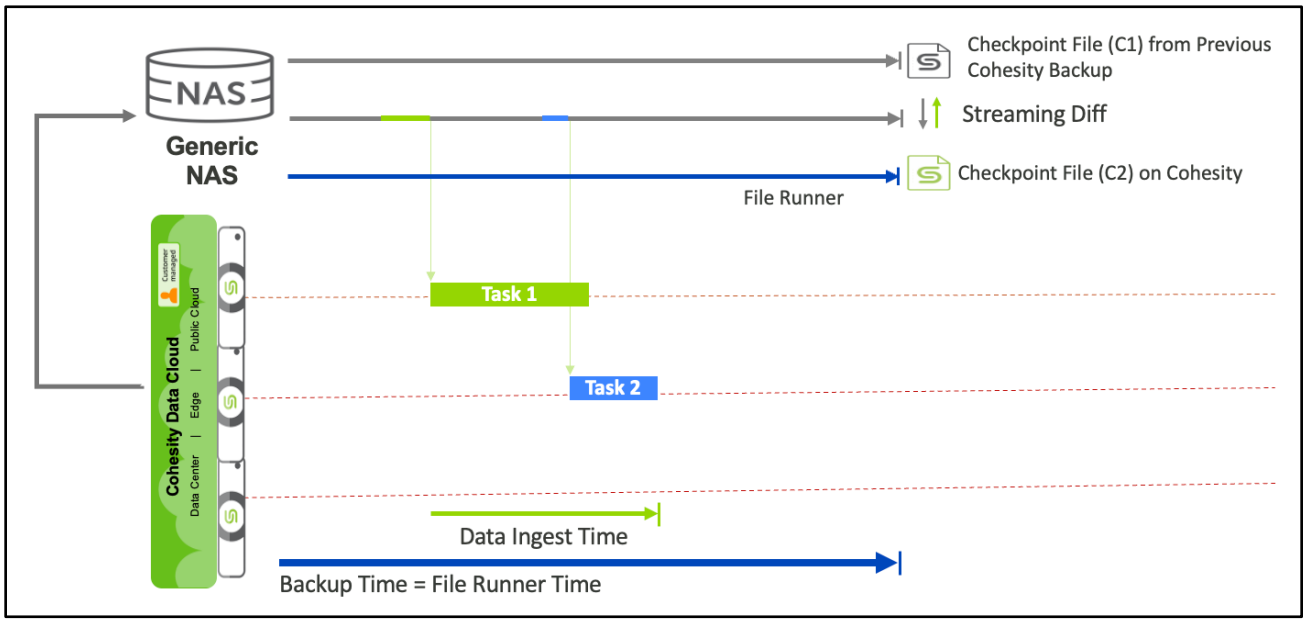
- **File Runner**: Starts the high-speed file runner on the live filesystem and discovers the files & folders to back.
- **Checkpoint File**: The file runner stores the metadata in a checkpoint file (C1).
- **Data Ingest**: Creates data-ingest tasks as new files & folders are discovered, and distributes them in parallel across all nodes in the cluster.

After the first full backup is complete, it is followed by incremental forever backups that send only changed data. Cohesity uses its built-in CFT based on streaming diff technology.

Incremental Forever Backups with Built-in Cohesity CFT

With a full backup in place, Cohesity uses an incremental forever approach for all subsequent backups. The goal of an incremental backup is to locate and transfer only the data that has changed since the last backup. Cohesity identifies the changed data by performing its own built-in CFT using streaming diff technology to discover the changed files and folders to back up.

Figure 7: Cohesity's Incremental Generic NAS Backup Process



During the incremental backup, Cohesity DataProtect performs the following operations in parallel, thereby dramatically reducing backup times:

- **File Runner**. Starts the high-speed file runner on the live filesystem and discovers the files & folders to backup.
- **Checkpoint File**. The file runner stores the metadata in a new checkpoint file (C2).
- **Streaming Diff**. This operation compares the file runner output with the previous checkpoint file (C1) and identifies the changed files to protect.
- **Data Ingest**. Creates data-ingest tasks as changed files are discovered and distributes them in parallel across all nodes in the cluster. Cohesity DataProtect creates the tasks as changed files are identified, and does not wait for the new checkpoint file (C2) to complete.

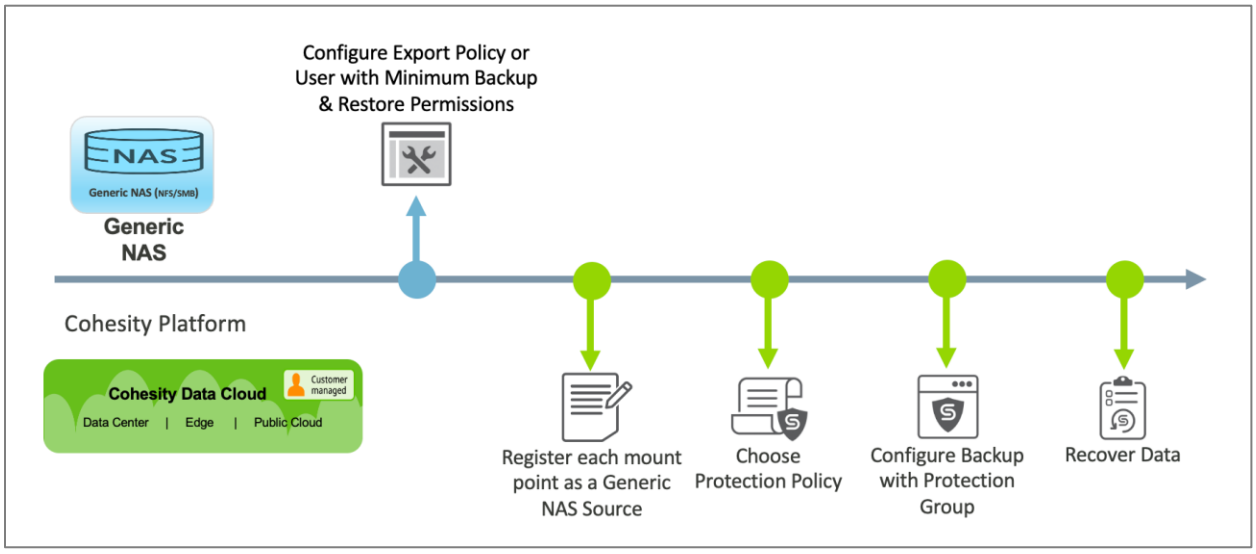
Protect Generic NAS Data with Cohesity DataProtect

Using Cohesity DataProtect, you can back up one or more Generic NAS NFS mount points or SMB shares while preserving ACLs and extended attributes on SMB.

To prepare Cohesity DataProtect to back up your Generic NAS sources, ensure your Cohesity and Generic NAS sources meet the prerequisites:

1. Ensure the Prerequisites are met.
2. Register your Generic NAS mount points as individual sources in Cohesity.
3. Choose a Cohesity Protection Policy.
4. Create a Cohesity Protection Group.
5. Recover Generic NAS data using Cohesity DataProtect.

Figure 8: Protect Generic NAS mounts with Cohesity DataProtect



Add Your Generic NAS mounts as a Cohesity Source

To back up your Generic NAS mounts on Cohesity DataProtect, you need to register each Generic NAS mount as a source in Cohesity.

Prerequisites

Our solution requires the following to protect Generic NAS mount points:

- Cohesity 6.8.x or higher
- All NAS vendors supporting NFS (v3, v4.1) and SMB (v1, v2 and v3)

> **NOTE**: See the Cohesity Software Version Support Matrix below for the software version compatibility details.

- Required permissions for backup and recovery.
  - For NFS exports
    - The NFS export should be configured to have Cohesity VIPs and Node subnets whitelisted in its export policy.
    - The export policy should also be configured with a minimum Read-Only role for backup and Read-Write role for restore operations.
  - For SMB shares
    - To backup Generic NAS SMB/CIFS shares to the Cohesity cluster, the user must have local or domain user credentials that allow at least read access to the SMB share.
    - To recover the SMB/CIFS shares from the Cohesity cluster, the local or domain user must have full access control on the target where data is being restored.

> **NOTE**: If assigning granular permission is a must, you can assign the following privileges to the SMB backup user account.
>
> - **SeBackupPrivilege** to the SMB user to back up the SMB data without modifying the ACL on the SMB shares.
> - **SeRestorePrivilege** to restore files and directories, override any ACLs, and set a valid user or group SID as the file owner.
> - **SeChangeNotifyPrivilege** to bypass traverse checking. Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

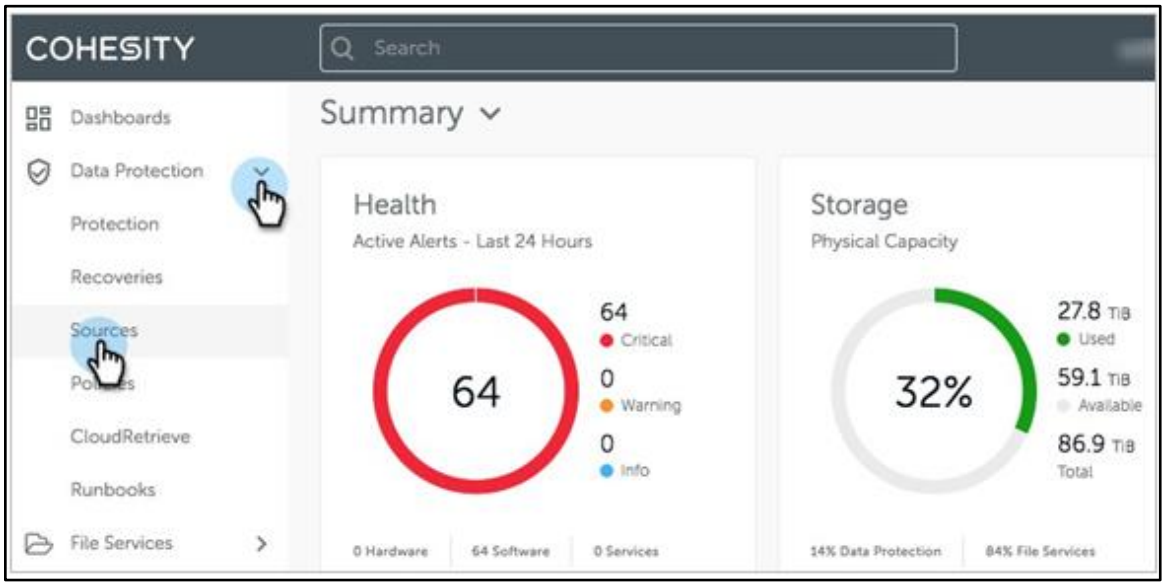
- Ensure that TCP/UDP ports 111, 635, 2049, and 445 are open in the firewall between Cohesity and your Generic NAS.

> **NOTE**: Refer to Manage Firewall Ports in the online Help for more information.

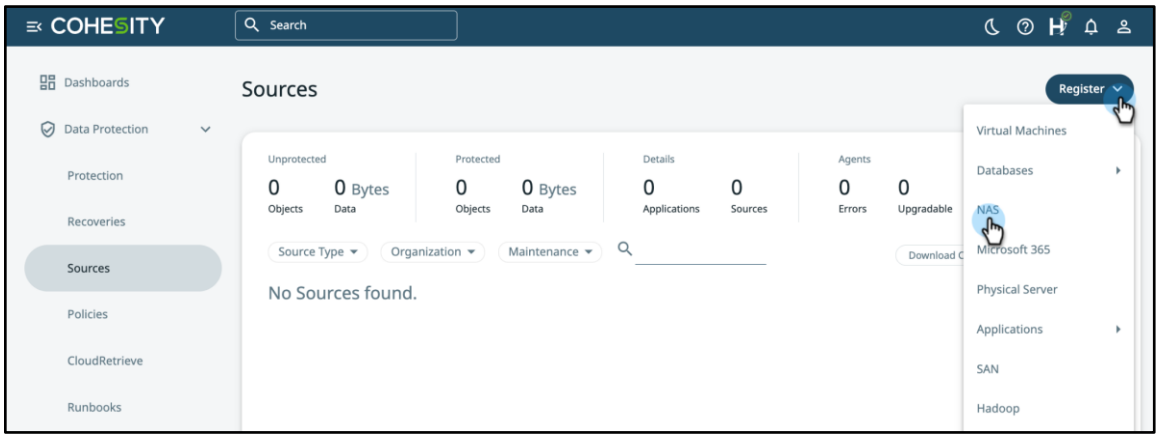
Register Your Generic NAS mount point as a Source in Cohesity

Once the prerequisites are satisfied, you can register your Generic NAS in Cohesity. To do so:

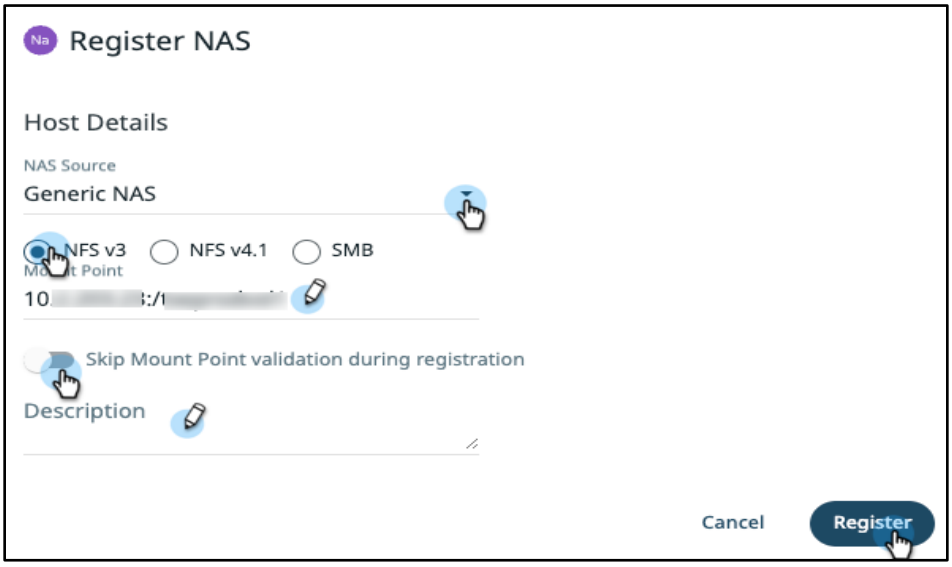
1. Log in to Cohesity and navigate to **Data Protection** > **Sources**.



2. Click **Register** on the top-right of the page and then select **NAS.**



3. In the **Register NAS** form, select NAS source as **Generic NAS**. Enter the NAS registration details (using Table 3 below) and click **Register**.



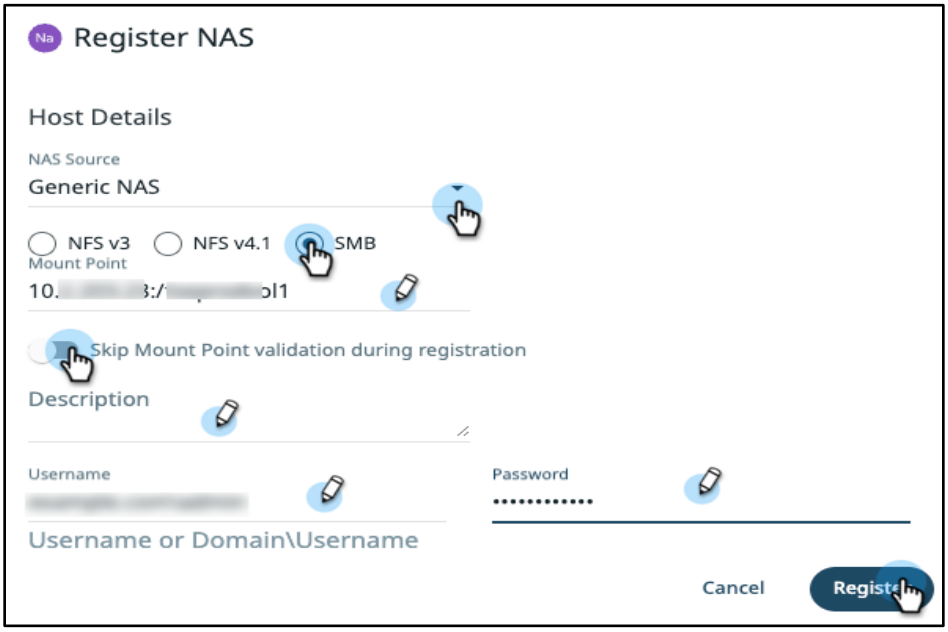


Table 3: Register Generic NAS with Cohesity

FIELD NAME	DESCRIPTION
Mode	NFSv3, NFSv4.1, or SMB
Mount Path	The path for mounting the NAS. Use the following format: • “Hostname or IP:/Volume" for NFS mode • "\\Hostname or IP\Share" for SMB mode. **NOTE:** Do not edit an existing mount path. To change the mount path, perform the following: • Register the new mount path Source. • Edit any Protection Group to remove the old mount path and add the new mount path. • Unregister the old mount path Source.
Password	Password for the provided username.
Skip Mount Point validation during registration	The option to skip the mount point validation during registration. The following will be skipped: • for NFS mount point, mounting the volumes that have been tested whether the mount point exists and is reachable from the Cohesity cluster. • for SMB mount point, establishing a connection with the sources and consequently querying some basic information of the share (like size).
Description	An optional description for the mount point.
Username	SMB mount credentials that allow the reading and backing up of files. If you are providing a domain user account, then you must specify the user name in the following format: **fully_qualified_domain_name\username. For example, xydc.local\user1**
Password	SMB mount credentials that allow the reading and backing up of files.

See Register or Edit NAS in the online Help for more.

Your Generic NAS mount is now a registered source on Cohesity. To protect it, Create a Cohesity Protection Group below.

NOTE: Every NFS mount point or SMB share that needs to be backed-up should be registered as an individual Generic NAS source.

Choose a Cohesity Protection Policy

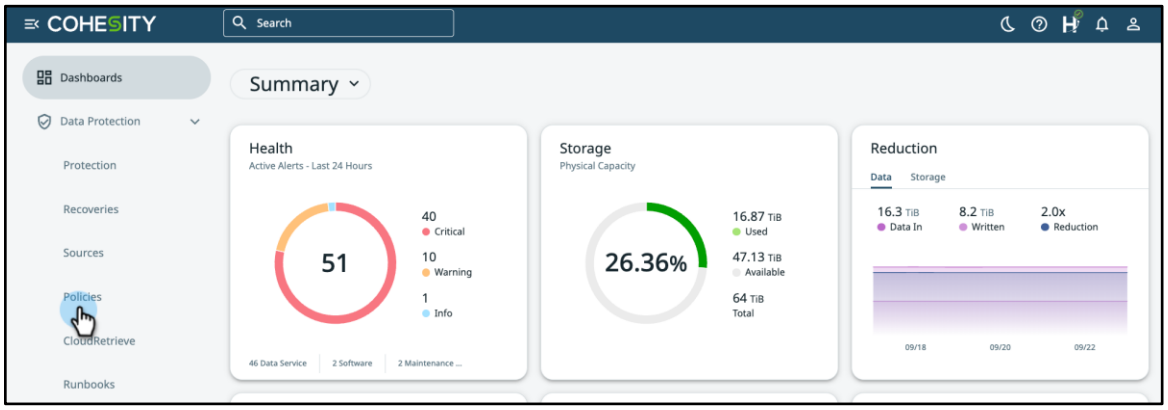
In Cohesity, Protection Groups use Protection Policies. Protection Policies reflect business needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs), while a Protection Group defines operational requirements, such as which source objects to protect, the Protection Policy to use, and operational considerations like indexing, exclusions and inclusions, alerts, app consistency, and more. This process of combining business needs (Policy) with the objects to protect (source data) and the operational requirements (Group) provides rich flexibility to customers.

Cohesity includes three standard policies: Gold, Silver, and Bronze. For their default settings, see Manage Policies in the online Help. If an existing policy meets your needs, you can proceed directly to Create a Cohesity Protection Group next. If the existing Policies do not meet your needs, you can create a custom Policy.

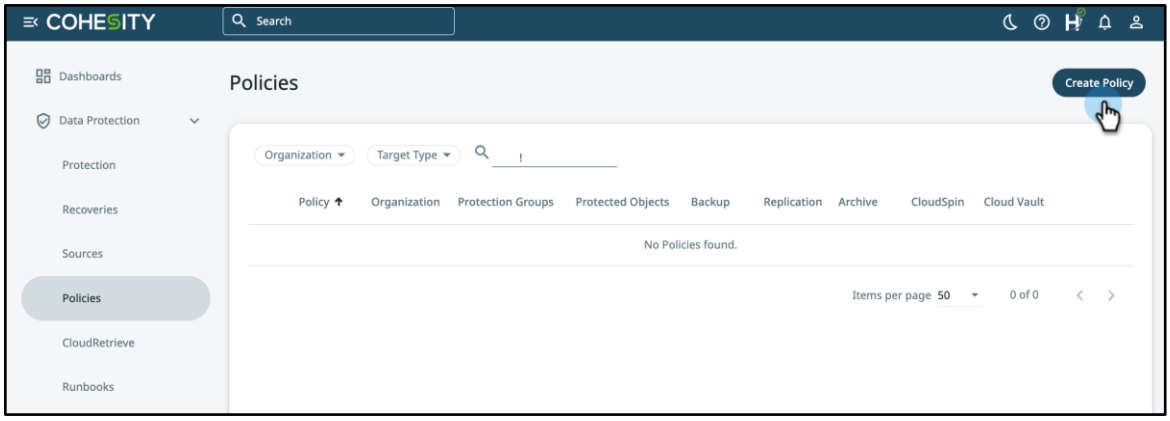
NOTE: See our recommendations for protecting Generic NAS data in Best Practices below.

To create a custom Protection Policy:

1. Log in to Cohesity and navigate to **Data Protection** > **Policies**.

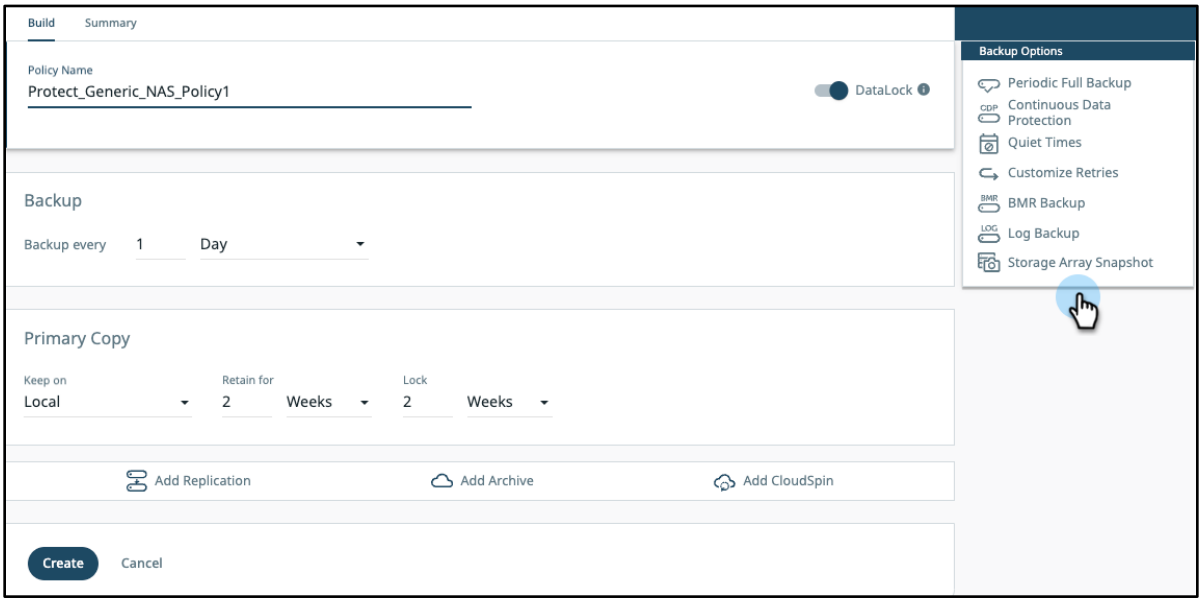


2. Click **Create Policy** located at the top right of the page.

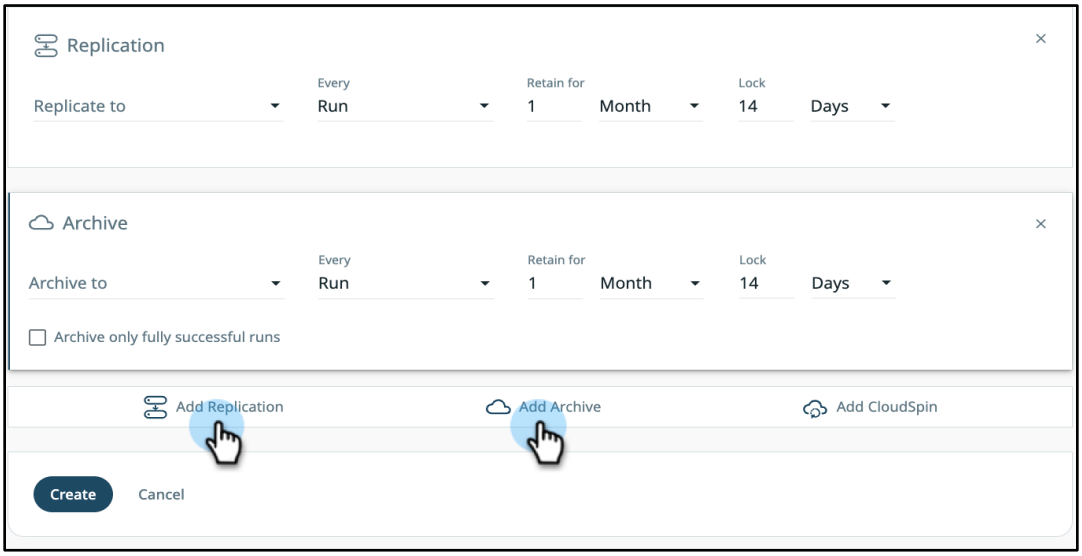


3. In the **Create Protection Policy** form, enter a **Policy Name** and select the backup interval and retention times for the **Scheduled Backup**. Click **More Options** to configure the advanced settings.

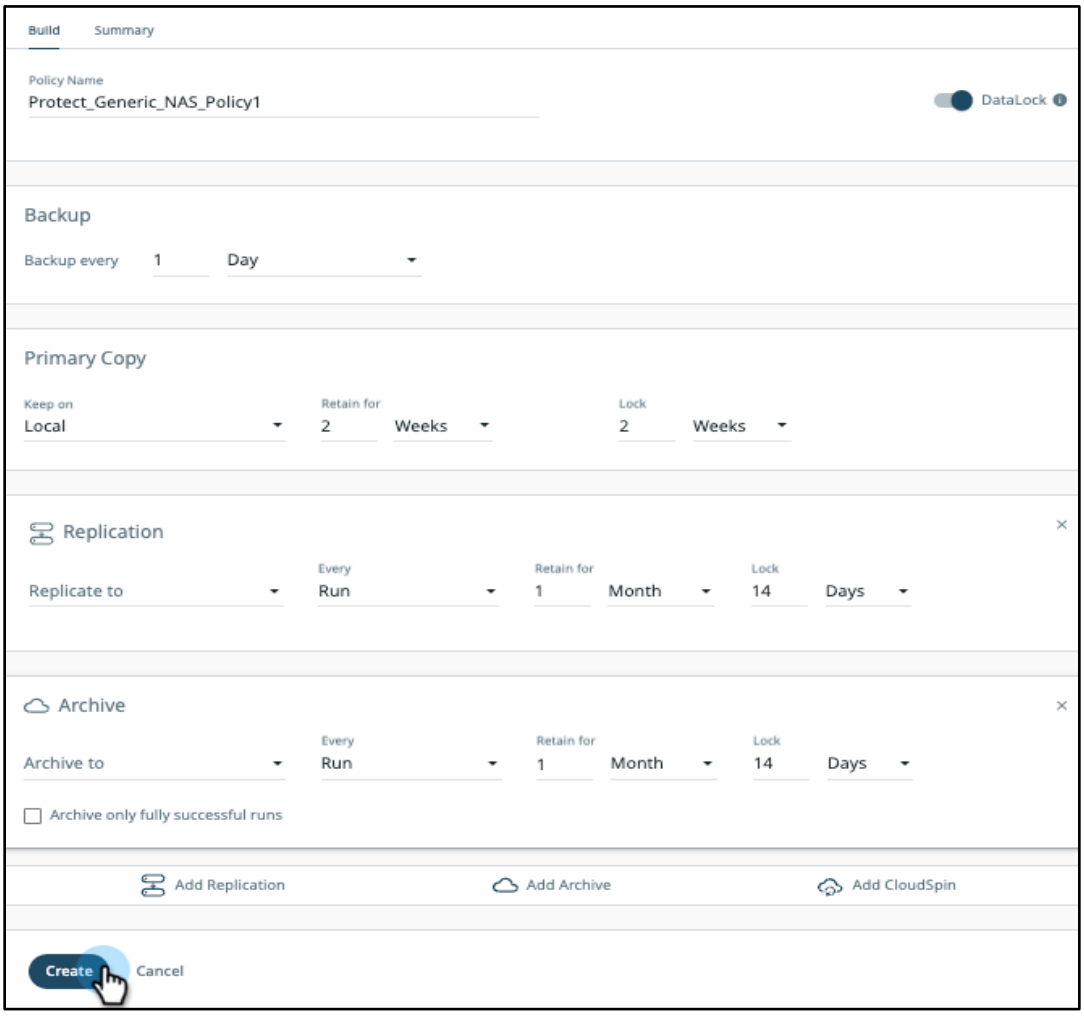
4. In the **Create Protection Policy** form, you can edit the **Retry Options**. If required, from the floating menu on the right, you can add **Periodic Full Backup**, **Define Quiet Times**, and more. When you do, you can configure the options for each as you add them.



5. If required, add **Replication** or **Archive** for your backed up Generic NAS data from the menu on the bottom and configure the options.



6. When you're done, click the **Create** button**.**



NOTE: **DataLock** in this form is enabled by default which helps prevent protected data from being modified or deleted until the DataLock expires. For more, see Create or Edit a Standard Policy in the online Help.

You can also add a Legal Hold, which behaves differently from a DataLock, to a specific Protection Run (a snapshot) to preserve it for legal reasons. See Add or Remove a Legal Hold to a Snapshot in the online Help.

Your custom Protection Policy can now be used in Protection Groups.

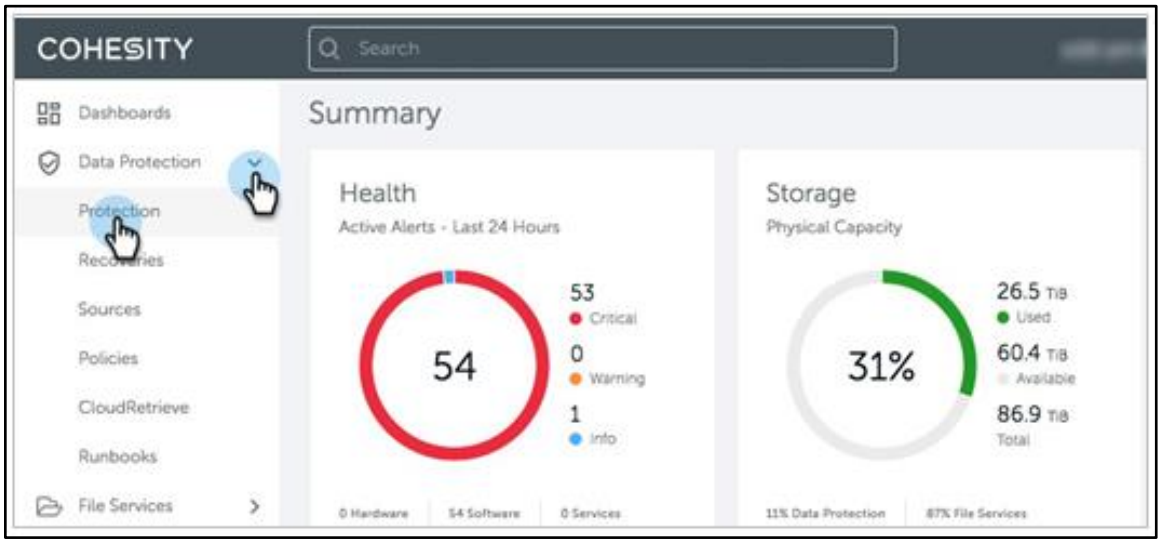
For the complete list of Protection Policy parameters, see Create or Edit a Standard Policy in the online Help.

Create a Cohesity Protection Group

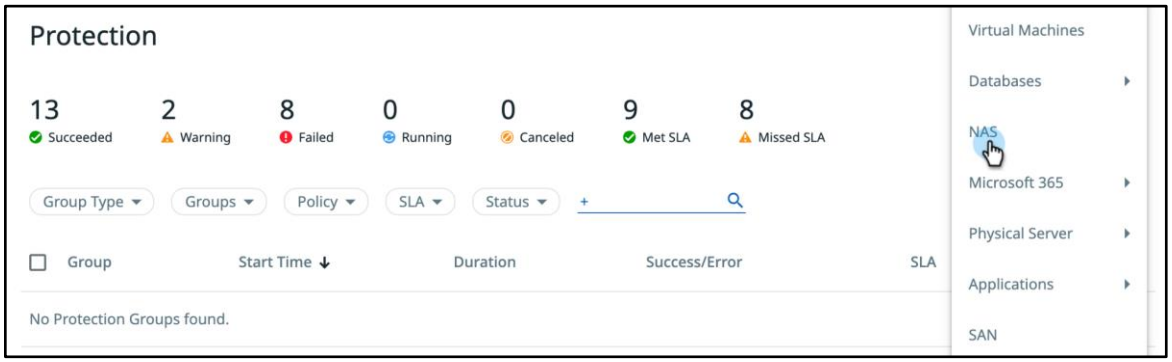
Protection Groups combine operational requirements such as which objects to protect, indexing, alerts, exclusions, inclusions, etc., with the business requirements that are defined in a Protection Policy.

Multiple Protection Groups can use the same Protection Policy, but each Group can have only one Policy. To create a Protection Group:

1. Log in to Cohesity and navigate to **Data Protection** > **Protection**.

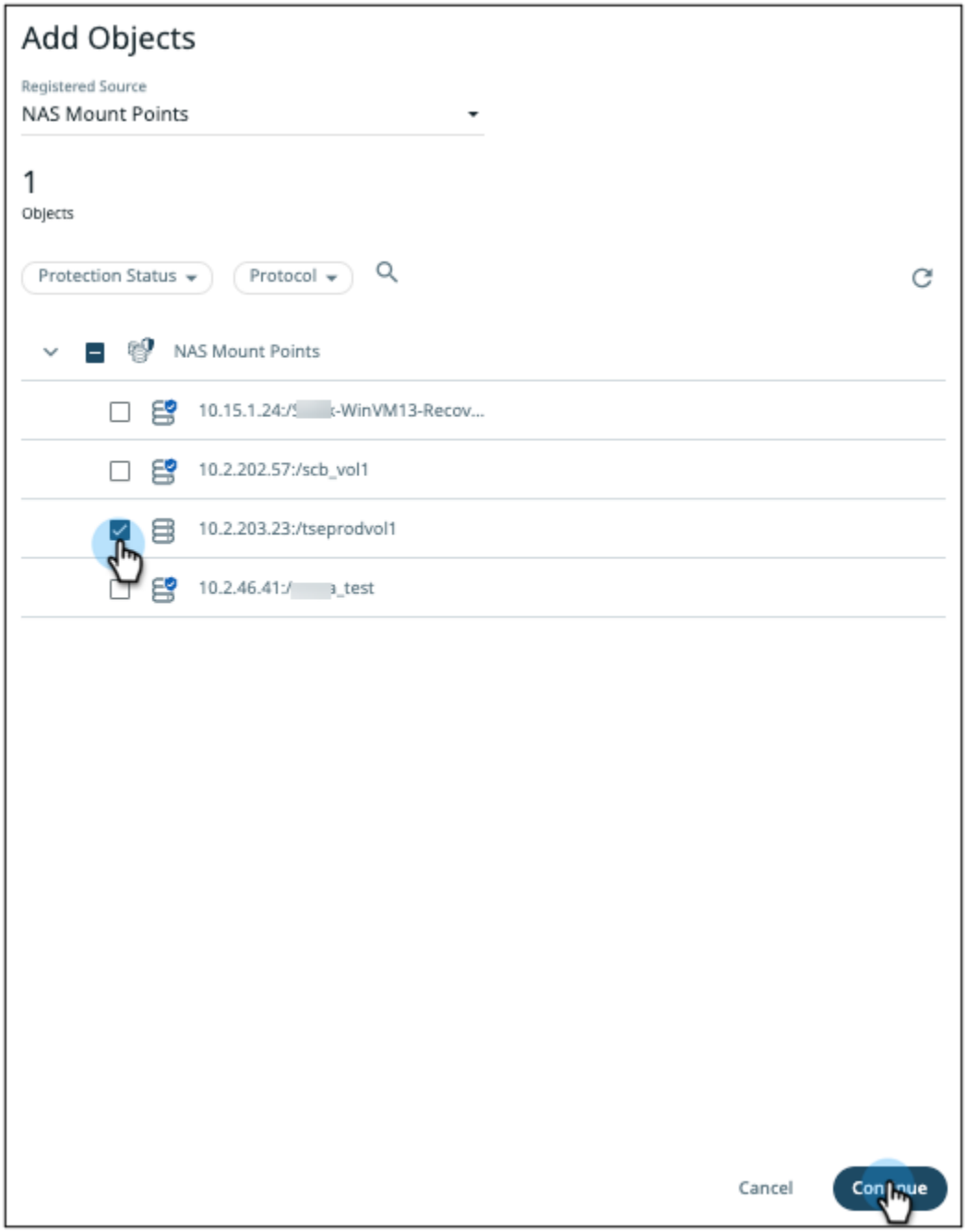


2. Click **Protect** on the top-right of the page and then select **NAS**.

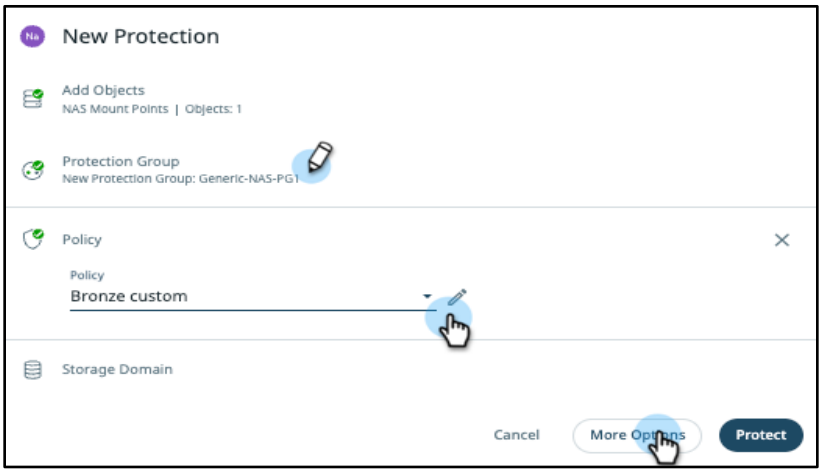


3. In the **New Protection** form, under **Source**, select the Generic NAS mount you registered earlier, select the objects you wish to protect, and then click **Continue**.

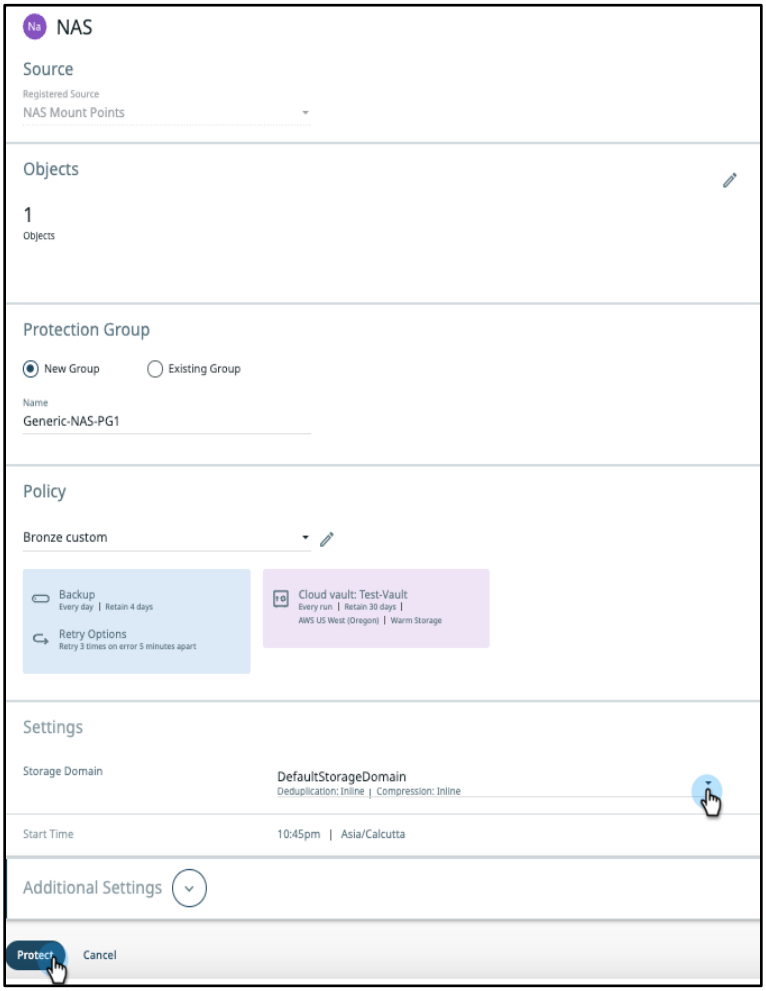
> **NOTE**: If you want to stream your data directly to lower-cost storage on an External Target without storing a local backup, then enable CloudArchive Direct. See Archive Your Data Directly with Cohesity CloudArchive Direct for details.



4. Enter a **Group Name** and select the Policy you chose earlier. Click **More Options.**



5. Select a **Storage Domain** and click **Protect**.



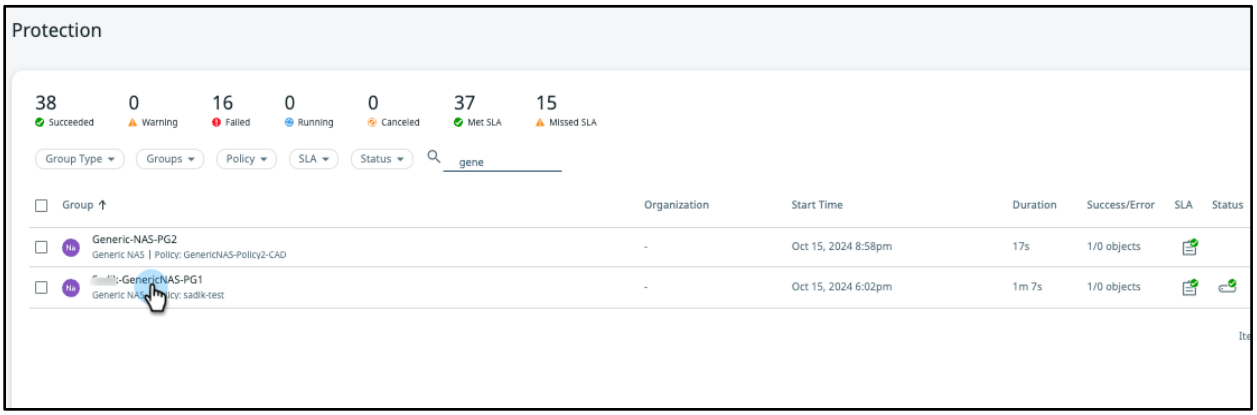
Your new Protection Group is now active and running.

For more details, including the **Additional Settings** in a Protection Group, see Add a Protection Group to Protect NAS Volumes in the online Help. For best performance, see Best Practices for Protecting Generic NAS.

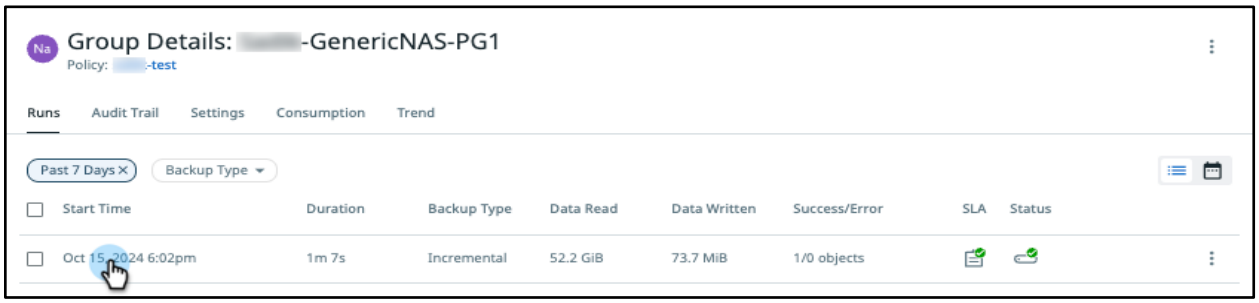
Check the Status of Your Protection Group

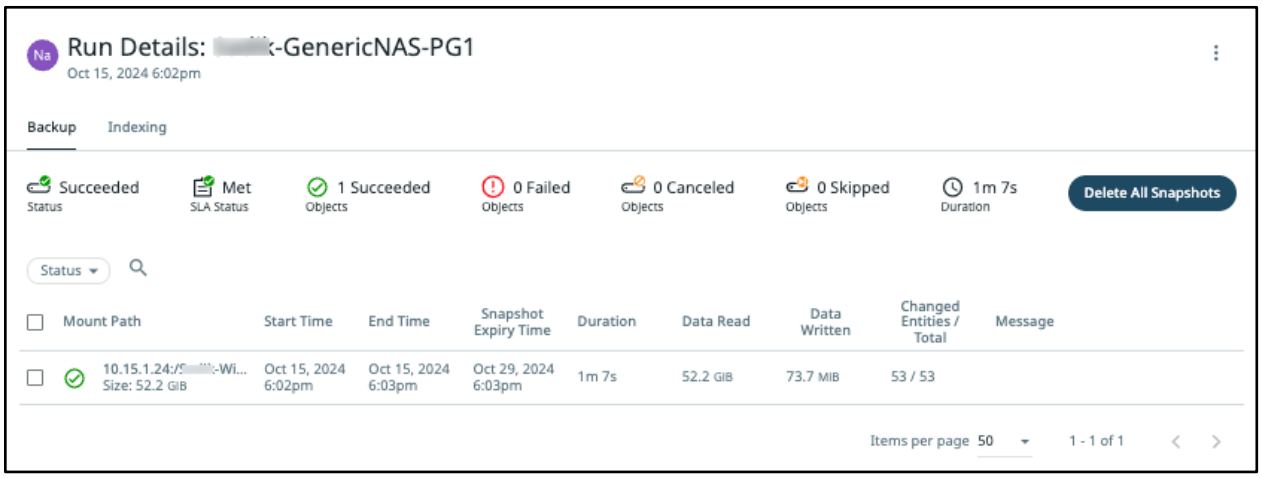
To check the status of the Protection Group and progress on its Protection Runs:

1. Navigate to **Data Protection** > **Protection**.
2. Enter a search term to find the Protection Group and check the **Status** column in that row to see its status details.
3. Click the Protection Group name to view the Job runs**.**



4. Select and click the Job Run to view the Backup and Indexing details.





Understand Cohesity's Generic NAS Recovery Approach

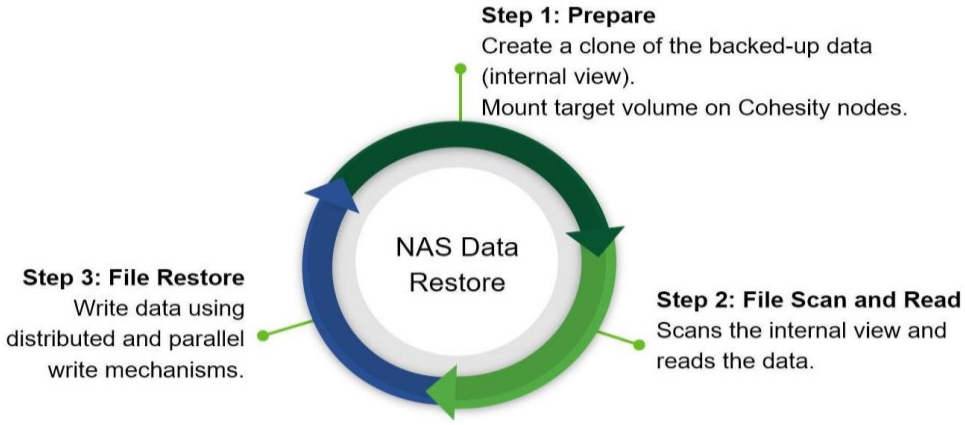
Generic NAS data recovery is essentially the rebuilding of NAS data that is lost due to unfortunate incidents such as media or storage failure, application failure, data corruption due to power interruption, or data deletion due to human errors. Cohesity DataProtect offers efficient data recovery options by protecting your data in backups and allowing you to instantly recover it whenever necessary, with uncompromised data availability and reduced downtimes.

Cohesity DataProtect recovers Generic NAS data from snapshots of storage volumes created earlier by a Protection Group. Restoring data for Generic NAS using Cohesity DataProtect is simple, fast, and intuitive. Recovery can be performed at various levels of granularity, including at the Files/Folders and Volume levels. You can recover NAS volumes and files & folders to their original location or to a newly specified location, which can be in the original source or a different NAS source. You can also perform an instant mount of your backup and download files from specific snapshots that were created by a Cohesity Protection Group.

Cohesity NAS Recovery Internal Workflow

Once a NAS is backed up with Cohesity DataProtect, you can start a recovery task that restores specific Generic NAS volumes or files as per your business requirements. During the recovery task run, Cohesity DataProtect executes multiple operations in the background to complete the recovery successfully.

Figure 9: NAS Recovery Internal Workflow



In Cohesity's NAS restore internal sequence, Cohesity DataProtect executes:

1. **Prepare**: Creates a clone of the data (an internal view) that needs to be recovered and mounts the target volume on the Cohesity nodes.
2. **File Scan and File Read**: Performs a file scan on the cloned internal view and reads the data.
3. **File Restore**: Performs writes on the target in batches, using distributed and parallel write mechanisms.

See Appendix A: Restore Write Behavior for more details on recovery operations.

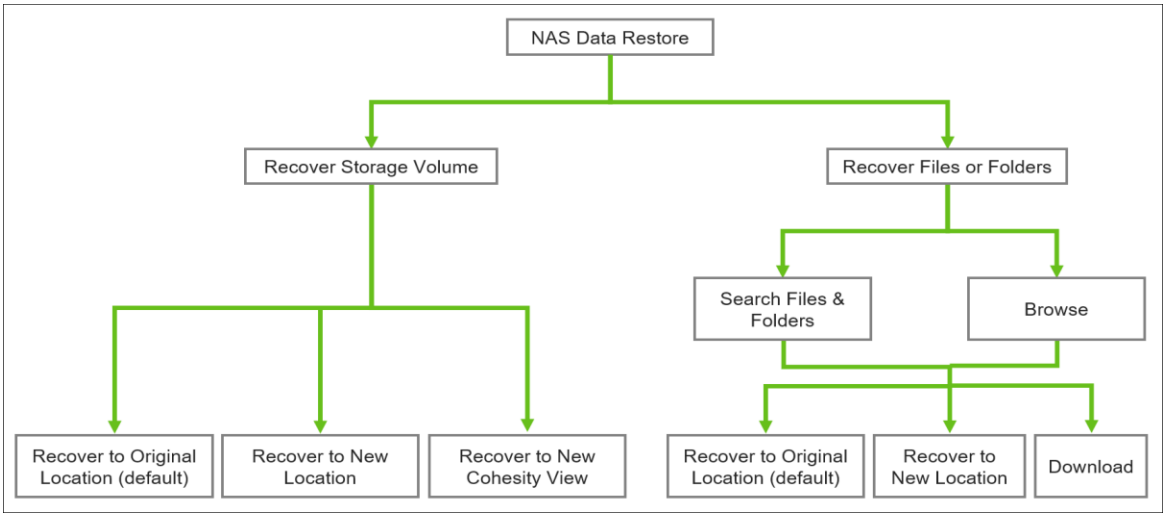
Recover Generic NAS Data with Cohesity DataProtect

Cohesity DataProtect offers two levels of recovery granularity for Generic NAS data:

- Recover Storage Volume
- Recover Files or Folders

In each case, you can search for the specific data you need and choose how and where to recover it. Figure 10 illustrates the phases and choices you encounter in a typical NAS data restore workflow.

Figure 10: NAS Data Recovery Decision Tree



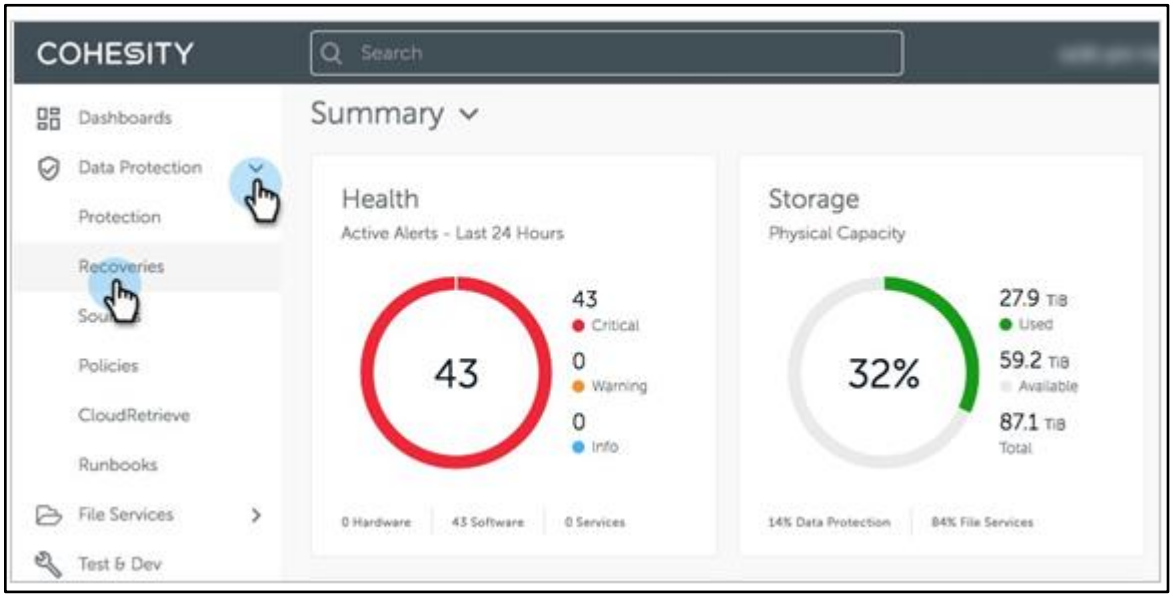
Recover Storage Volume

Cohesity DataProtect's Recover Storage Volume capability allows IT administrators to select and restore specific shares from any previous backup. With this feature, you can also instantly mount Generic NAS shares as Cohesity Views on any Linux or Windows system with access to Cohesity DataProtect.

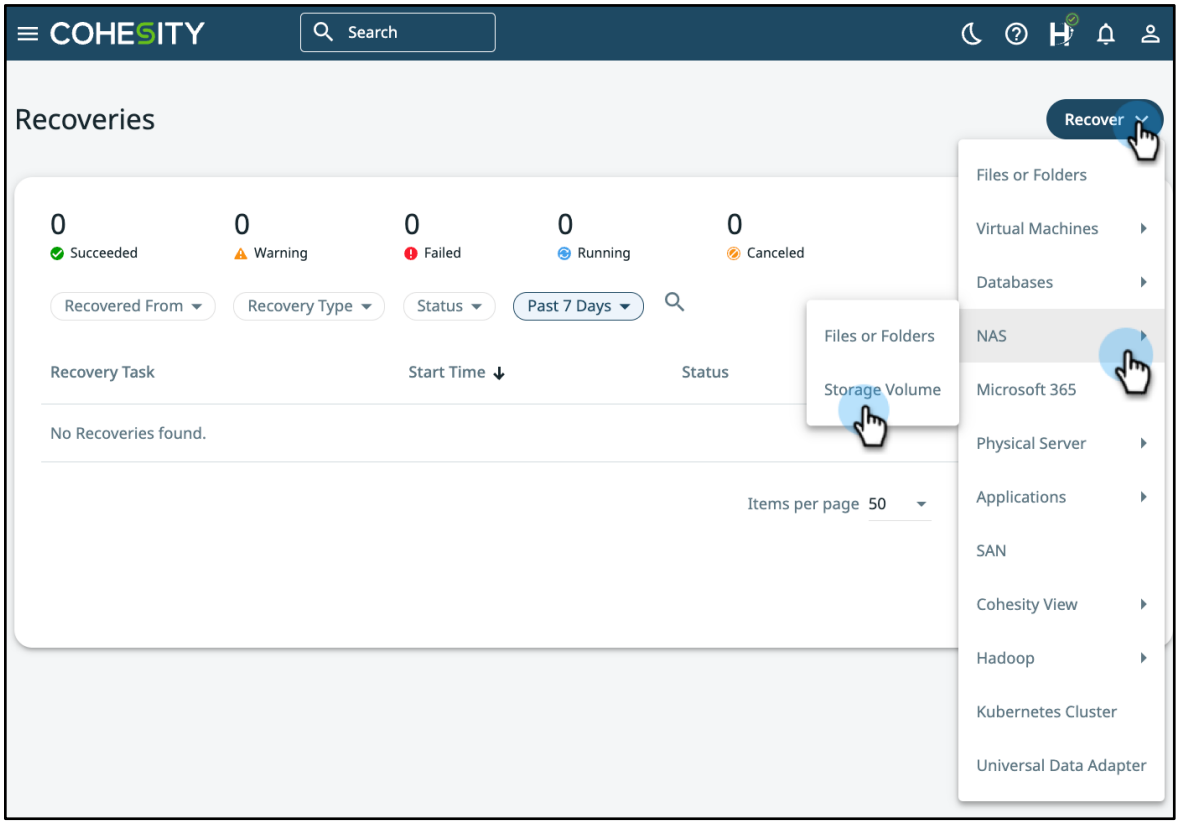
NOTE: Before recovering storage volumes, ensure that snapshots of those volumes exist in the Protection Groups on your Cohesity cluster.

To recover a Generic NAS storage volume:

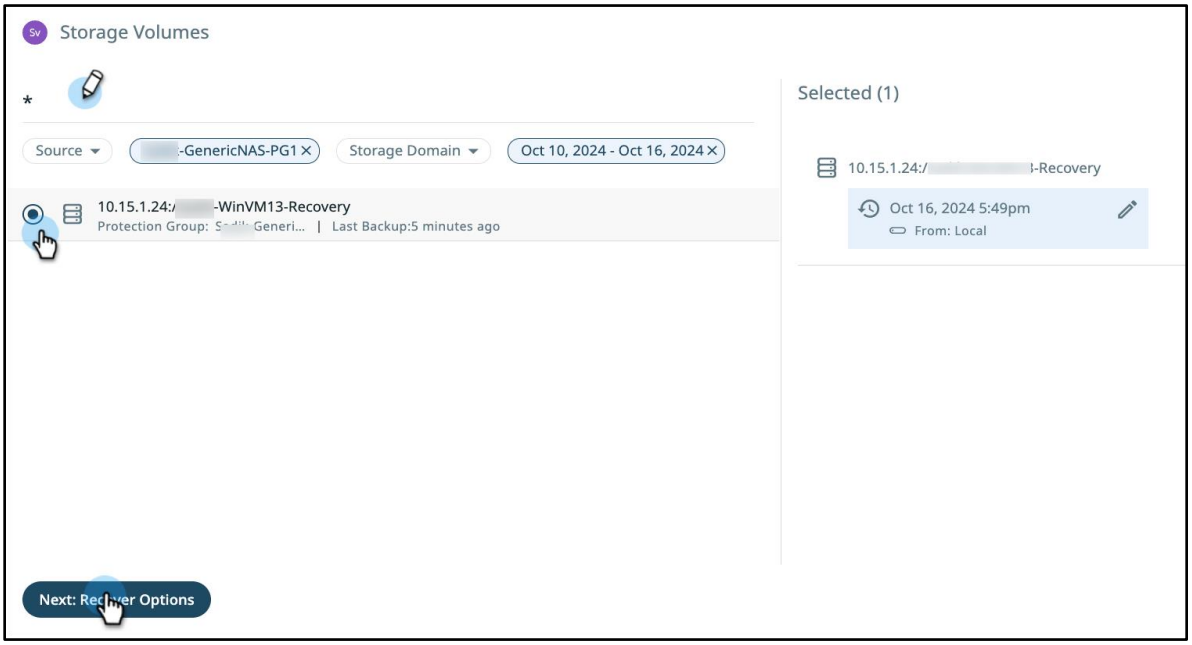
1. Log in to Cohesity and navigate to **Data Protection** > **Recoveries**.



2. On the Recoveries page, click the **Recover** button and select **Storage Volume** under NAS.



3. Under **Storage Volumes**, enter a search query for the volume you want to recover, click the desired volume in the results, then click **Next: Recover Options**.



NOTE: Cohesity DataProtect supports wildcard characters and search filters to simplify the management and recovery of Generic NAS volumes.

4. Set the **New Recovery** options.
   a. Select the **Snapshot**. By default, the **Latest** snapshot of the volume is selected. To select a different recovery point, click the **Edit** pencil icon on the right and select the required snapshot from the Recovery Point **Timeline** or **List** view.
   b. Select the **Recover To** target. Choose one of three restore destinations:
      - Original Location
      - New Location
      - New Cohesity View
   c. If you choose to recover to a new Cohesity View, you can change the default **Name** of the recovery View and choose a QoS Policy. (If you choose the Original Location or New Location, see below.)
   d. Under **Cluster Interface**, select **Auto Select** or click the field to manually enter the interface group name.
   e. You can also click the **Task Name** to replace the automatic recovery task name, if necessary.

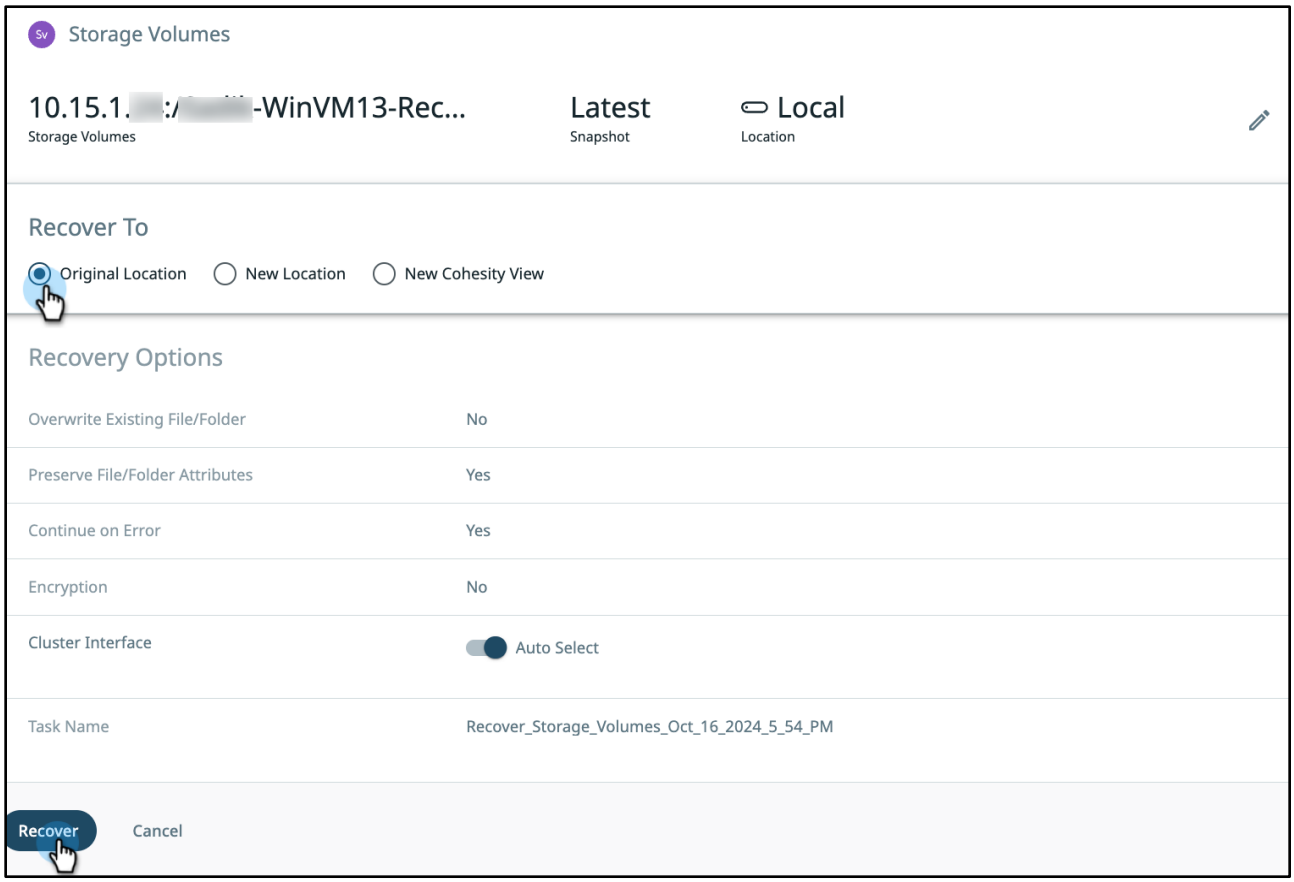
f. Finally, click **Recover**.

Recover to Original Location (Default)

If your data becomes unavailable or is lost from the source from which it has been backed up but your original source infrastructure is still functional, you can recover it to your original NAS location (target) with this option.

NOTE: Data is recovered along with metadata, including ACLs.

To recover a Generic NAS volume to its original NAS target, select **Original Location**. Edit the **Recovery Options** as necessary and click **Recover**.



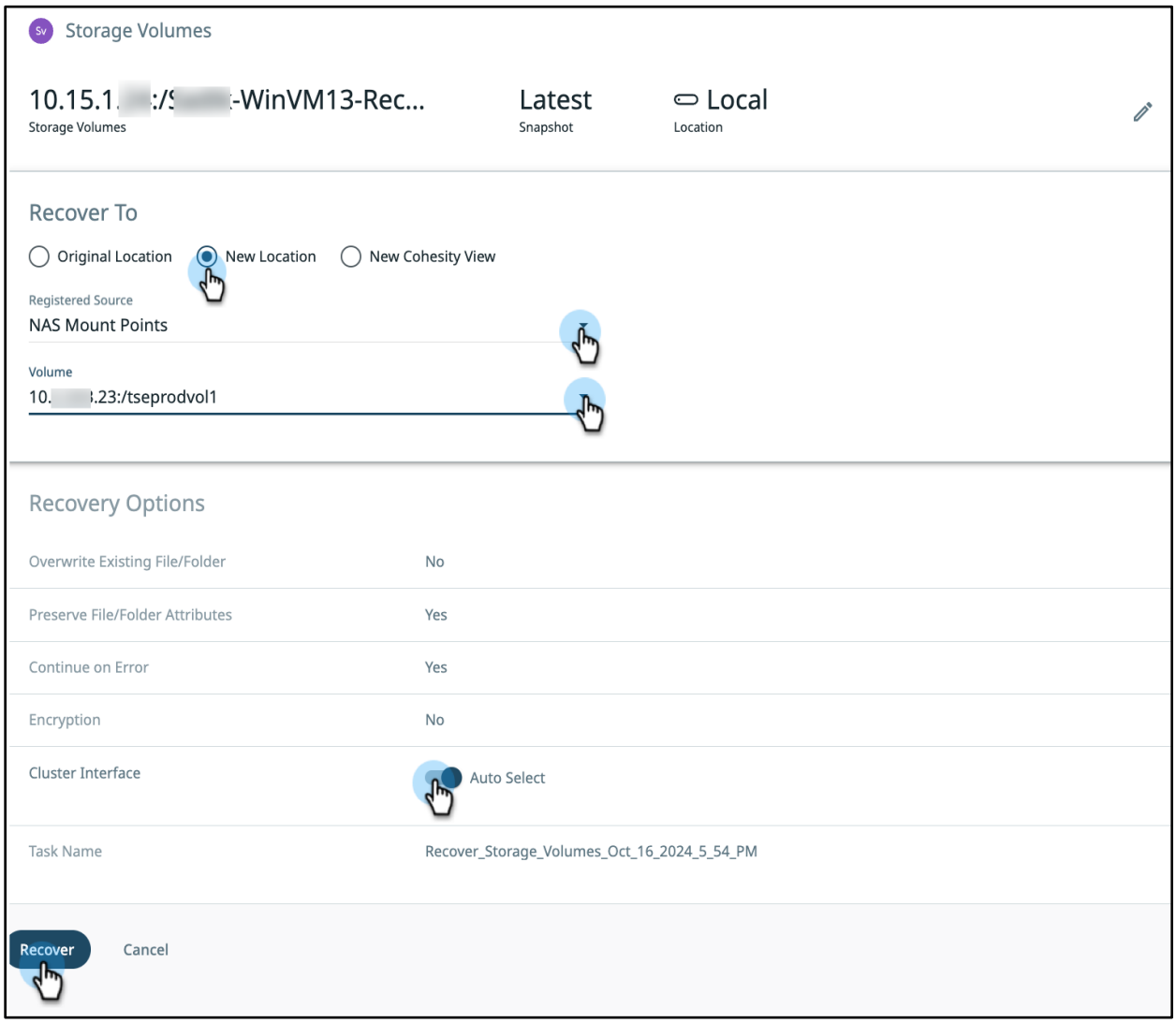
Refer to Recover Storage Volumes to the Original Location in the online Help for details on the Recovery Options.

Recover to a New Location

If some of your source data becomes unavailable or you need to migrate it, you can recover it to a new location. With this option, you can restore your original NAS data easily and quickly to different NAS locations in the same sources, or in different sources like NetApp, Dell EMC, or any generic NAS.

NOTE: The target NAS mount point must be registered as a Generic NAS source in Cohesity.

To recover a Generic NAS volume to a new NAS target, select **New Location** and select a **Registered Source** and **Volume**. Edit the **Recovery Options** as necessary and click **Recover**.



See Recover Storage Volumes to a New Location in the online Help for details on the **Recovery Options**.

Recover to a New Cohesity View

This option gives you the flexibility to repurpose the backup data without delay and disruption. You can instantly create dev/test environments from a backup on demand, because recovering to a Cohesity View doesn't require the data to be written to a location. When recovering to a Cohesity View, Cohesity clones the selected backup to a new View within the Cohesity cluster and provides you instant access to it.

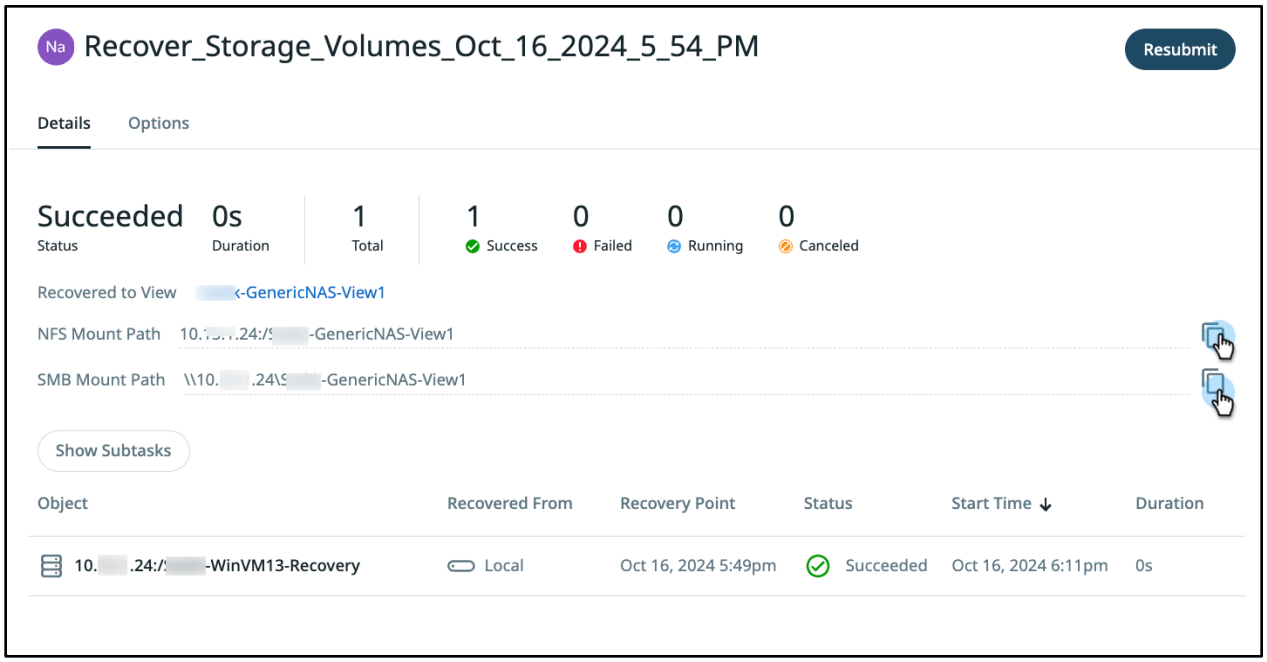
To recover the Generic NAS volume to a Cohesity View, select **New Cohesity View**, edit the automatically assigned **Name** for the new View if necessary, and select the QoS Policy that is most appropriate for the workload. Edit the **Recovery Options** as necessary and click **Start Recovery**.

NOTE:

- Refer to QoS Policies in the online Help for more about Quality of Service policy settings and their use cases.
- Refer to Recover Storage Volumes as a Cohesity View in the online Help for details on the **Recovery Options**.

Once recovery is complete, mount the View to a system of your choice to start using it. To locate the mount point information, navigate to **Data Protection** > **Recoveries** and click the completed recovery task to view its results page. From there, you can copy the **NFS Mount Path** for NFS systems and **SMB Mount Path** for Windows systems.

Figure 11: Retrieve NFS & SMB Paths to Recovered View



Recover Files or Folders

Cohesity DataProtect's *Recover Files or Folders* capability allows IT administrators to search and recover specific files and whole folders from any previous backup.

This feature also allows you to restore the files or folders to their original location or to a newly specified location, which can be within the original source or a different one, without losing the original permissions and attributes. You can also download specific files and folders directly from any snapshot that a Cohesity Protection Group created.

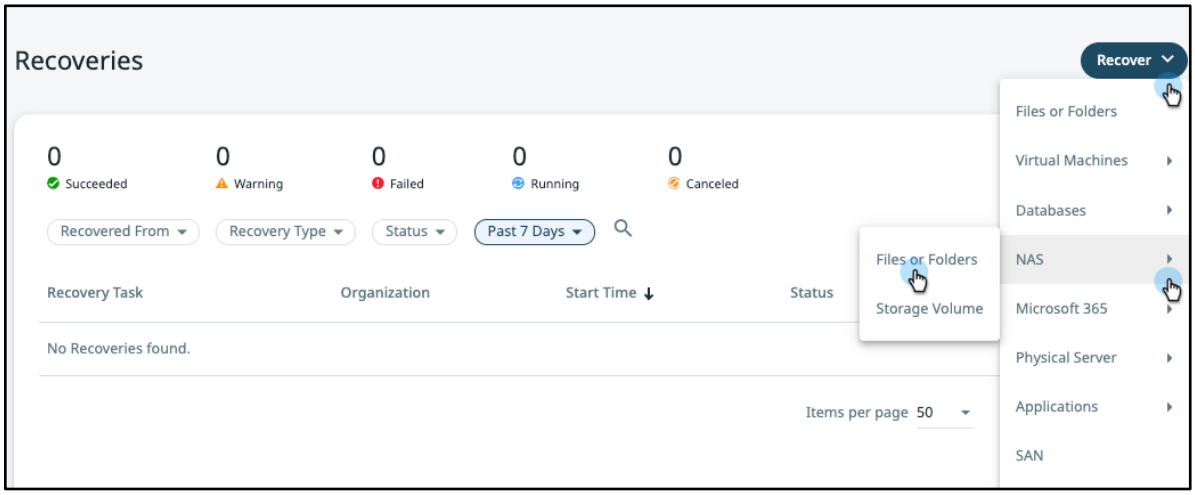
NOTE: Before you try to recover files or folders, ensure that snapshots of these files and folders appear on the Cohesity cluster in a Protection Group.

To recover files and folders from Generic NAS backups:

1. Log in to Cohesity and navigate to **Data Protection** > **Recoveries**.

> **NOTE**: For backed-up SMB volumes, the user account must have full control over the target, as Cohesity DataProtect uses that user account to perform recovery.

2. On the **Recoveries** page, click the **Recover** button and select **Files or Folders** under NAS.



3. Select **Files and Folders** or Browse and enter the search query for the files and folders you need to recover.

> **NOTE**: You can also use the wildcard character ***** or narrow the search results by specifying filter criteria. For example, you can filter the search results by a specific Protection Group. Click one or more of the filter types to narrow your search.

The next steps in the procedure depend on the type of search you select.

- To search by file or path name, see Search Files and Folders next.
- To browse or enter the path, see Browse below.

Search Files and Folders

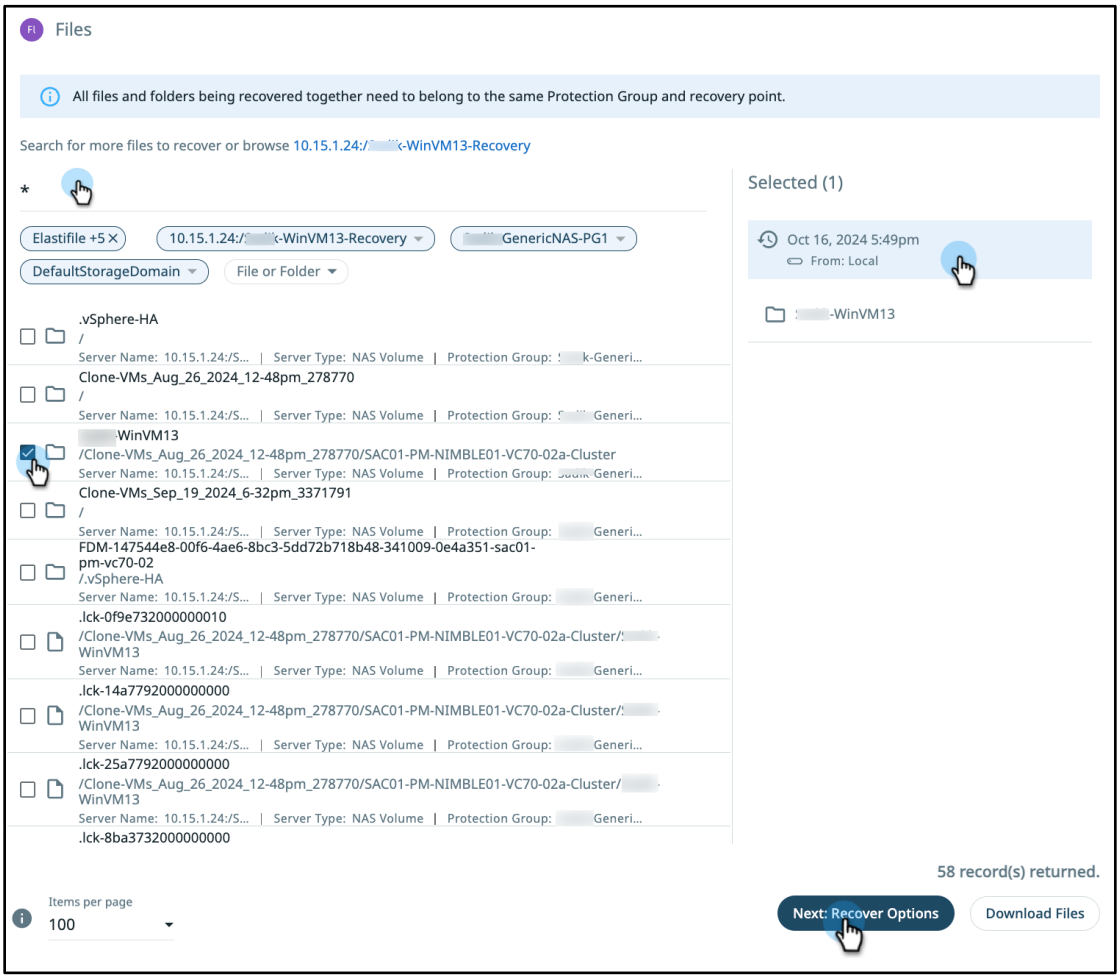
The Files or Folders search option allows you to search and recover files using file or folder names from any backup available on Cohesity.

NOTE:

- To be able to use this search option, you need to enable indexing for the Protection Group. This ensures backup metadata is indexed and allows Google-like search, enabling instant granular file-level recovery to any point in time across billions of files.
- To enable indexing, see Appendix B: Index for Faster Granular-level Recovery.

To search for files and folders:

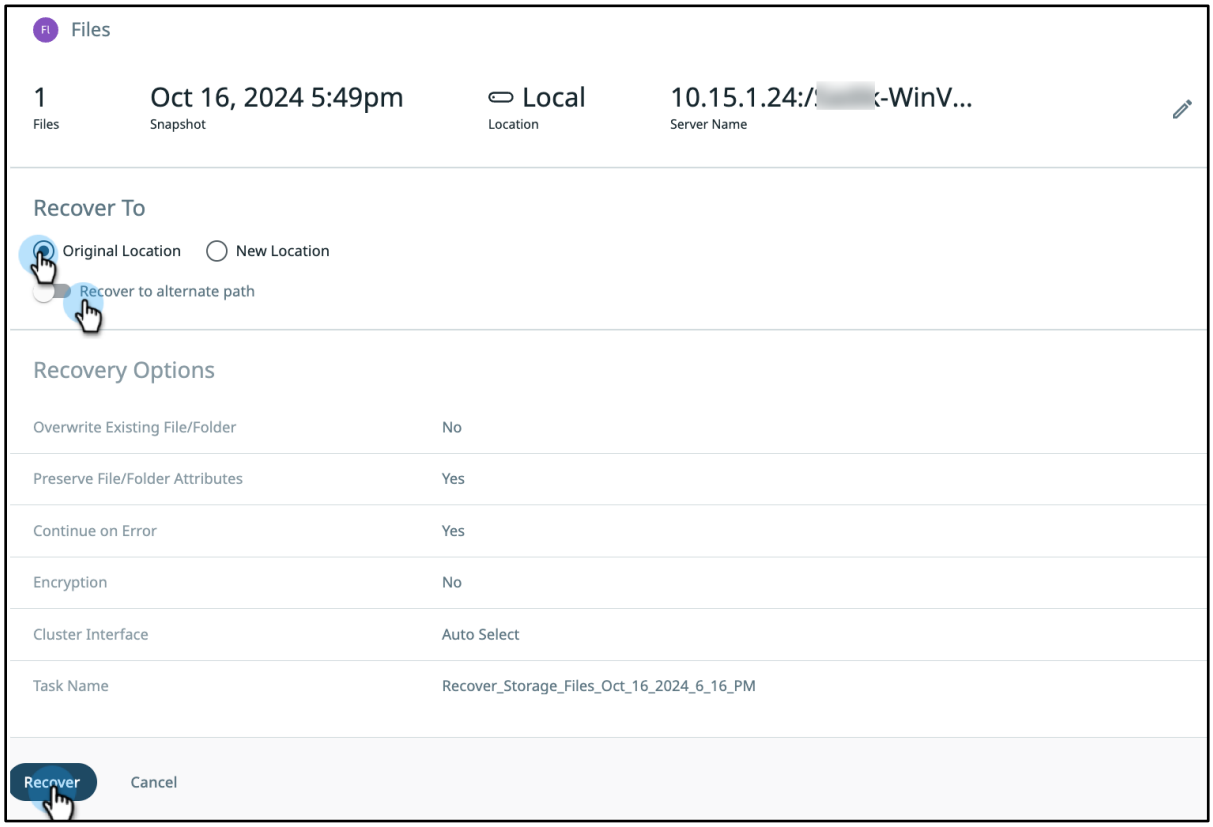
1. Enter the full or partial file name or path and select the file from the search results. By default, the latest snapshot is selected. To recover from a different recovery point, click the **Edit** pencil icon in the right pane under **Selected** and choose the snapshot you need.



NOTE: Deleted snapshots might be displayed as valid recovery points for a brief period after deletion, until they are removed from the search index by a background process.

2. Click one of the buttons at the bottom:

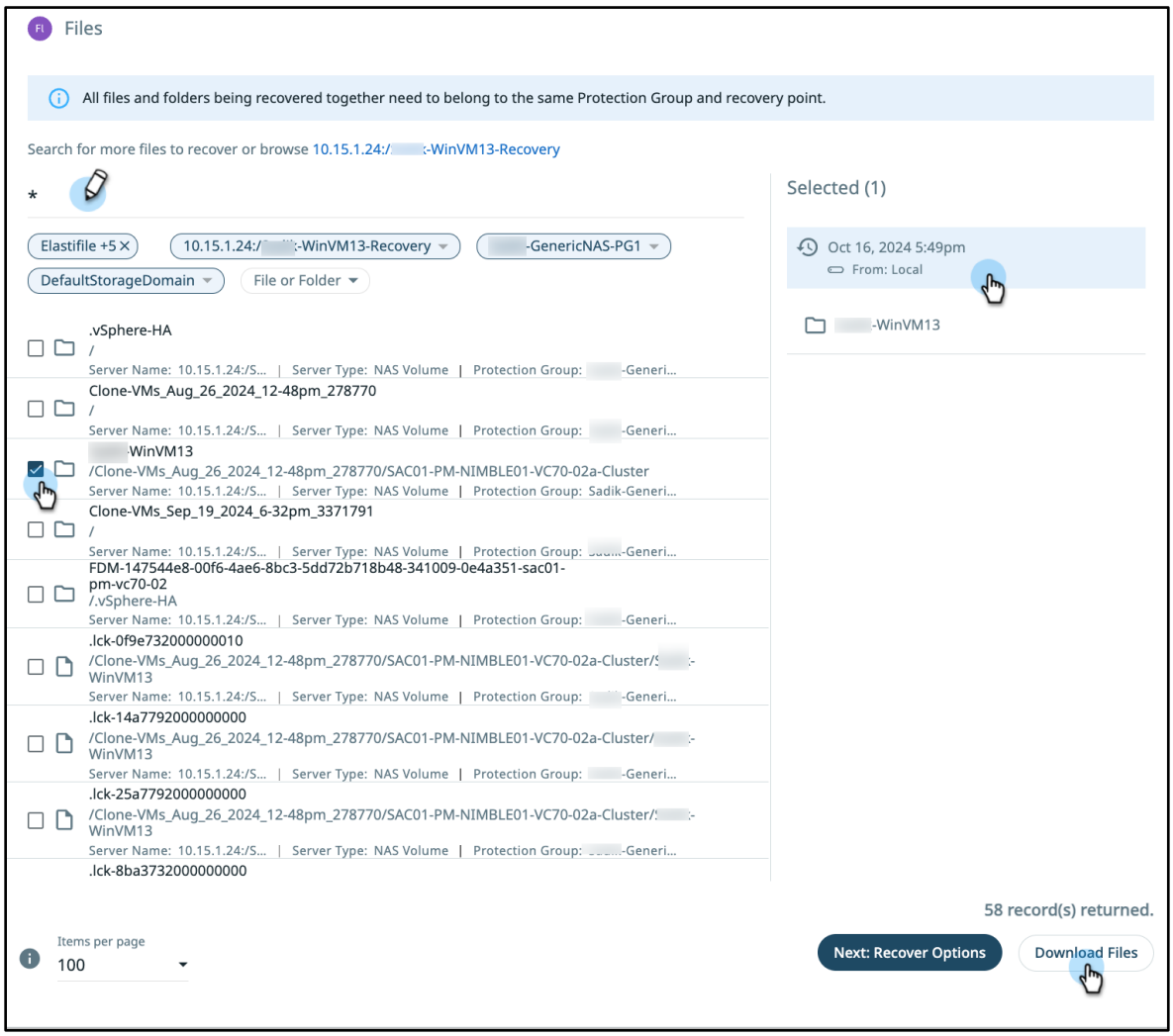
   a. Next: **Recover Options**. On the Files page, select Original Location or enter a New Location and click Recover.



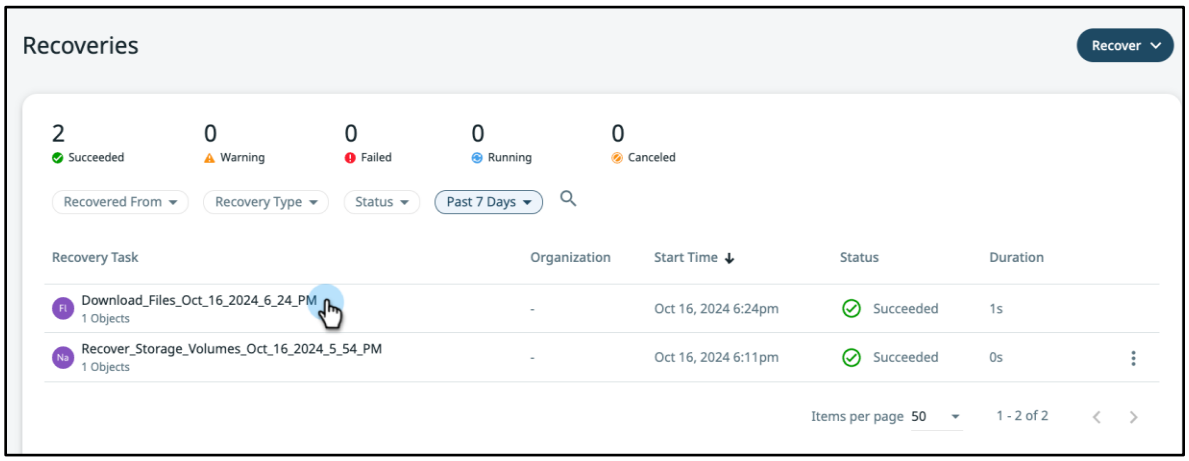
NOTE:

- To recover files or folders to an alternate path in the original NAS source, enable **Recover to alternate path** toggle switch and enter the alternate path.
- For details about the **Recovery Options**, refer to Recover NAS Files or Folders in the online Help.

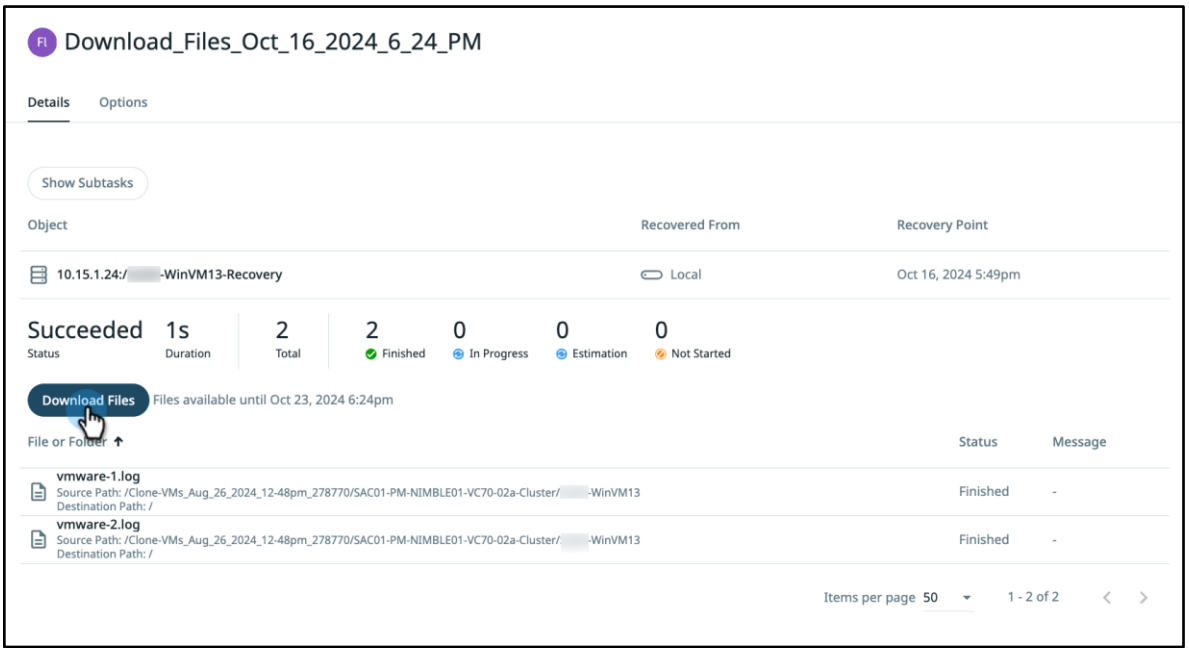
b. **Download Files**. If you are recovering a single file, this option downloads the file to your browser's download folder.



For all other selections, this creates a recovery task. When the task is completed, click the task name.



Click **Download Files** again to download the generated zip file.



For details on Cohesity DataProtect's actions in each file recovery use case, see Appendix A: Restore Write Behavior for more details.

Browse

The **Browse** option allows you to search and recover files using the name of the server or Protection Group from any backup available on Cohesity.

To browse by server or Protection Group name:

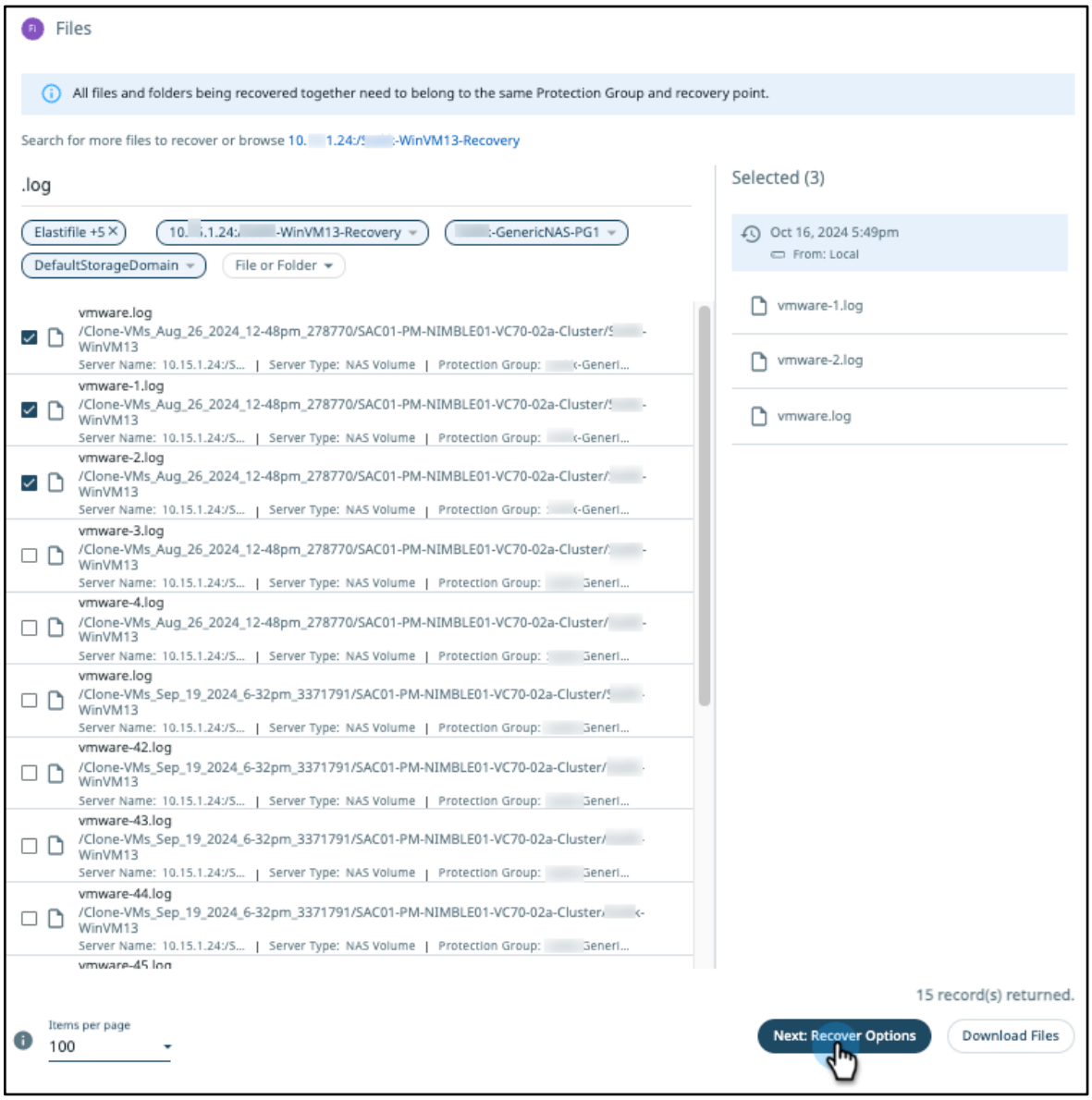
1. In the **Files** form, select **Browse** and enter the full or partial name of the server or Protection Group. Use the **Object Type**, **Source**, **Protection Group**, and/or **Storage Domain** filters to further narrow your results as needed.
2. Find the object that contains the files and folders you want to recover and click **Browse** in that row.

3. By default, the latest snapshot is selected. To recover from a different recovery point, click the selected date range at the top and choose the snapshot you need. Select the files and folders you need and click **Next**.

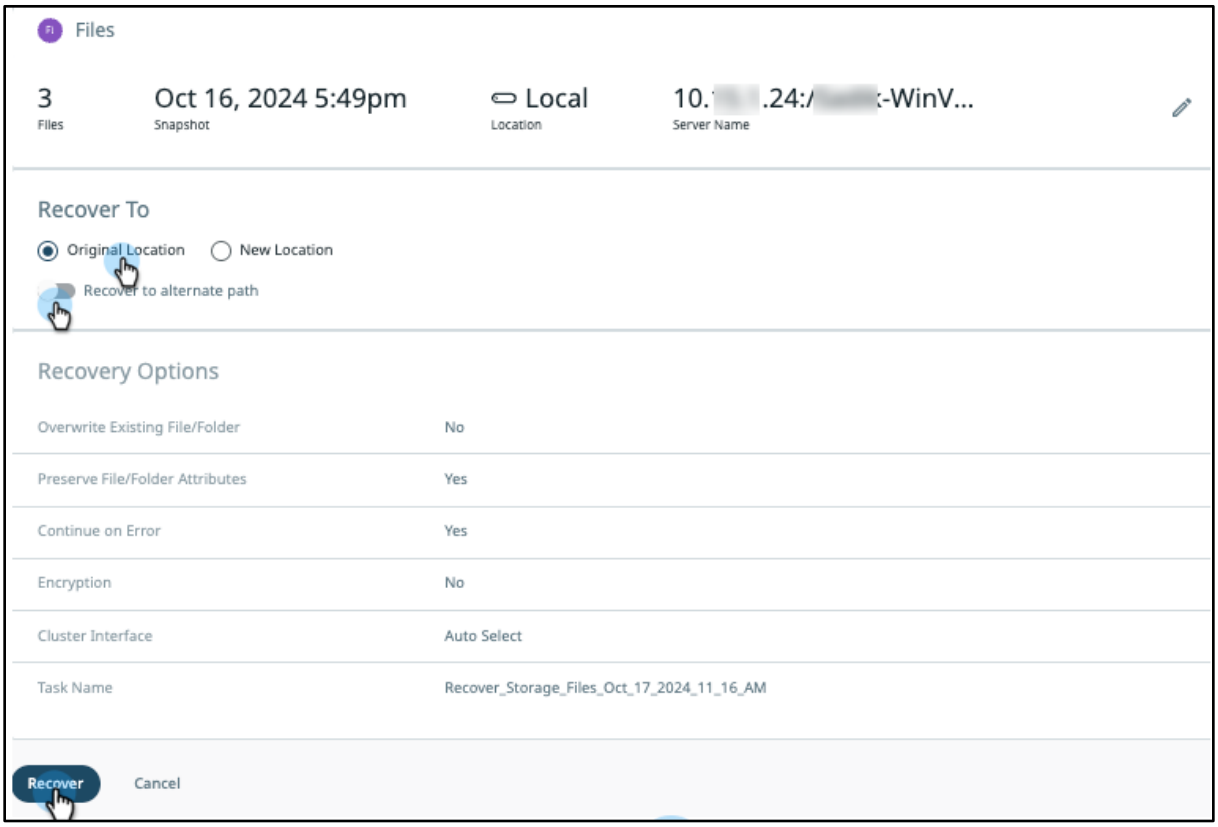
NOTE:

- Deleted snapshots might be displayed as valid recovery points for a brief period until they are removed from the search index by a background process.
- Changing the snapshot when you have already selected items will clear your selections.
- By default, only the files and folders that are indexed are displayed. To display all the available files and folders, disable Browse on Indexed Data at the top.

4. Select the files and folders to recover and click on **Recover Options.**



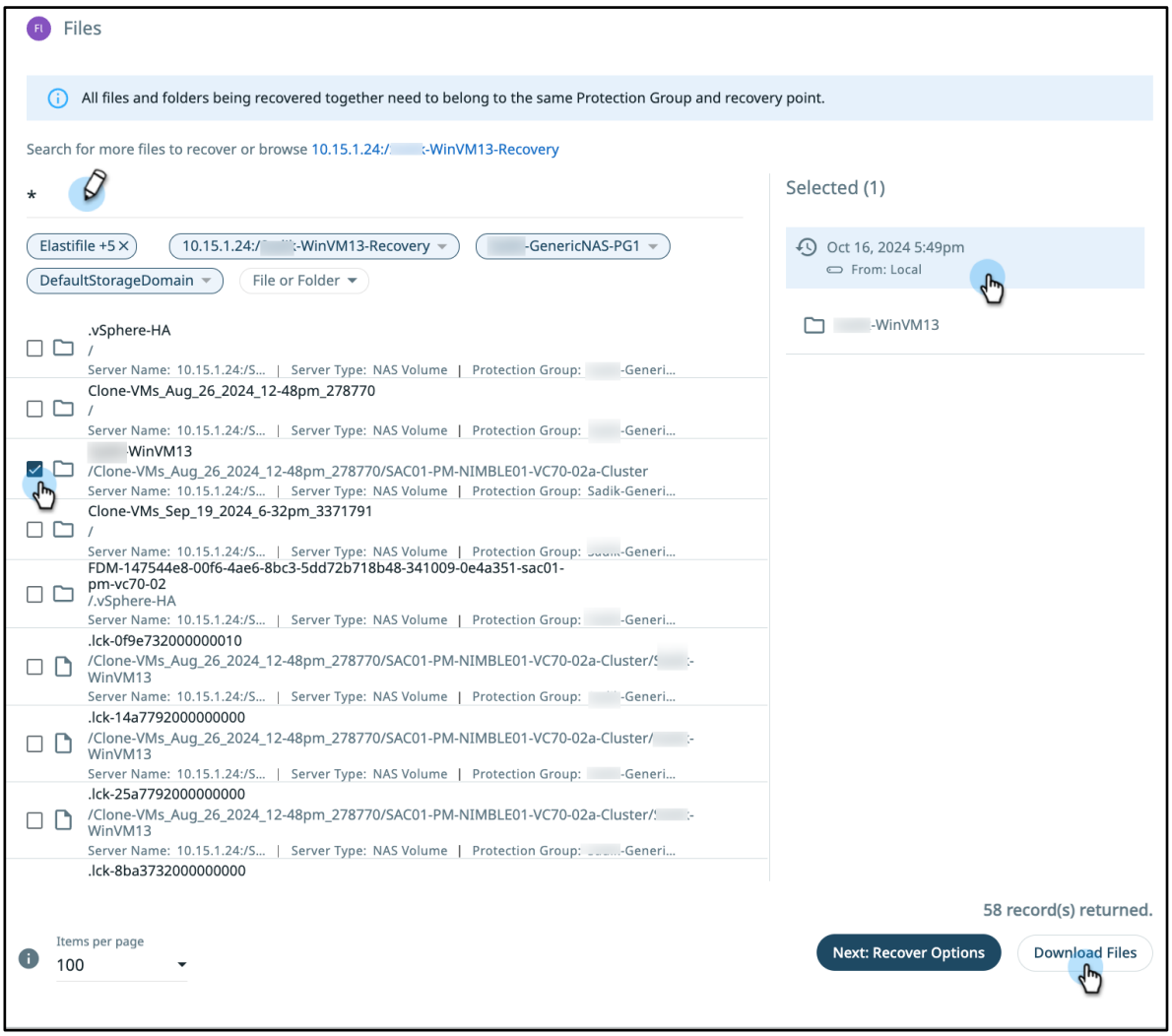
5. On the Files page, select Original Location or enter a New Location and click **Recover**.



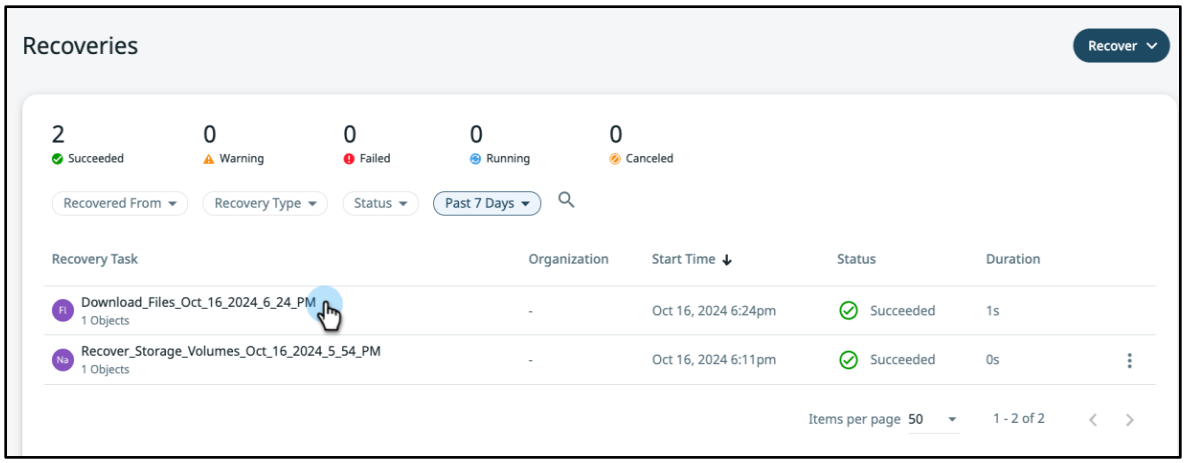
NOTE:

- To recover files or folders to an alternate path in the original source, enable the **Recover to an alternate path** toggle switch and enter the alternate path.
- For details about the **Recovery Options**, see Recover NAS Files or Folders in the online Help.

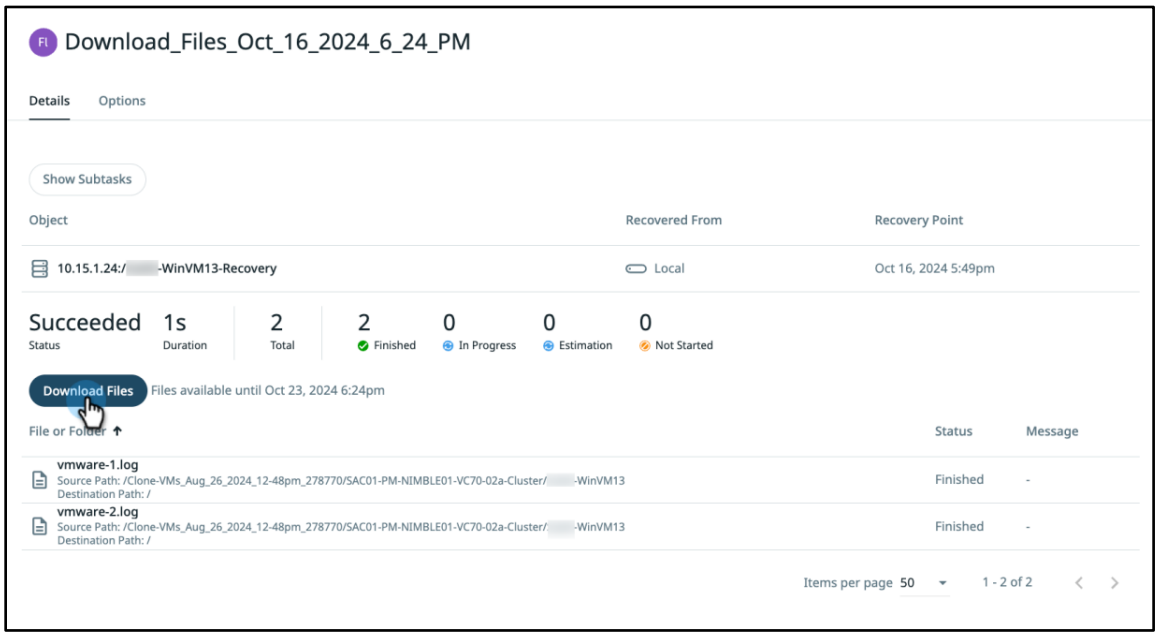
c. **Download Files**. If you are recovering a single file, this option downloads the file to your browser's download folder.



If you download more than one file, this creates a recovery task. When the task is completed, click the task name.



Click **Download Files** again to download the generated zip file.



See Appendix A: Restore Write Behavior for more details on recovery operations.

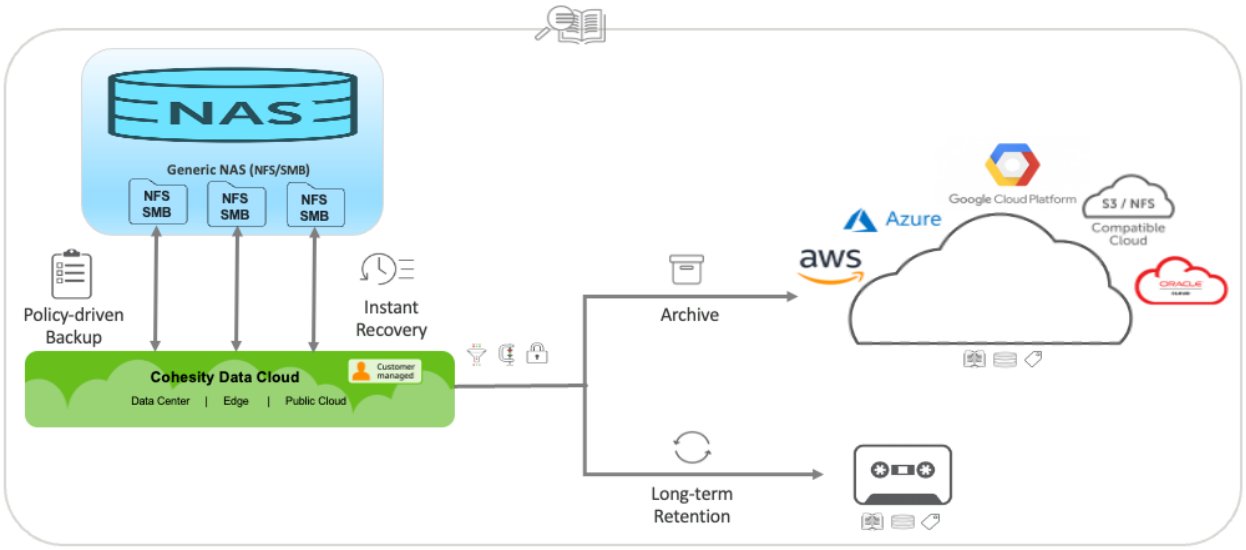
Use CloudArchive for Long-term Retention

The exponential growth of data volumes and the resulting IT management demands have prompted businesses to seek more cost-effective, reliable data storage and protection solutions. Cohesity DataProtect provides a policy-based method to archive to public clouds (AWS, Azure, GCP), to any S3-compatible storage, tape, and/or to any NFS mount point. Cohesity CloudArchive offers a complete, self-contained copy of your backup, containing backup data, backup metadata, indexing data, and deduplication fingerprints.

NAS administrators can take advantage of Cohesity CloudArchive to address long-term data retention requirements. The archived data is efficiently transferred and stored by sending only deduplicated, compressed, incremental backups, thereby reducing network and storage utilization. For added security, you can also enable Archive Object lock to lock archives on external targets and prevent data from being modified, deleted, or overwritten. Refer to Archive Object Lock for more details.

CloudArchive is very flexible. It can be used with AWS, Azure, GCP, NAS, and any S3-Compatible cloud object storage.

Figure 12: Leverage Public Cloud Infrastructure for Long-term Data Retention and Archival



Maintain Business Continuity with Disaster Recovery

Cohesity DataProtect provides two mechanisms for protecting your backup data from disruptions and disasters:

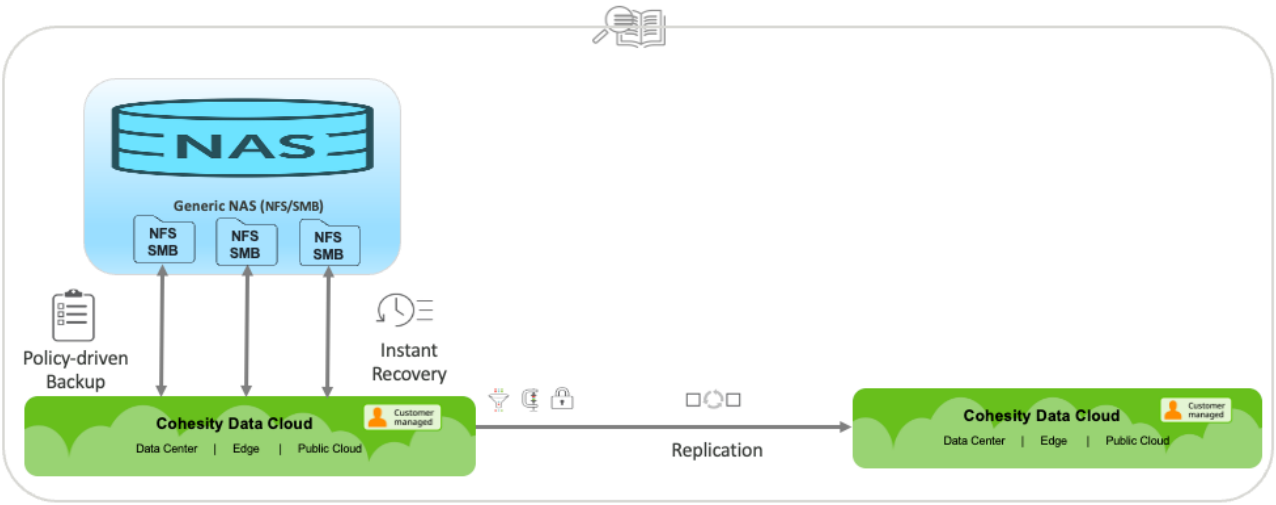
- **Replication** provides a simple way to store and retrieve data in the event of major business disruptions, such as natural disasters and IT failures.
- **CloudRetrieve** works with CloudArchive to restore your data to an alternate Cohesity cluster.

Replicate Backups to Other Cohesity Clusters

NAS administrators can take advantage of Cohesity replication for cost-effective disaster recovery (DR). Cohesity DataProtect provides a policy-based data replication solution from the core to the cloud to the edge, from one Cohesity cluster to another Cohesity cluster in your DR site.

As part of replication, Cohesity DataProtect always performs source-side deduplication and compression first and sends only the changed data over the network. If the primary site becomes unavailable, application and backup admins can fail over to the DR site for backup and recovery of their data.

Figure 13: Replicate Backups to Other Cohesity Clusters



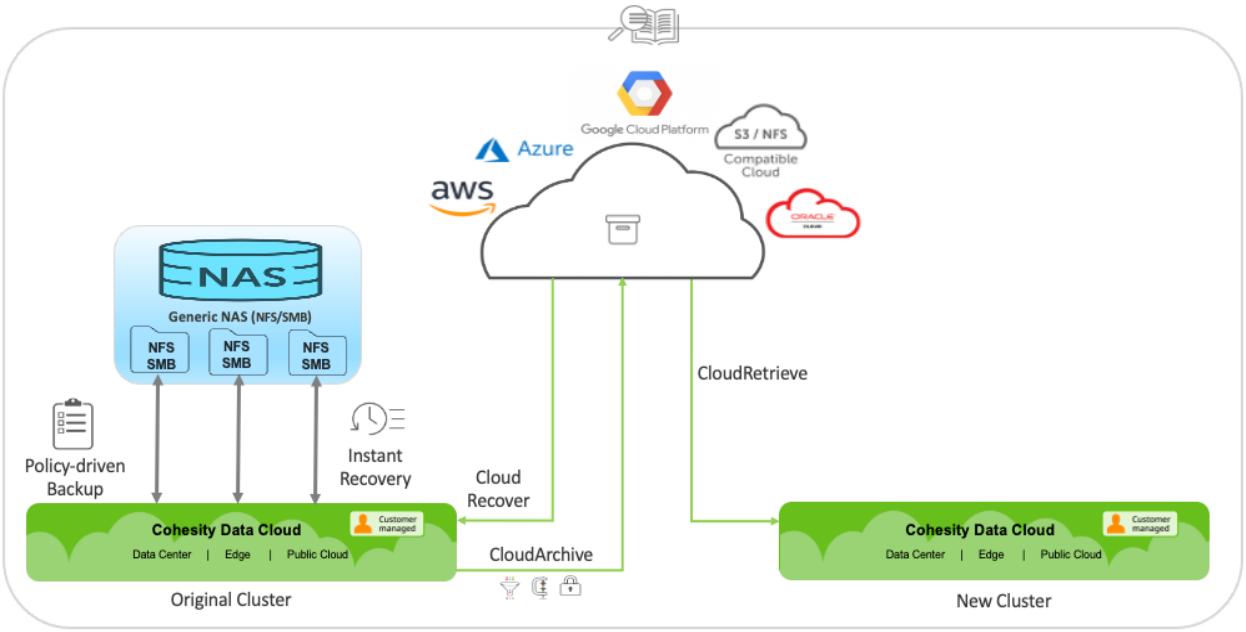
For more, see About Replication in the online Help.

Access Your Cloud-stored Data

Once the data is archived, administrators can also take advantage of the Cloud Recover and CloudRetrieve features:

- **Cloud Recover** to source Cohesity cluster: Recover all objects in your original Cohesity cluster.
- **CloudRetrieve** to new Cohesity cluster: Retrieve your previously archived data onto an entirely new Cohesity cluster as a cost-effective alternative for disaster recovery, geo-redundancy, and business continuity.

Figure 14: Cloud Recover to Original Source & CloudRetrieve to New Cluster



To learn more, see the CloudArchive & CloudRetrieve Deployment & Recovery Guide for AWS, Azure, GCP, NAS, and S3-Compatible cloud object storage.

Best Practices for Protecting Generic NAS

Some tips for getting the best performance from our solution for protecting your Generic NAS data:

1. Limit the Protection Group's object selection to a specific set of files and directories that you intend to protect. Excluding the unwanted files and folders such as tmp files and directories will reduce the overall backup (File scan, Read and Write) and indexing time. To do so you must use the **Exclusions and Inclusions** option under Protection Groups's advanced settings.
2. To use the **Exclude Folder** option while creating a Protection Group (for example, to exclude some custom folders in SMB shares or NFS exports from the backups), you must provide the exact name of the custom folders, and the folder names are case-sensitive.
3. To be able to recover at granular levels later, enable Indexing when you create a NAS Protection Group.
4. Avoid adding the same shares to multiple Protection Groups. If the main share is protected in a protection group, its sub-folder should not be protected in another protection group.
5. Cohesity scans the live filesystem when protecting a Generic NAS source and is not a point-in-time copy. If you wish to achieve a Point-in-Time backup, you can use the **Pre & Post Scripts** option in the protection group settings to point to your vendor specific custom scripts.

   Refer to Appendix C: Generic NAS Backup with Pre-Post scripts for more information.
6. If you want to efficiently backup a Generic NAS mount point that contains millions or billions of files, you must identify the directory structure under the main mount point and try to split the backup into multiple Protection Groups. To do so, you will have to register each sub-directory as a separate individual Generic NAS source.

   Refer to the Appendix D: General considerations for backing up Generic NAS mount points containing a large number of files for more information.
7. File Level Recovery (FLR) from a Generic NAS mount point, hosted on a Unix file server source, may fail with error **[kPermissionDenied]** (errno: 13 [Permission denied]). The Unix host exports have a default attribute of **root_squash.** The root_squash attribute prevents root users connected remotely from having root privileges and assigns them the user ID for the user **nfsnobody**. When Cohesity performs a FLR, it tries to change files and folders' ownership of the newly recovered files and fails due to the root_squash export parameter. You can use the **no_root_squash** option in the export settings to turn off root squashing.

   Example: Edit the /etc/exports

   /Share1 10.15.0.0/20(rw,sync,no_subtree_check,no_root_squash)

Appendix A: Restore Write Behavior

During recovery from your backups, Cohesity DataProtect performs the restore write operations differently depending on the type of restore: a NAS volume restore or a Files and Folders restore, and with or without the “Overwrite Existing File/Folder” option.

Write Operations in NAS Volume Recovery

In Generic NAS Storage Volume restore operations, the recovery task:

1. Writes the data on the target with temporary file names in the format:

   `ch_<InternalViewID>_<SubTaskID>_<FileName>`

   > **NOTE**: Folders are written the same as source names.

2. Renames the temporary file names to the original file names.
3. Sets the file/folder’s attributes on the recovered file/folder.

Write Operations in File/Folder Recovery

In Generic NAS Files or Folders restore operations, the recovery task:

1. If Recovering to New Location, creates the “/tmp/Recover-Files_<TimeStamp>” directory structure on the target and performs the recovery under that directory. This is a default path and can be changed.
2. If Recover to Original Location, creates the “/tmp/Recover-Files_<TimeStamp>” directory structure on the target and performs the recovery under that directory. This is a default path and can be changed using the “Recover to alternate path” toggle switch.
3. Writes recovered files in the format:

   `__ch_<InternalViewID>_<SubTaskID>_<FileName>`

   > **NOTE**: Folders are written the same as source names.

   Renames the temporary file names to the original file names.
4. Sets the file/folder’s attributes on the recovered file/folder.

Recovery Behavior With and Without “Overwrite Existing File/Folder”

As you **restore** files and folders from your Generic NAS backups, the restore operations behave differently depending on the restore location, target volume, and the “Overwrite Existing File/Folder” option.

Table 4: Recovery Behavior With and Without “Overwrite Existing File/Folder”

RESTORE TO	SELECT VOLUME	OVERWRITE EXISTING FILE/FOLDER	RECOVERY BEHAVIOR
Original Location	N/A	Enabled	Data is restored to the original location. In the same path, folders with the same name are merged with the backed-up folders, and files with the same name are overwritten. Unique data on the target (data that is not present in the recovery point snapshot) is not touched during the restore task run.
		Disabled	Data is restored to the original location. In the same path, folders with the same name are merged with the backed-up folders, and files with the same name are skipped. Unique data on the target (not present in the recovery point snapshot) is not touched during the restore task run.
New Location	Same as source volume	Enabled	Same behavior as “Restore to Original Location.”
		Disabled	Same behavior as “Restore to Original Location.”
	Alternate volume	Enabled	Data is restored to the alternate location. In the same path, folders with the same name are merged with the backed-up folders, and files with the same name are overwritten. Unique data on the target (not present in the recovery point snapshot) is not touched during the restore task run.
		Disabled	Data is restored to the alternate location. In the same path, folders with the same name are merged with the backed-up folders, and files with the same name are skipped. Unique data on the target (not present in the recovery point snapshot) is not touched during the restore task run.

Appendix B: Index for Faster Granular-level Recovery

Cohesity DataProtect allows you to index your backup content, allowing you to search for a single file among billions of files.

Indexing scans the backup data with simple, text-based search-and-restore functionality to find files quickly, thus enabling instantaneous data retrieval from the backed-up snapshots.

Improved Indexing

Cohesity DataProtect's indexing engine has continued to evolve to deliver better performance and faster results through incremental indexing:

- **Incremental Indexing**. Cohesity indexing engine only scans the data that has changed since the previous snapshot. This is much less resource-intensive and results in faster indexing.

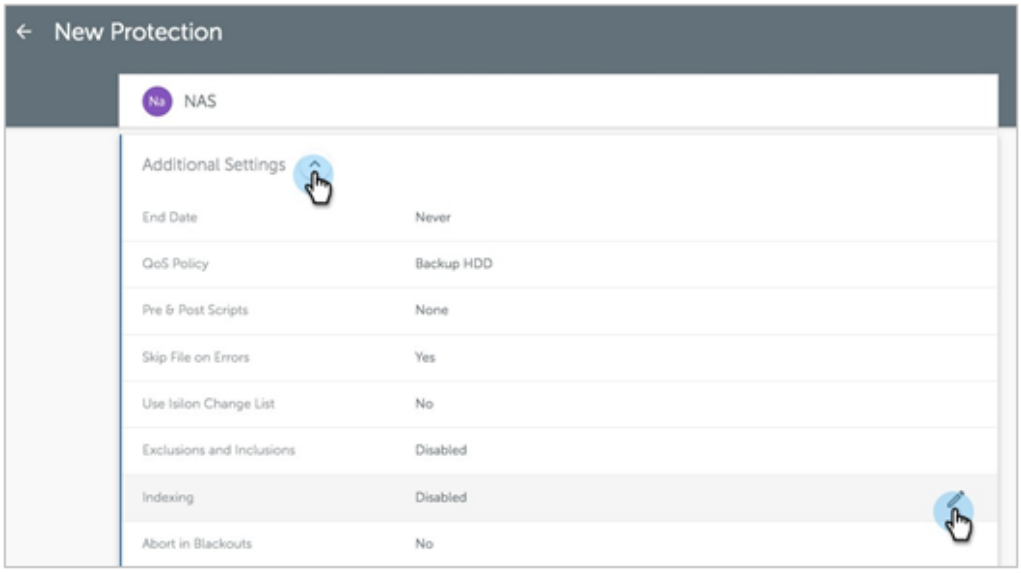
Enable Indexing

To enable "Files and Folders" search, enable **Indexing** in the Protection Group.

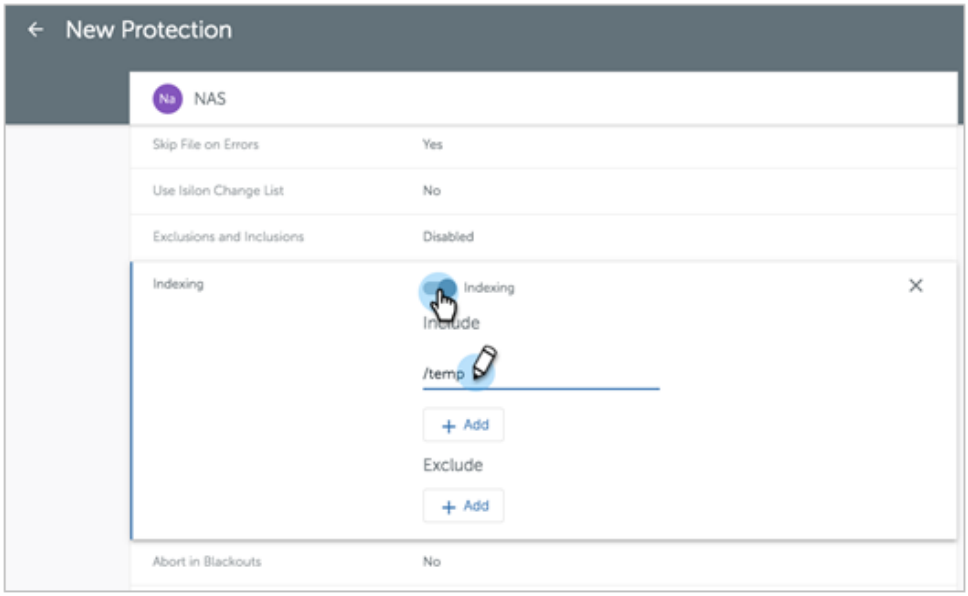
Once indexing is enabled in the Protection Group, everything in the protected SMB/NFS share is indexed by default. However, because indexing is resource-intensive, we recommend that you exclude the files and directories where file-level recovery is not required, such as scratch spaces, binaries, temp files, etc. You can limit the indexing to a specific set of files and directories by defining them in the **Include** and **Exclude** settings under **Indexing** in the Protection Group settings.

To enable indexing in a Protection Group:

1. When you create a Protection Group, click **Advanced Settings** and the **Edit** pencil icon in the **Indexing** row.



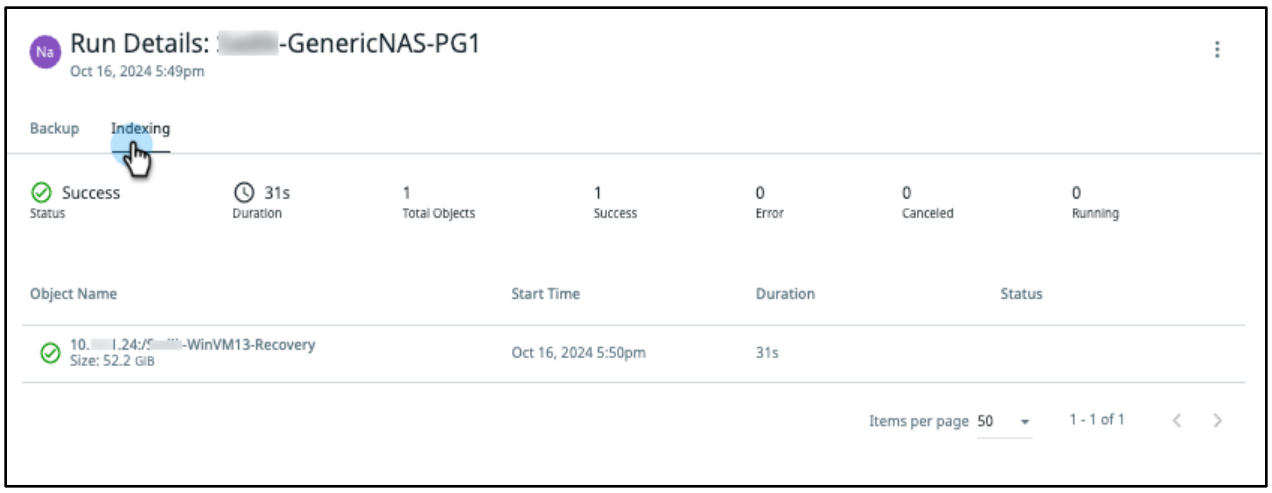
2. Click the **Indexing** button to enable it. If you wish to, you can also add folders/directories under **Include** and **Exclude**.



3. Edit any other **Advanced Options** as necessary and click **Protect**.

Once a Protection Run is completed successfully, the Protection Group starts indexing the backup metadata. You can track the progress of the **Indexing** in the Protection Run Details.

Figure 15: Click a Completed Protection Run for Indexing Progress



NOTE: During a Protection Run, the indexing engine scans the successfully backed up objects and skips any objects that failed to back up. The indexing engine runs for all successfully backed-up objects, even if a Protection Run is completed with warnings.

Appendix C: Generic NAS Backup with Pre-Post scripts

Cohesity has API integration with specific NAS vendors such as NetApp and Dell EMC Isilon. These NAS sources are backed up using Cohesity NAS Adapter (API based). All the other NAS vendors where Cohesity does not have API integration are referred to as Generic NAS.

Generic NAS adapter does the file walk on the live filesystem to discover the files to backup. Hence, the backup copy is not a point-in-time copy of the data. Also, in some scenarios like files being deleted during backup run, you could see errors or warnings in the protection group run. To take a point-in time backup copy of your Generic NAS data, you can use the Pre & Post Scripts option to leverage your custom scripts.

The following are the required steps at a high level:

1. **Copy the script to the UNIX/Linux management host—**from where the script will be run via Protection Group configuration.

   > **NOTE**: Creation of the Pre & Post Scripts is the customer's responsibility.

2. **Enable Key Based authentication to access NAS filer from Management Host**— for a secure connection between the unix management host and the NAS filer.
3. **Configure RSA authentication on the UNIX/Linux Host to authenticate Cohesity**—for a secure connection between the unix management host and the Cohesity Cluster.
4. **Registering a Source**—Register the Generic NAS NFS export path or SMB share path to backup

   To register a source:

   a. Navigate to **Data Protection** > **Sources**.
   b. Click "Register" and choose NAS.
   c. Select NAS Source as "Generic NAS".
   d. Select the mode as NFSv3, NFSv4.1 or SMB.
   e. In the Mount Path: Specify the NFS/SMB volume snapshot share path that needs to be backed up.

      > **NOTE**: In the Mount Path, specify the NFS/SMB volume snapshot path that the script will create upon execution. The Protection Group will then scan and back up this snapshot.

      NFS Mount Path Format:

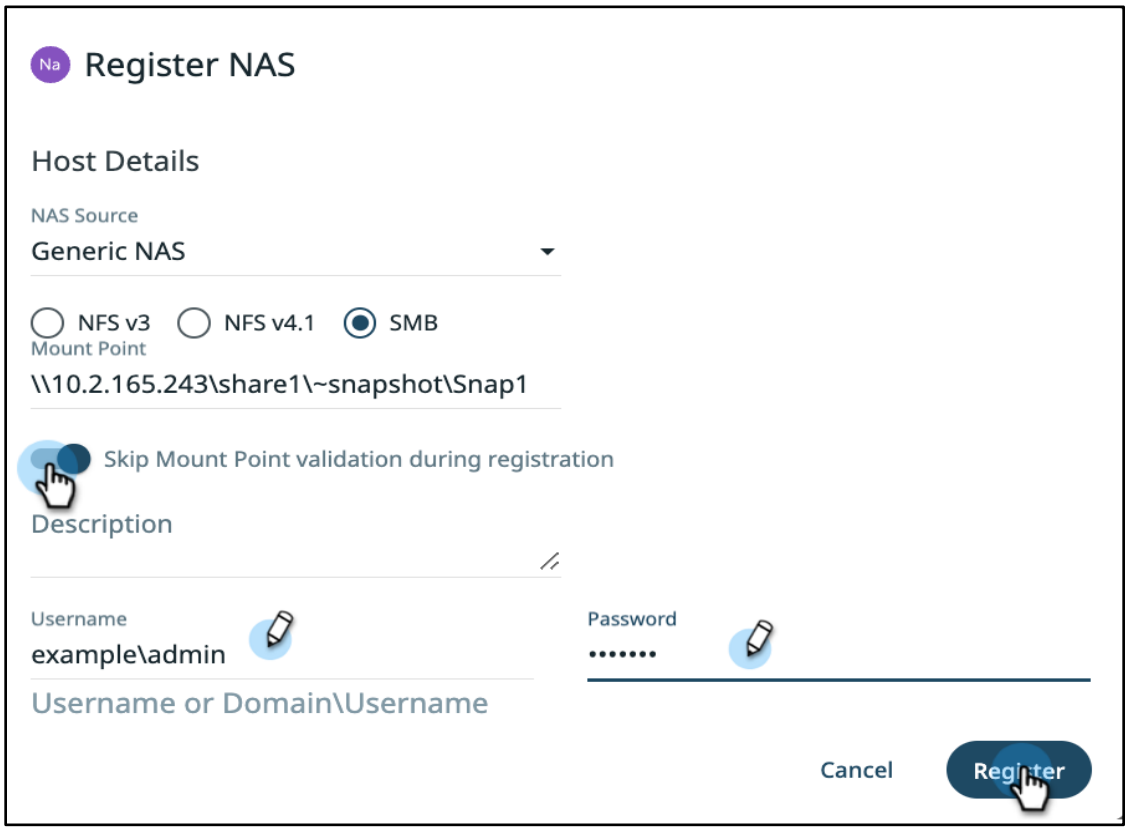
      `<NAS_IP>:<NFS_Volume_Path>/.snapshot/Cohesity_PG_Snap`

      SMB Mount Path Format:

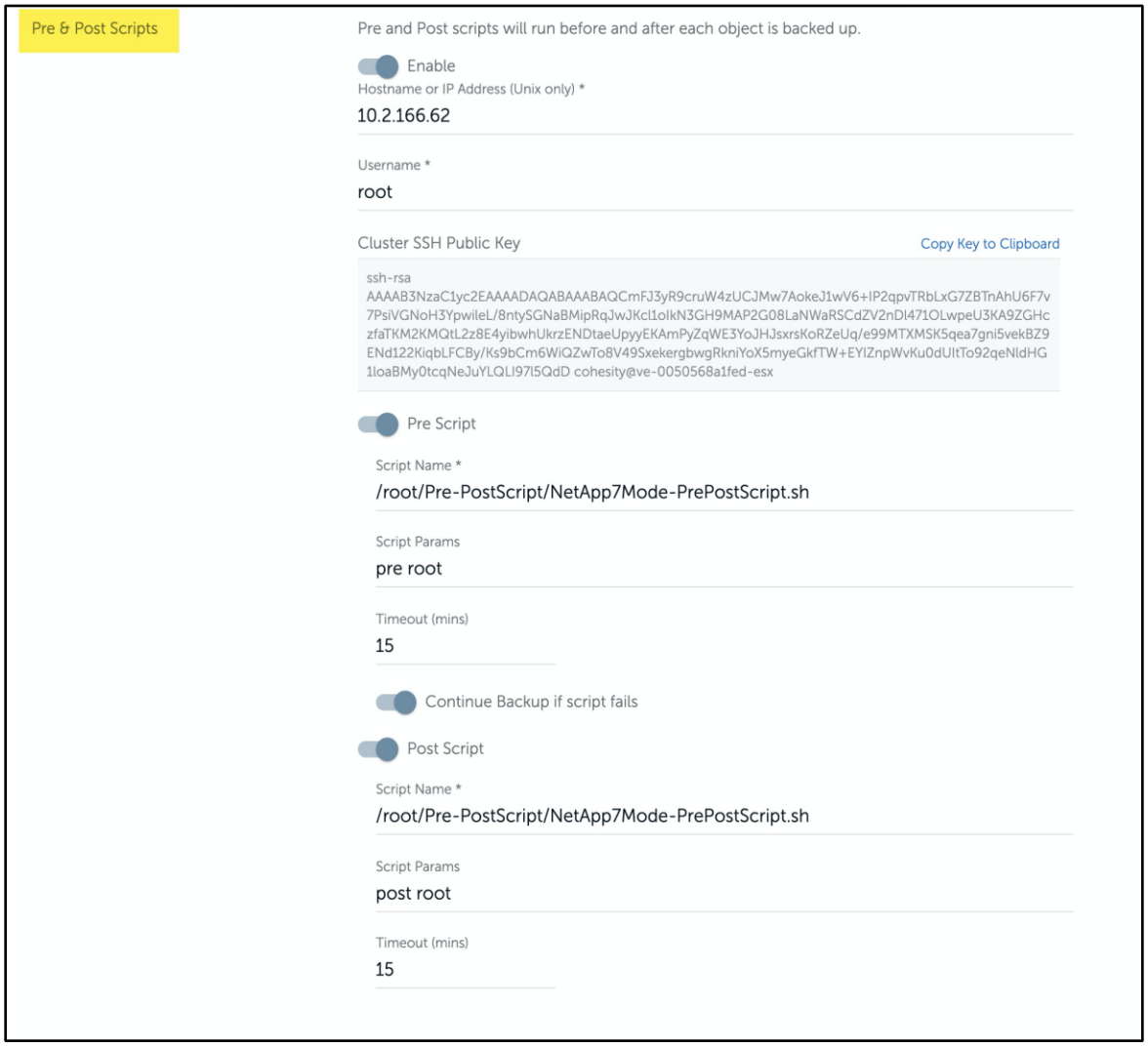
      \\<NAS_IP>\\<SMB_Volume_CIFS_Share>\\~snapshot\\Cohesity_PG_Snap

   f. Toggle on "Skip Mount Point validation during registration."

g. In case of SMB share, provide the SMB mount credentials that allow the reading and backing up of files. If you are providing a domain user account, then you must specify the user name in the following format: **fully_qualified_domain_name\username**. For example, **xydc.local\user1**.



5. Configure the Protection group
   a. Enter the mandatory values to configure a Protection Group (Protection Group name, Source, Storage Domain, Policy, etc.).
   b. Under the Advanced Settings:
      - Toggle on to Enable Pre & PostScript
      - The screenshot below captures the necessary details to configure Pre & postscript.



Below table explains all the Pre & Post Scripts configuration input values:

FIELD NAME	VALUE	NOTES
Hostname or IP Address	Linux/UNIX Hostname or IP Address	Linux/Unix Hostname where Pre & Postscript is hosted
Username	Linux/UNIX username	Linux/Unix username which would run the script on the UNIX host
Pre Script > Script Name	The absolute path of the Pre Script	The absolute path of the Pre Script hosted on Linux/Unix server
Script Params	*pre <NAS Filer username>*	NAS Filer Username is the filer's local username which will run script on NAS. Example: pre root
Post Script> Script Name	The absolute path of the PostScript	The absolute path of the PostScript hosted on Linux/Unix server
Script Params	*post <NAS Filer username>*	*NAS Filer* Username is the filer's local username which will run script on NAS. Example: post root

NOTE:

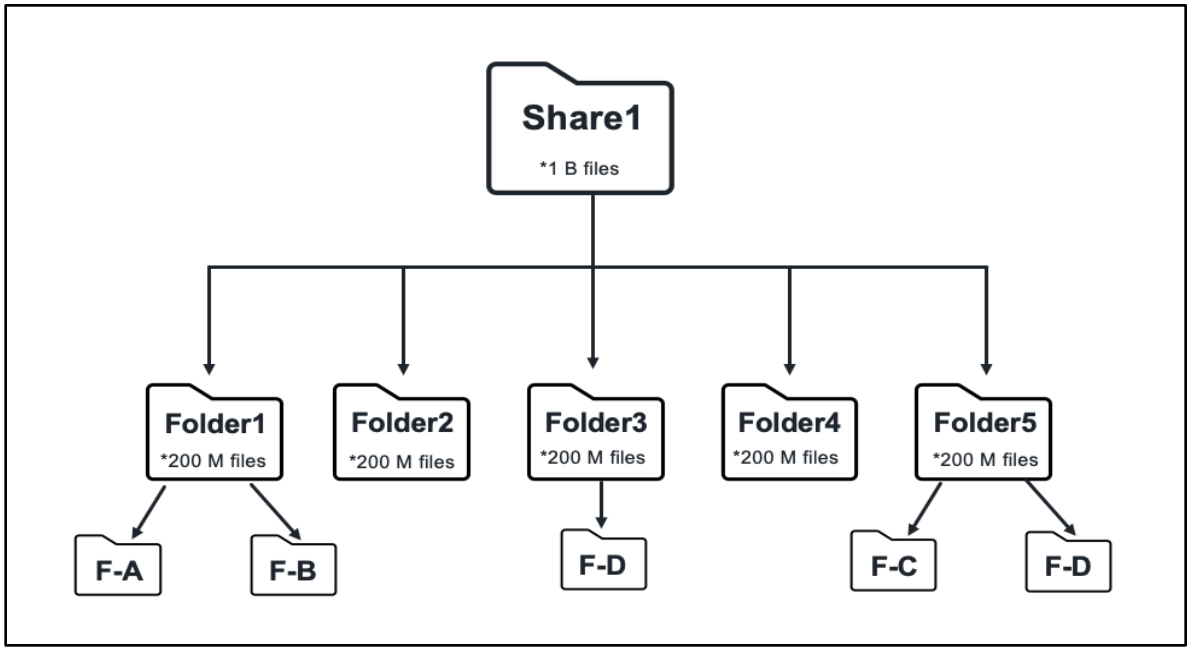
- Refer to Configure the settings for running the Pre and Post scripts for more details.
- Creation of the Pre & Post Scripts is the customer's responsibility.

Appendix D: General considerations for backing up Generic NAS mount points containing a large number of files.

When backing up a Generic NAS mount point containing a large number of files (Billions of files) you will experience degraded backup performance. When performing Generic NAS backup, Cohesity scans the live filesystem of the registered Generic NAS mount point. The larger the number of files, the more time it will take to perform the Scan operation during the File discovery phase. The file discovery operation is a multi-threaded task but is executed on a single Cohesity node.

To perform an efficient backup of Generic NAS mount points containing a large number of files, you must understand the directory structure inside the mount point and choose to split the backup into multiple protection groups.

Figure 16: Example of an Export/mount point with Large File count.



In the above example, the main share is named "**Share1**" and it contains 1B files. Under **Share1,** the subfolder named **Folder1** through**Folder5** contains 200 M files each. If you register the main share **Share1** as a Generic NAS source and protect this mount point as a single object in a Protection group, you may experience extended backup time. This is because the protection group will use a single Cohesity node for its file scan operation in the File discovery phase.

To take advantage of Cohesity's parallel and distributed architecture in this use case, you could spread the backup of the main share "**Share1**" (1B files) across multiple Protection groups. In the above example, register each sub-folder (**Folder1** through**Folder5**) as an individual Generic NAS source and protect each mount point in its own separate protection group. Since the backup is now spread across multiple protection groups, you will leverage the cluster's parallel and distributed architecture, leading to faster backups and indexing.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sadik Sayed is a Technical Solutions Engineer at Cohesity. In his role, he is focused on NAS backup solutions with Cohesity.

Other significant contributors included:

- Kaiwalya Pethe, Cohesity Engineering
- Rich Kuhn, Product Solutions

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	May 2025	Added DFS referral support
1.0	November 2024	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.