COHESITY

Protect Dell EMC Isilon with Cohesity

Bringing Scalability and Simplicity to Isilon Data Protection

Version 3.6

May 2025

ABSTRACT

Cohesity streamlines the protection of the petabytes of Dell EMC Isilon 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 Isilon Data 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 Isilon

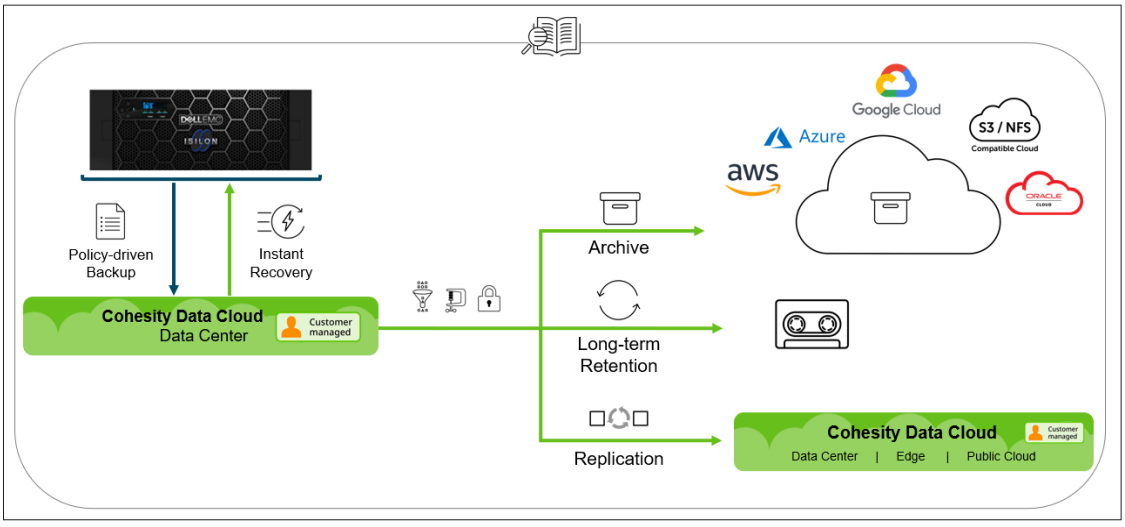
Organizations that rely on Dell EMC Isilon as their primary NAS need a fast, powerful, and simple backup and recovery solution that scales well to grow with their ever-growing data.

To meet these 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.

With Cohesity DataProtect™, you can protect your primary and secondary Isilon directories. Once you back up your Isilon 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.

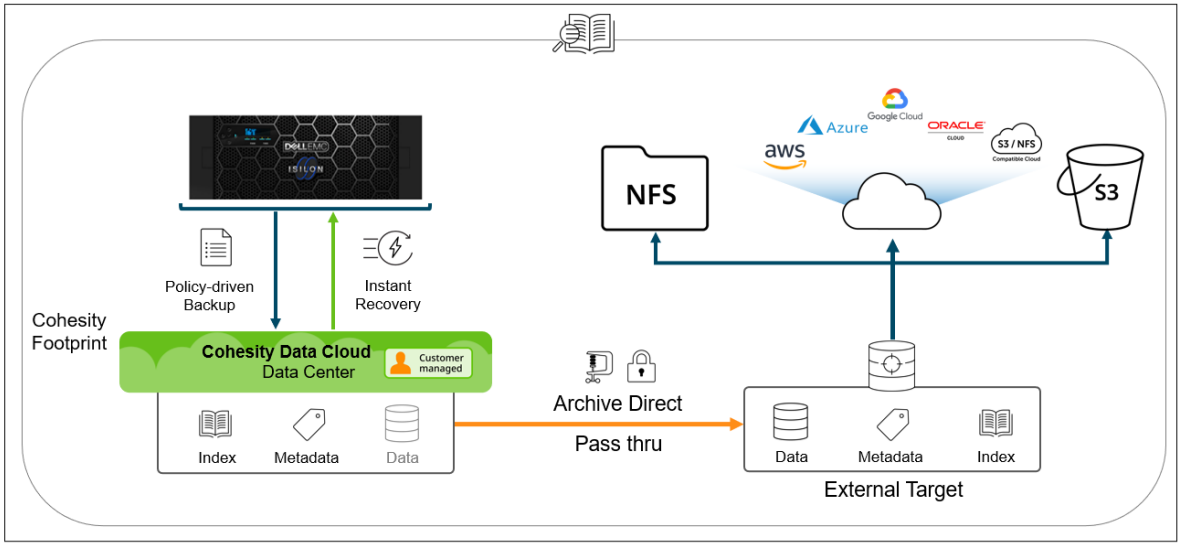
Figure 1: Protect Dell EMC Isilon Data with Cohesity



Cohesity CloudArchive Direct Architecture for Isilon

Cohesity has built CloudArchive Direct for NAS, a cost-efficient solution that processes and streams the data directly from Isilon storage 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 Isilon dataset (the data along with metadata and indexes) is stored only on the External Target.

Figure 2: Make Isilon 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:

- **Snapshot-based Backups**. Cohesity leverages its native snapshot capabilities to take snapshots of storage volumes. Point-in-time (PIT) snapshots are captured and mounted locally for faster backups. For Isilon backups, Cohesity uses the Isilon Changelist native API to track changes between snapshots.
- **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 consolidation of infrastructure and datasets, which leads to a better return on investment (ROI).
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 Isilon 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 Isilon Adapter's Capabilities

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

- **Incremental Backup with the Isilon Changelist**. You can use the Isilon Changelist to find the changed files during an incremental backup just by enabling "Use Isilon Changelist" in the Protection Group's advanced settings. The Isilon Changelist is an internal OneFS job engine that quickly identifies the file and folder differences between any two snapshots.

  See Incremental Forever Backups with Vendor-native CFT for details.

- **Encrypt Backup Traffic Between Isilon and Cohesity**. You can encrypt your backup traffic between Isilon and Cohesity 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 Isilon to access the SMB volume data to back up. The encrypted SMB session encrypts all the session traffic between Isilon and Cohesity.

NOTE:

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

Table 2: Encryption Behavior Relationship with SMB Encryption Status in Isilon

COHESITY VERSION	ENCRYPTION ENABLED IN PROTECTION GROUP?	OPERATION	SMB ENCRYPTION *ENABLED* ON ISILON SHARE	SMB ENCRYPTION *DISABLED* ON ISILON SHARE
6.8.1, 7.0, 7.0.1, 7.1, 7.1.1 and 7.1.2	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 Isilon.

NOTE: Following are the requirements for encrypted NFS backup.

- Configure NFS Kerberos on Isilon.
- Configure an NFS export policy to allow Kerberos krb5p.
- Join your Cohesity cluster to the Active Directory (AD) domain.

For more, see Dell EMC's Integrating OneFS with Kerberos Environment for Protocols technical white paper.

- **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.
- **Filter IPs (Allow\Deny) for backup and recovery communication**. Enable this option to filter the IP addresses of the Isilon cluster. By filtering IP addresses, you can allow or deny the communication of the Cohesity cluster to specific IP addresses or subnets of the Isilon cluster at the Protection Group level.

  To filter the IP addresses of the Isilon cluster, select one of the following options:

  - **Allow IPs**: Select this option and specify the IP addresses of the Isilon cluster source through which communication to the Cohesity cluster must happen. You can provide the IP addresses in a comma-separated list or in a CIDR format.
  - **Deny IPs**: Select this option and specify the IP addresses of the Isilon cluster source through which communication to the Cohesity cluster must not happen. You can provide the IP addresses in a comma-separated list or in a CIDR format.
- **File DataLock to Preserve Access Time of Isilon SmartLock Directories**. With Cohesity 6.5.1 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:

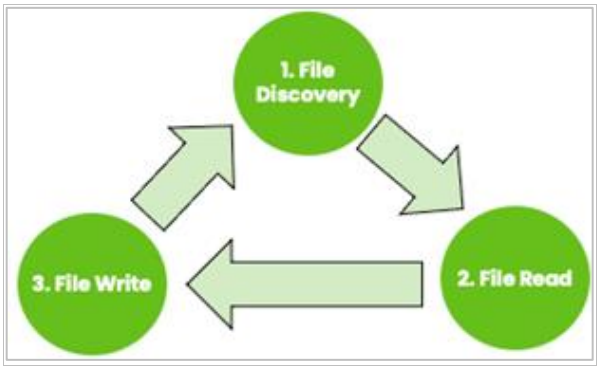
- Supports Enterprise or Compliance modes.
- Preserves the access times of both hard and symbolic links.
- You cannot enable or disable File DataLock once a Protection Group is created.
- You can delete Protection Groups and snapshots that have File DataLock enabled. However, once the data is recovered 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.

Understand Cohesity's Isilon Backup Approach

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

To understand how Cohesity Isilon data protection works, it helps 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 Isilon backup run, the Cohesity file runner discovers the list of files and folders that need to be backed up from the user-selected Isilon object in the Cohesity Protection Group. You can choose to back up the entire /ifs filesystem or a subset of it. 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 does not support the inclusion or exclusion of paths in Changelist-enabled Isilon Protection Groups

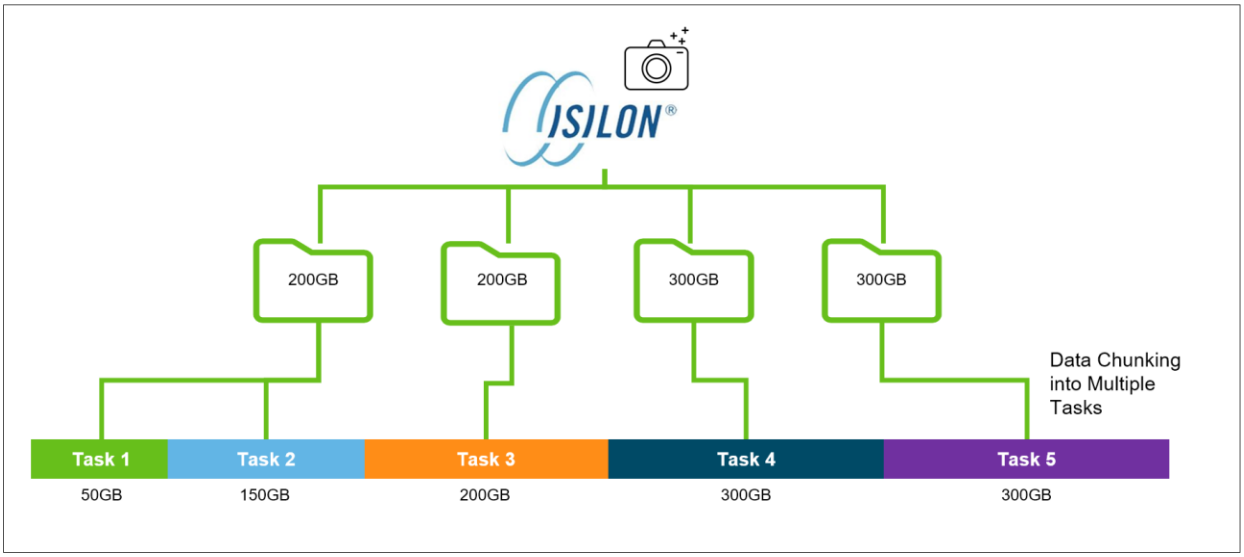
Cohesity performs slightly different file-discovery processes during full and incremental backups. See Cohesity Isilon Backup Workflows below for details

File Read

Cohesity DataProtect uses a parallel and distributed architecture to read the Isilon NAS dataset, using native SMB/NFS protocols that are identified during the File Discovery phase above. It uses an intelligent algorithm to divide the identified dataset into multiple tasks (data chunks) based on both the size of the data 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

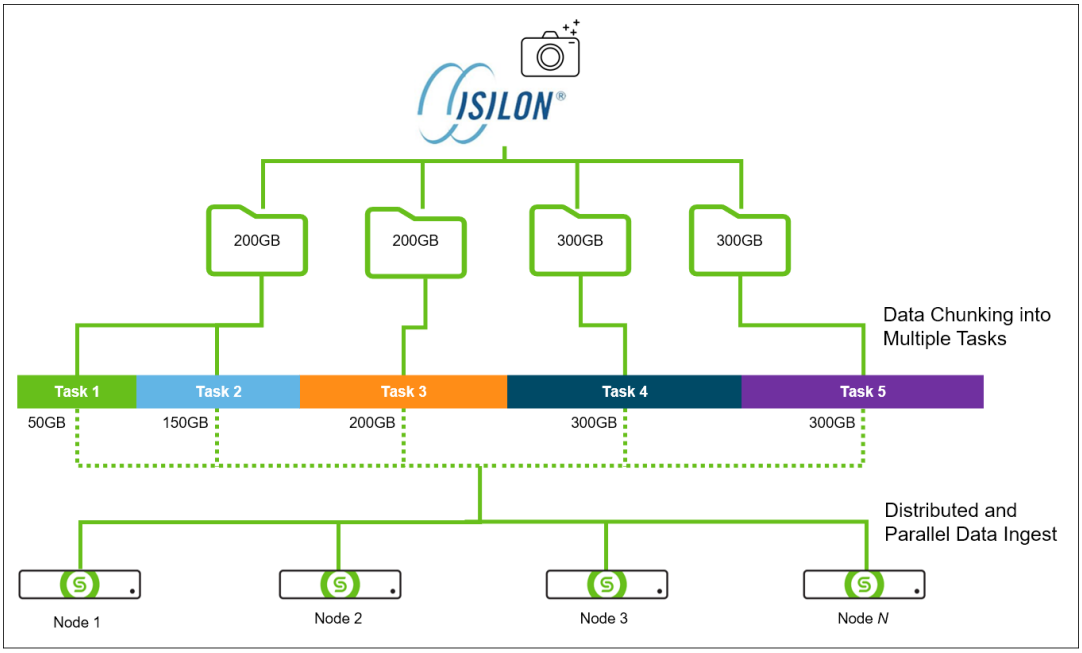


File Write

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.

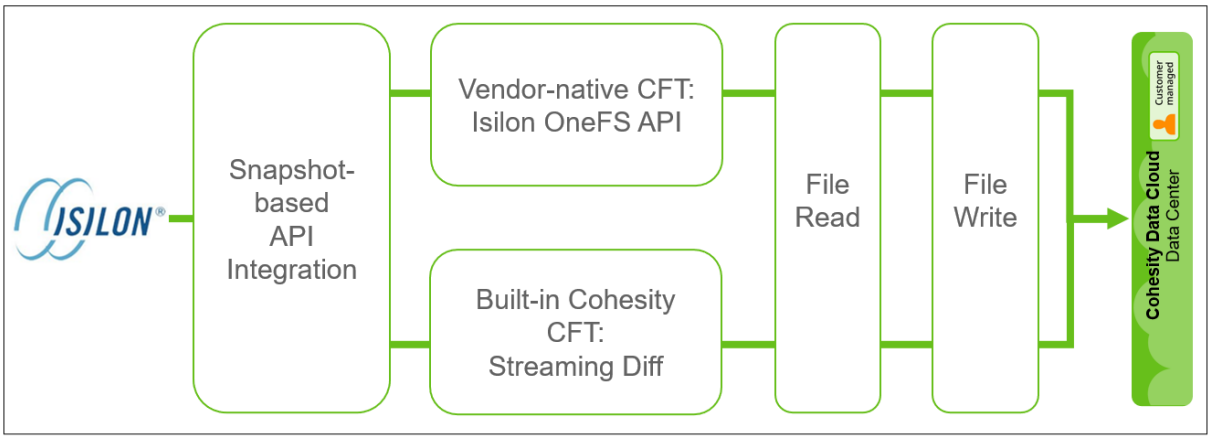
After a Protection Run is complete, all files are indexed by Cohesity to enable global search and rapid recovery.

Cohesity Isilon Backup Workflows

As you prepare to protect your Isilon 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 one of two CFT (Changed File Tracking) methods:
  - Vendor-native CFT: The Isilon Changelist.
  - Built-in Cohesity CFT: Cohesity streaming diff technology.

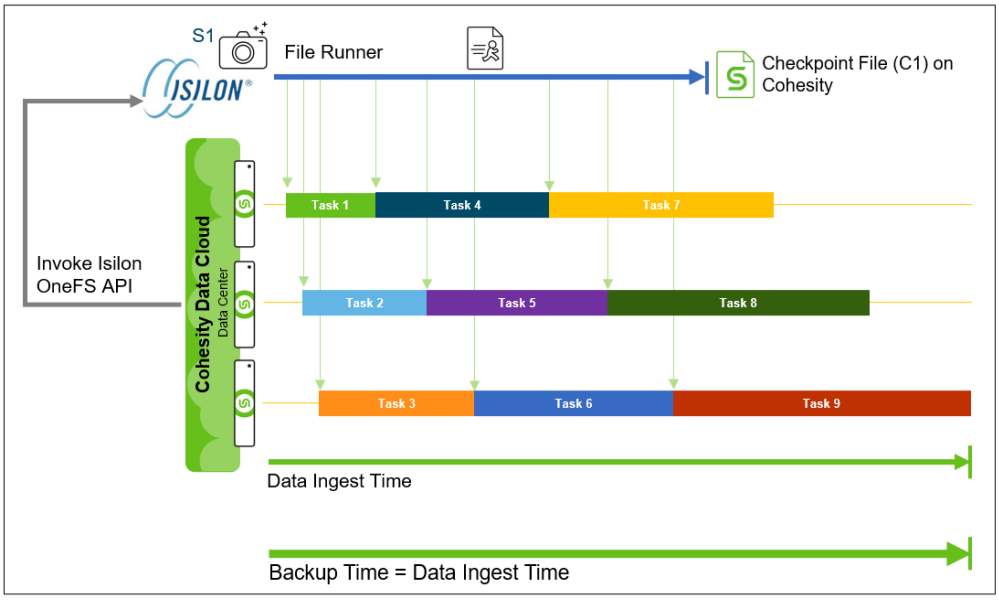
Figure 5: Cohesity's Approach to Protecting Isilon NAS Data



Full Backup with High-speed File Discovery

To start the protection, the initial backup is always a full data backup. Cohesity DataProtect leverages the Isilon OneFS API to create a snapshot for a point-in-time (PIT) backup by performing a high-speed file discovery using Cohesity's file runner.

Figure 6: Cohesity's Initial, Full Isilon Backup Process



During the initial, full backup, Cohesity DataProtect creates snapshot S1 using the Isilon snapshot API and performs the following operations in parallel, thereby dramatically reducing backup times:

- **File Runner**: Starts the high-speed file runner on the snapshot (S1) and discovers the files & folders to back up by accessing the snapshot on all the nodes of the Cohesity cluster.
- **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.

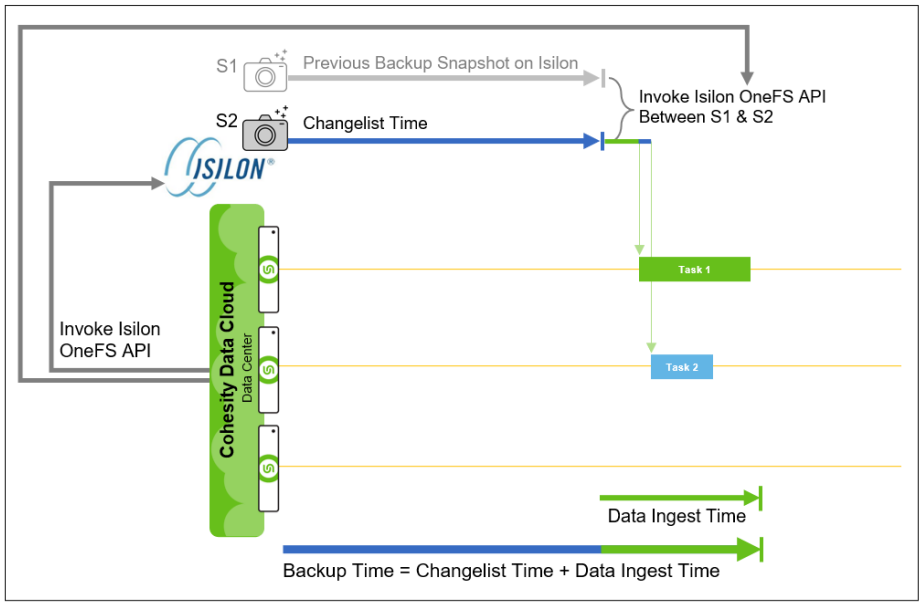
After the first full backup is complete, it is followed by incremental forever backups that send only changed data. Then:

- If vendor-native CFT is enabled in the Protection Group, Cohesity retains the S1 snapshot.
- If the Protection Group does not enable vendor-native CFT, Cohesity uses its built-in CFT based on streaming diff technology. In this case, it deletes snapshot S1.

Incremental Forever Backups with Vendor-native 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. If vendor-native CFT is enabled in the Cohesity Protection Group, Cohesity identifies the changed data by invoking the Isilon Changelist to reduce the time taken to discover the changed files and folders to back up. The Isilon Changelist is an internal OneFS job engine that quickly identifies the file and folder differences between any two snapshots. It can only be used for incremental backups.

Figure 7: Incremental Forever Backups with Vendor-native CFT



When vendor-native CFT is enabled, Cohesity DataProtect:

1. Creates a second snapshot (S2) using the Isilon snapshot API and accesses the snapshot on all the nodes of the Cohesity cluster.

   NOTE: Snapshot S1 is available on Isilon from the previous (full) backup.

2. Leverages the Isilon OneFS job engine to retrieve the data that has changed between the previous snapshot (S1) and the current snapshot (S2). Using the Isilon Changelist replaces the need for separate file discovery and reduces the total backup time.

3. Once the OneFS job engine returns the changelist, Cohesity DataProtect reads the files from it and produces the tasks for ingestion.

> **NOTE**: Isilon supports only one changelist request at any given time. If the Protection Group contains multiple shares to back up, changelists are created serially.

Once the incremental backup completes, the previous snapshot (S1) is deleted, and the new snapshot (S2) is retained. At any point in time, the most recent snapshot is retained on Isilon and used to compute the changes for the next backup.

If data ingestion fails (that is, the Protection Run has a status of failure), the new snapshot (S2) is deleted, and the previous snapshot (S1) is retained for the next backup run.

Enable Isilon Changelist for Faster Incremental Backups

Isilon Changelist allows you to find the changed files during an incremental backup. This has several benefits and considerations:

Benefits:

- With Isilon's native Changelist, Cohesity DataProtect retrieves the Changelist that is created by Isilon. It then backs up the file paths in the Changelist instead of scanning the entire file system to identify the changes.
- With Cohesity DataProtect using the Isilon Changelist, incremental backup times are dramatically reduced.

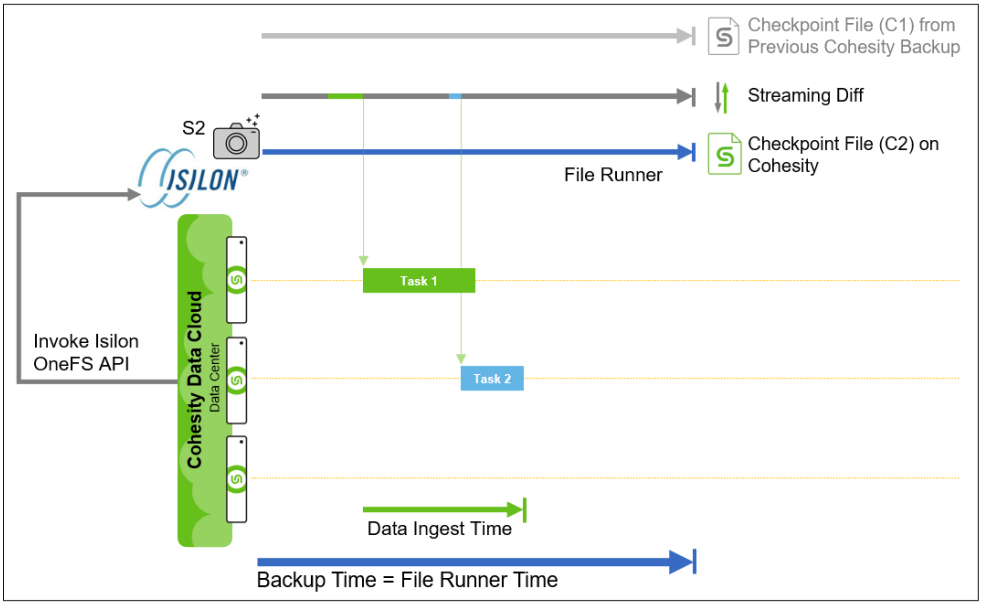
Considerations:

- Cohesity cannot determine the actual size because each share is a subdirectory of the root /ifs directory.
- For Isilon OneFS 9.5.x or earlier versions, the maximum filename length is 256 bytes, and the full path length is limited to 4096 bytes.
- Cohesity recommends a first full and incremental forever backup approach to back up your NAS sources.
- The first (full) backup is always performed using the high-speed file discovery in Cohesity's file runner, as the Isilon Changelist cannot be used until after the first incremental backup.
- The Changelist requires two snapshots to compute the difference. Hence, to use the Changelist, Cohesity retains the latest snapshot on the Isilon cluster for each SMB share or NFS export that is backed up.
- Isilon supports only one Changelist request at any given time. If the Protection Group contains multiple shares to back up, Changelists are created serially.
- Once a Changelist is available, multiple ingests can take place in parallel for multiple shares or mount points.
- If there are issues with access to the Isilon Changelist, the Protection Run falls back to identifying the changed data by performing its own built-in CFT, thereby continuing to execute an incremental forever backup.

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. If vendor-native CFT is not enabled in the Cohesity Protection Group, 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 8: Cohesity's Incremental Isilon Backup Process



During the incremental backup, Cohesity DataProtect uses the Isilon snapshot API to create a new snapshot (S2) and performs the following operations in parallel, thereby dramatically reducing backup times:

- **File Runner**. Starts the high-speed file runner on the new snapshot (S2) and discovers the files & folders by accessing the snapshot on all the nodes of the Cohesity cluster.
- **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.

When a Protection Group contains many objects, using this built-in CFT can be faster than vendor-native CFT, which is limited to only one Changelist call at a time. With built-in CFT, Cohesity runs all the above processes in parallel across all objects in the Protection Group.

NOTE: Because this approach relies on built-in CFT (comparing checkpoint files), the snapshots themselves are deleted after every backup operation is completed.

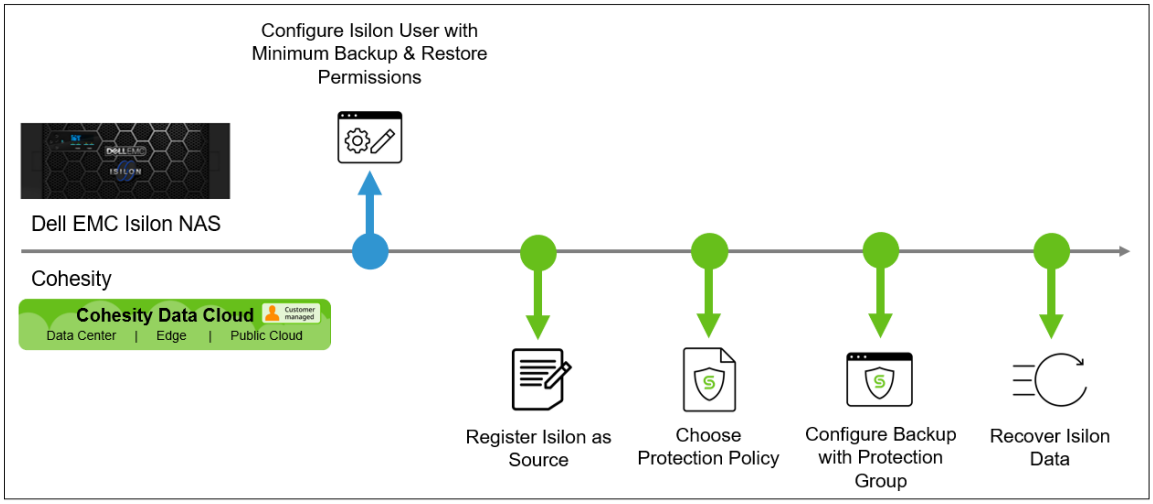
Protect Isilon Data with Cohesity DataProtect

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

To prepare Cohesity DataProtect to back up your Dell EMC Isilon cluster, ensure your Cohesity and Isilon OneFS meet the prerequisites and then:

1. Configure an Isilon user with the minimum required backup and restore permissions.
2. Register your Isilon cluster as a source in Cohesity.
3. Choose a Cohesity Protection Policy.
4. Create a Cohesity Protection Group.
5. Recover your Isilon NAS data using Cohesity DataProtect.

Figure 9: Protect Isilon NAS with Cohesity DataProtect



Add Your Isilon Cluster as a Cohesity Source

To back up your Isilon NAS cluster on Cohesity DataProtect, you need to register it as a source in Cohesity. Cohesity DataProtect then leverages Isilon's OneFS APIs to connect to Isilon and enumerate the shares/exports.

Prerequisites

Our solution requires the following to protect an Isilon cluster:

- Cohesity 6.8.x or higher
- Isilon OneFS Version 8.0, 8.1, 8.2, 9.0.x - 9.5.x.

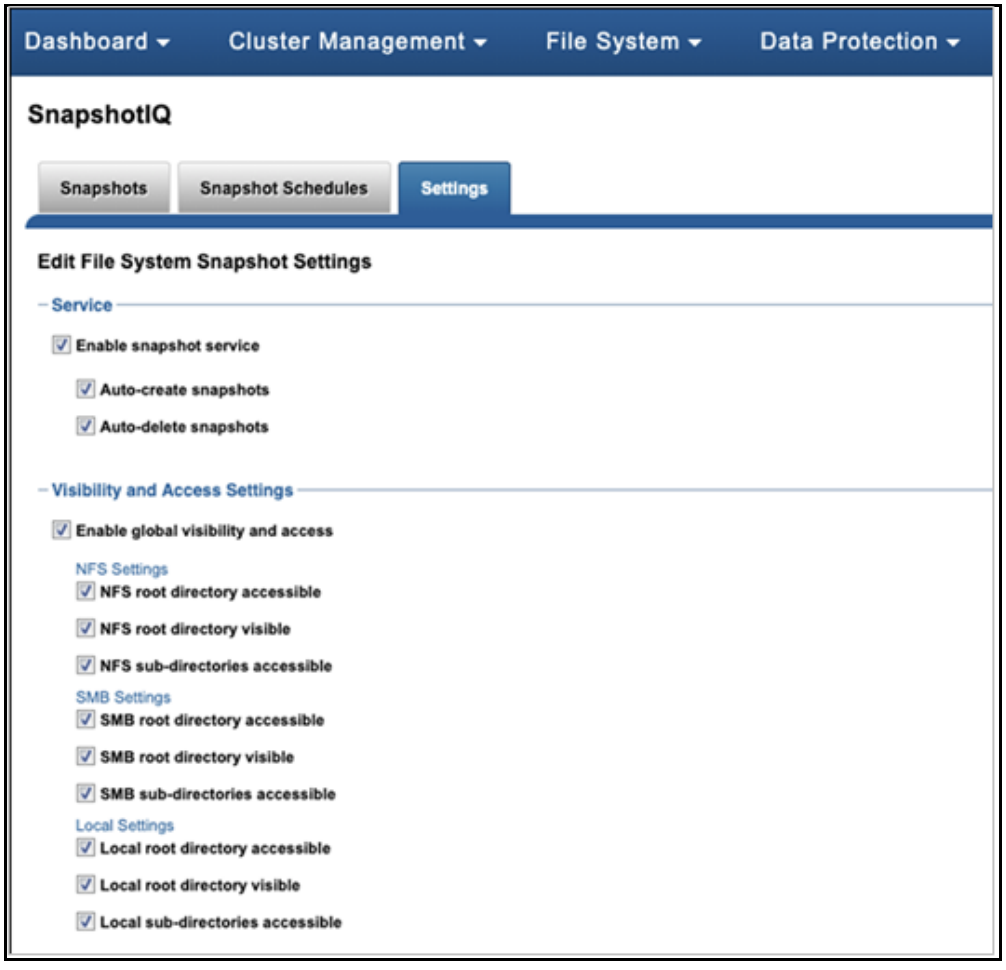
> **NOTE**: See the Cohesity Software Version Support Matrix below for the software version compatibility details.

- Configure the necessary Isilon permissions.
- Ensure that TCP/UDP ports 111, 300, 302, 304, 2049, 445, 8080, and 443 are open in the firewall between Cohesity and your Isilon device.

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

- Cohesity leverages SnapshotIQ to perform the backup of the Isilon source. Therefore, ensure to enable the SnapshotIQ license with the following settings on the Isilon cluster:
  - Enable Snapshot Service
  - Enable global visibility and access

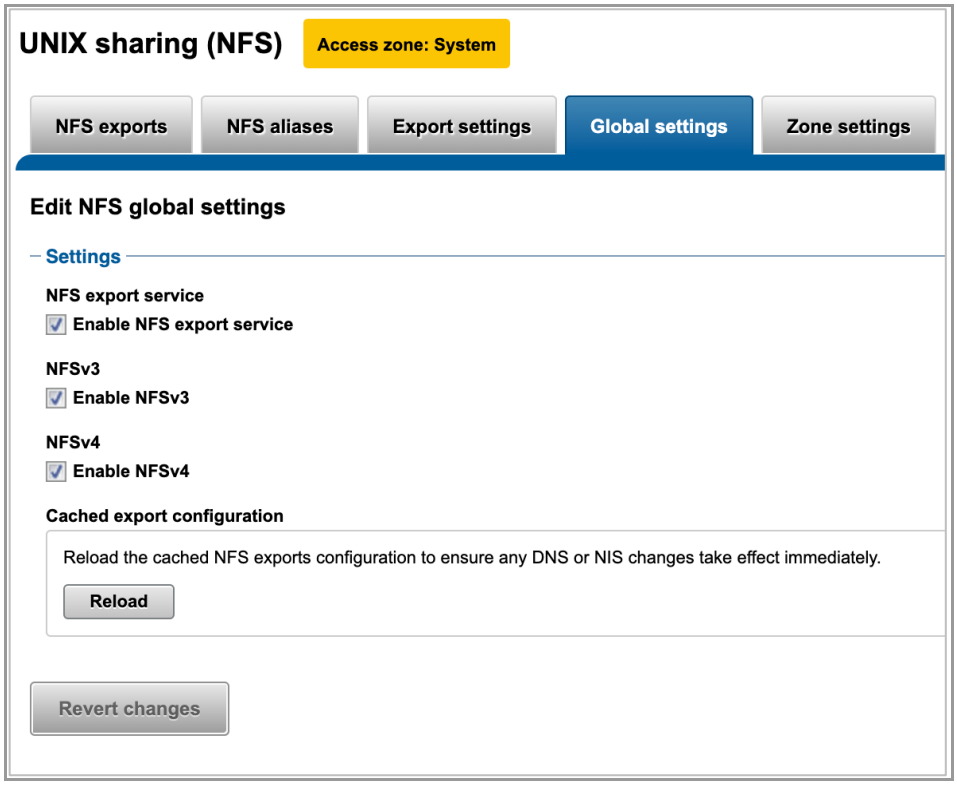
> **NOTE**: When enabling the Snapshot service and Global visibility and access, the settings under these options namely Auto create snapshot, Auto delete snapshot, NFS setting, SMB settings and Local settings are also enabled by default. These sub settings are not required by Cohesity and can be disabled if desired.



- Ensure NFS v3 is enabled for NFS export backups.

  NOTE:

  - Cohesity supports NFS v3 and SMB v2, or v3 for data protection.
  - Cohesity will treat NFS v4 exports as NFS v3 and perform backup via NFS v3.



Cohesity Software Version Support Matrix

Cohesity supports Isilon backup via both NAS adapter and Generic NAS. See Cohesity Support Matrix for version compatibility details.

Configure Isilon User with Backup/Restore Permissions

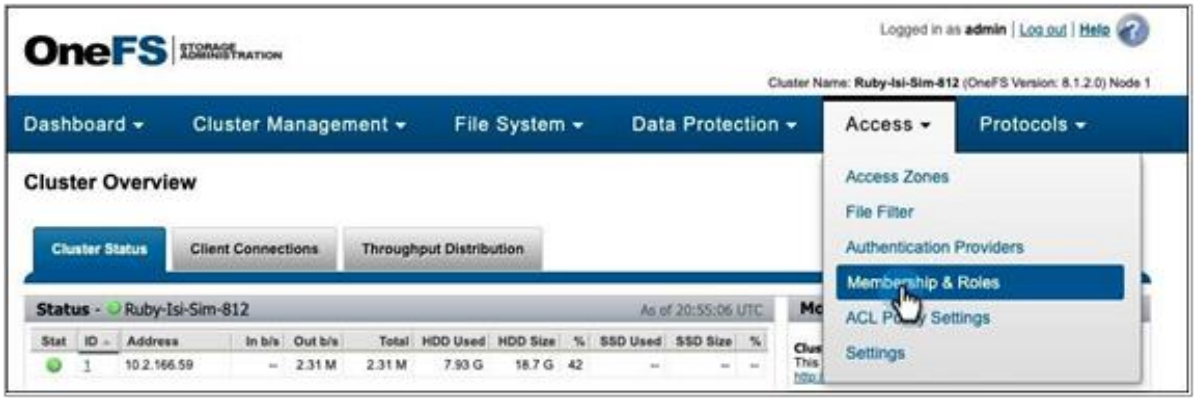
Cohesity DataProtect does not require administrator privileges on your Isilon cluster. It requires only the permissions necessary to back up and restore your Isilon data, as listed in Table 3 below.

Table 3: Required Minimum Permissions on Isilon

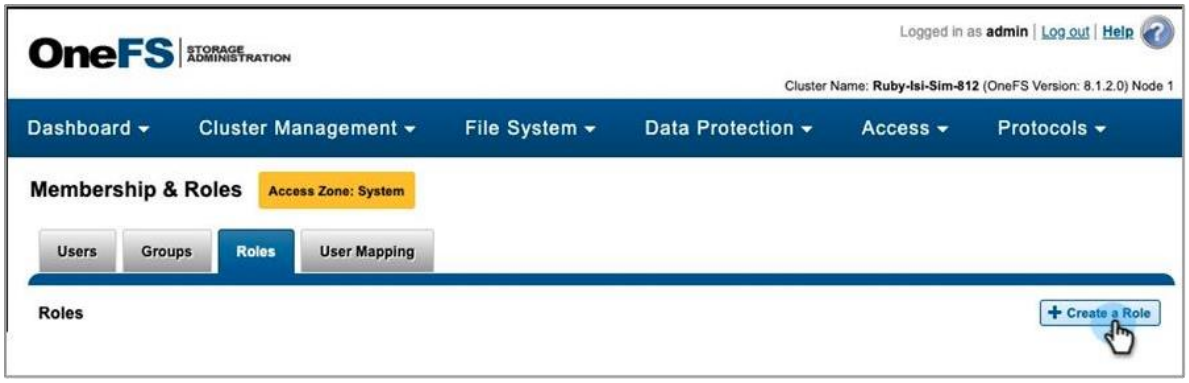
ACCESS	PERMISSION NAME	DESCRIPTION	PROTOCOL
Read-only	Platform API	For access to Isilon's APIs.	SMB/NFS
	Auth	To verify users and passwords.	
	Cluster	To obtain cluster identity and settings.	
	Network	To obtain the network interfaces.	
	SMB	To read the settings in the SMB server.	
Read/Write	Job Engine	To read and write Changelist jobs.	
	Snapshot	To fetch, create, and delete snapshots for shares and exports.	
	NFS	To read and write settings to and from the NFS server.	

To configure permissions on Isilon:

1. Log in to Isilon UI.
2. Navigate to **Access** > **Membership & Roles**.

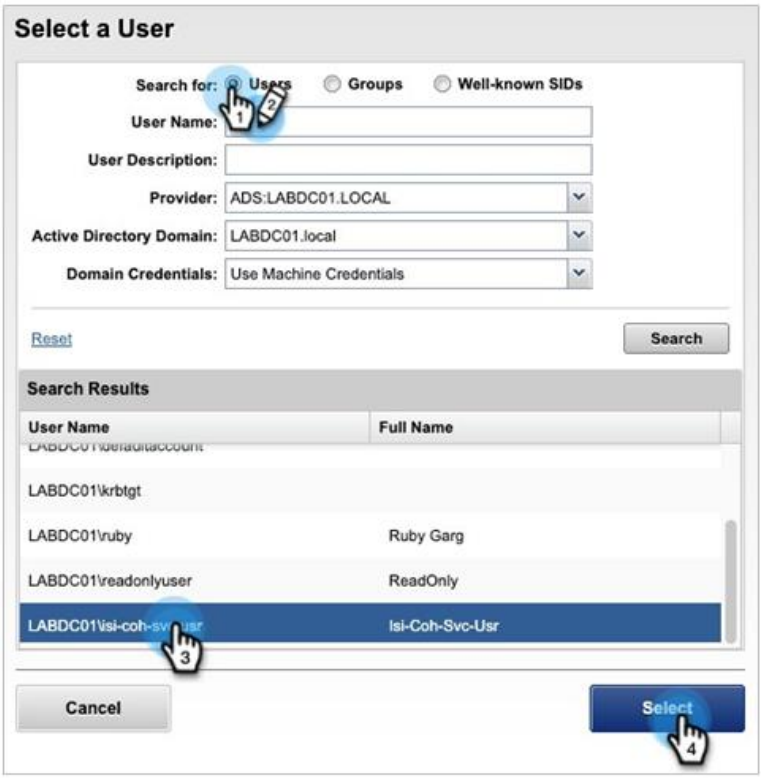


3. Under the **Roles** tab, click **Create a Role**.



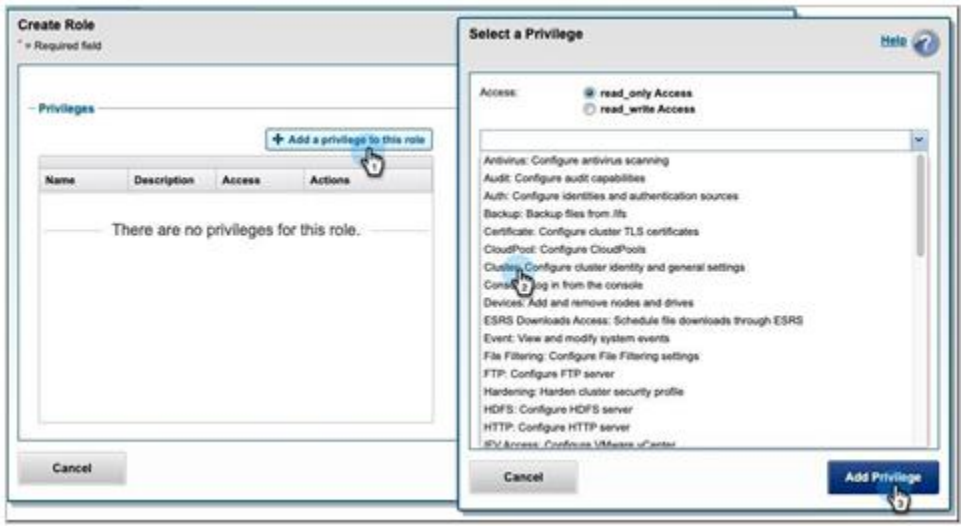
4. Enter **Role Name** and **Description** in the **Edit Role Details** screen and click Add a member to this role.

5. Under **Search for**, select **Users** and enter a search string for the user account you will use to register Isilon in Cohesity. Select that user from the list and click **Select**.

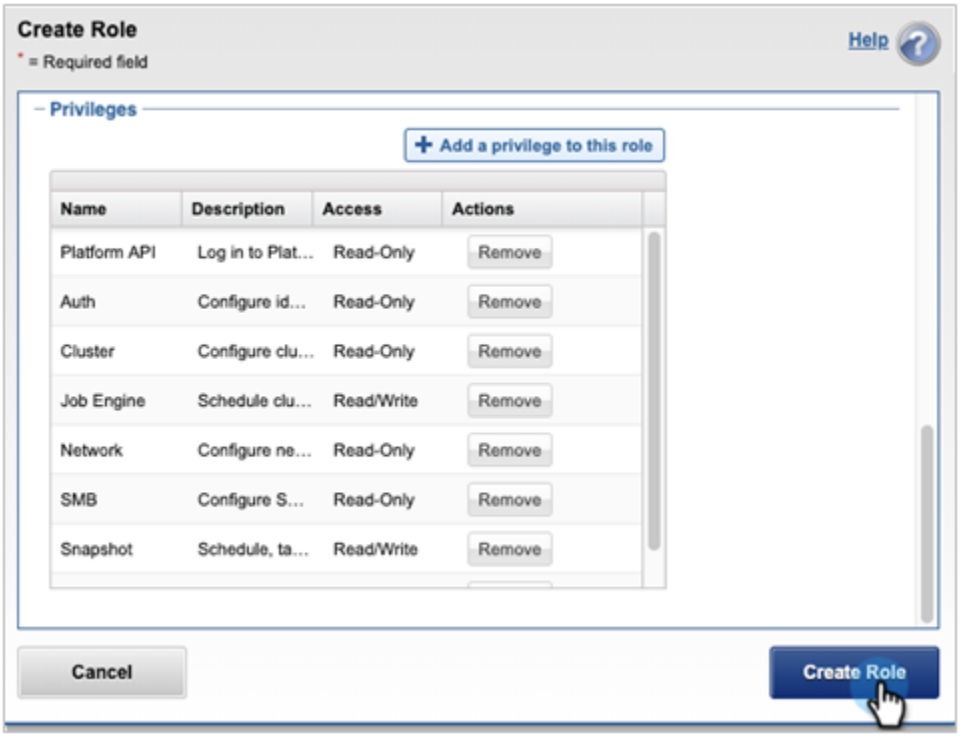


NOTE: Cohesity supports all three providers (Local, File, and ADS).

6. Scroll to the **Privileges** section, click **Add a privilege** to this role, and add all the privileges listed in Table 3 above.



7. Click **Create Role**.



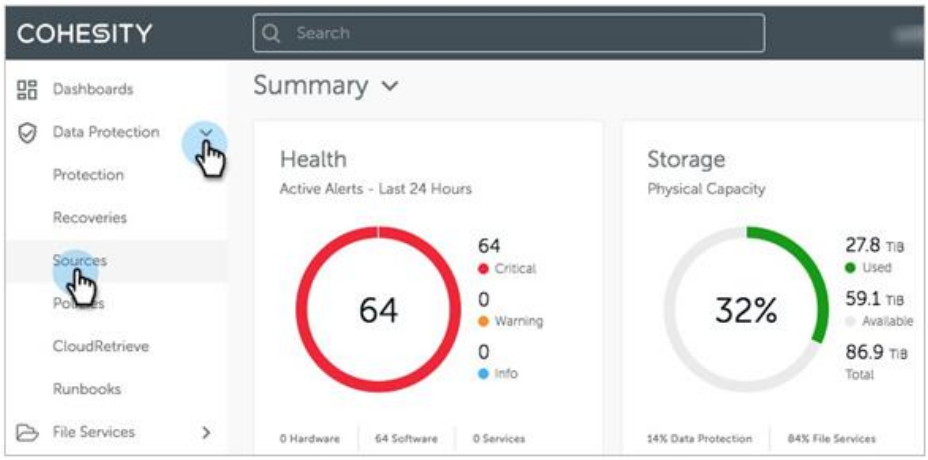
You have created the Isilon role you will use to register the Isilon cluster in Cohesity next.

> **NOTE**: Alternatively to the above, you can also use the PowerShell script to create the user with required permissions.

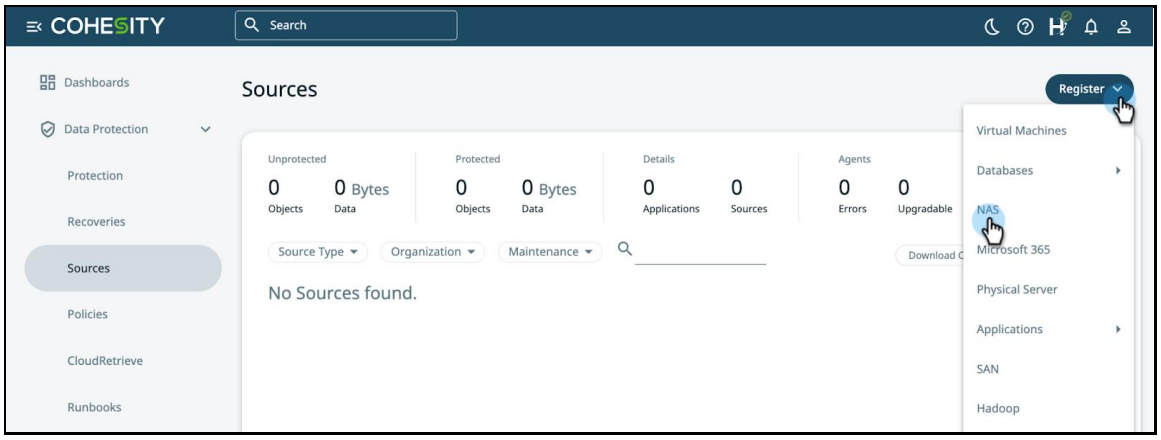
Register Your Isilon Cluster as a Source in Cohesity

Once the prerequisites are satisfied, you can register your Isilon 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 **Isilon**. Enter the NAS registration details (using Table 4 below) and click **Register**.

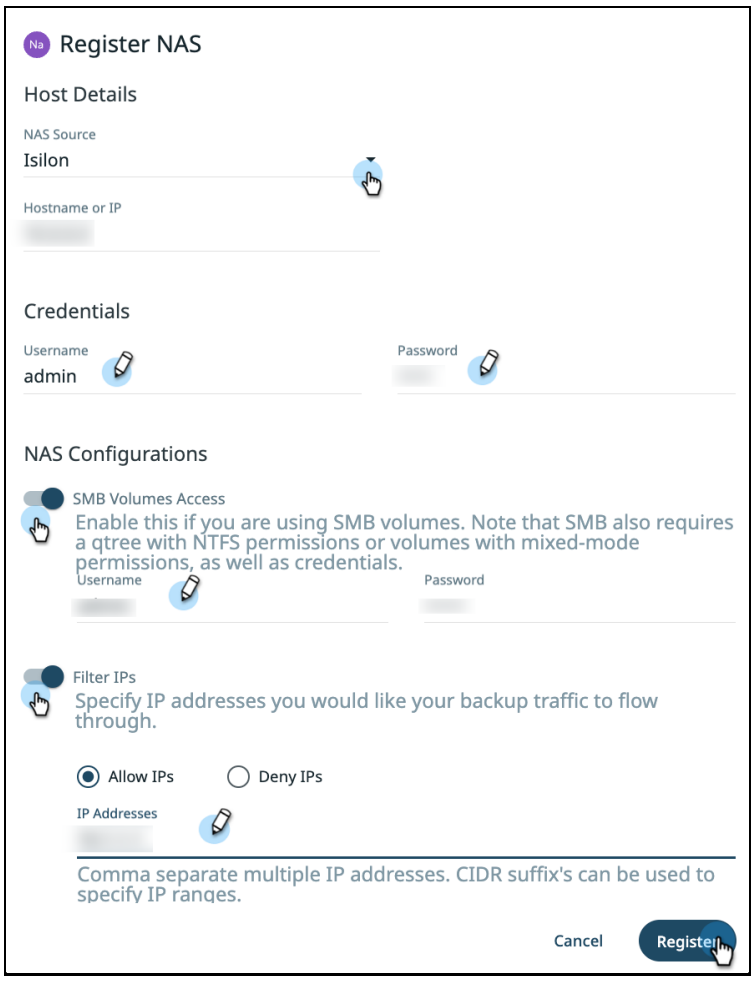
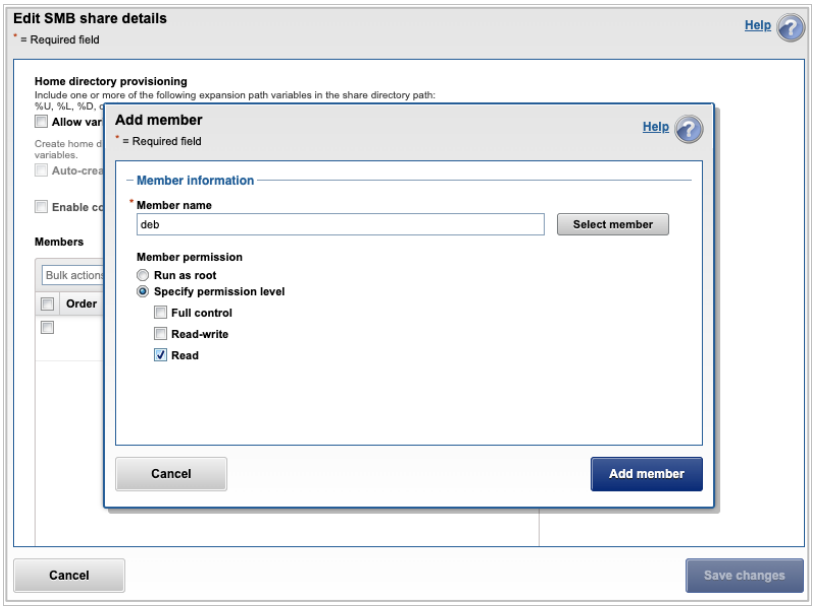


Table 4: Register Isilon with Cohesity

FIELD NAME	DESCRIPTION
Hostname or IP Address	Provide the management IP address or host name of the Isilon cluster.
Username	The user account that you configured with the required permissions on the Isilon cluster. **NOTE**: If you use a domain username, use format: **fully_qualified_domain_name\username. For example, xydc.local\user1**
Password	Password for the provided username.
SMB Volumes Access	If you plan to protect Isilon SMB shares, toggle to enable this option and provide the local or Active Directory (AD) user credentials that allow at least read access to the Isilon SMB share. To do so: a. On Isilon, Navigate to Protocols > Windows Sharing (SMB). b. Edit SMB Share to be backed up. c. Click Add User or Group. d. Select at least Read permission for the selected member. e. Click Add member.  **NOTES**: • You can assign the local or AD user to the built-in “BackupAdmin” role to permit the user to read the SMB data for backup without modifying the access control lists (ACLs). • See Appendix C: BackupAdmin Role and Access Zones for details.

FIELD NAME	DESCRIPTION
Filter IPs	Enable this option to filter the IP addresses of the Isilon cluster. By filtering IP addresses, you can allow or deny the communication of the Cohesity cluster to specific IP addresses or subnets of the Isilon cluster. To filter the IP addresses of the Isilon cluster, select one of the following options: • **Allow IPs:** Select this option and specify the IP addresses of the Isilon source through which communication to the Cohesity cluster must happen. You can provide the IP addresses in a comma-separated list or in a CIDR format. • **Deny IPs:** Select this option and specify the IP addresses of the Isilon source through which communication to the Cohesity cluster must not happen. You can provide the IP addresses in a comma-separated list or a CIDR format.

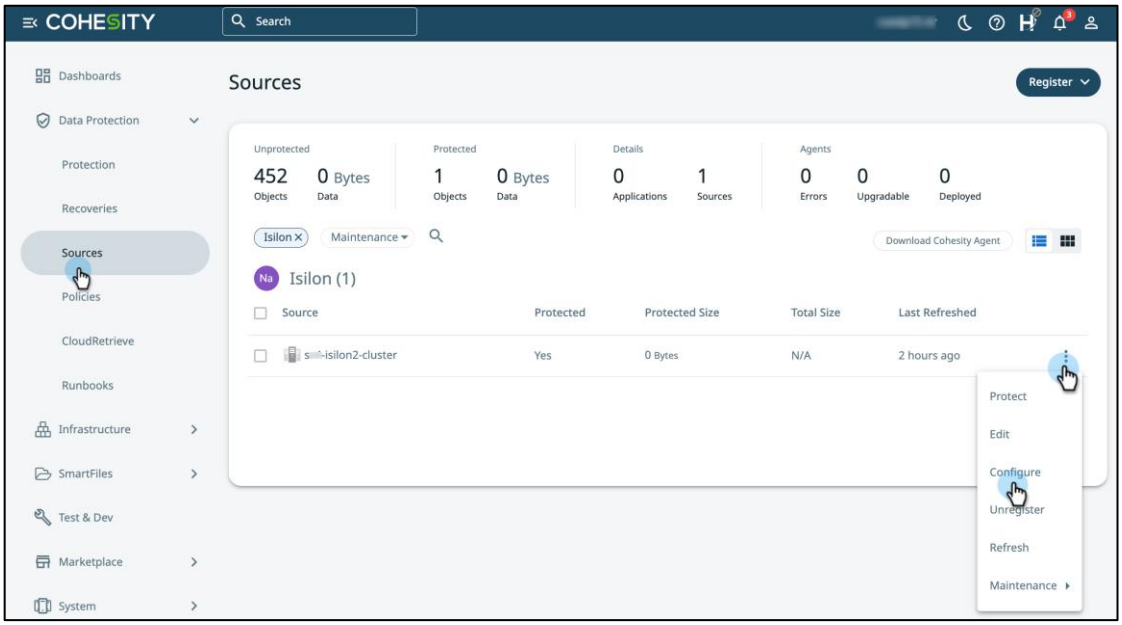
See Register or Edit NAS in the online Help for more.

Configure Smart Connect

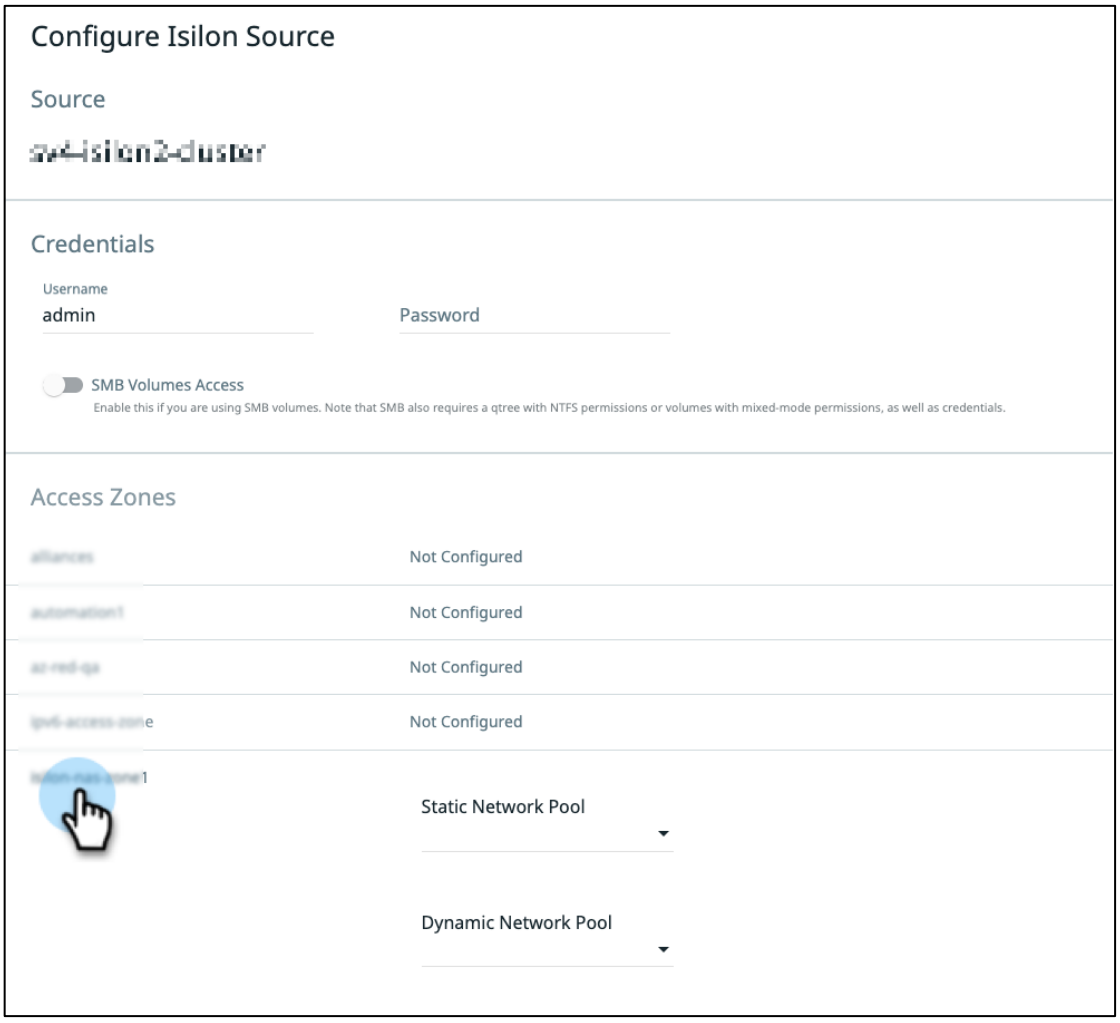
If you wish to use Smart Connect you may configure it after registering the Isilon source. Please note that this needs to be configured on a per Access Zone basis.

To configure Smart Connect:

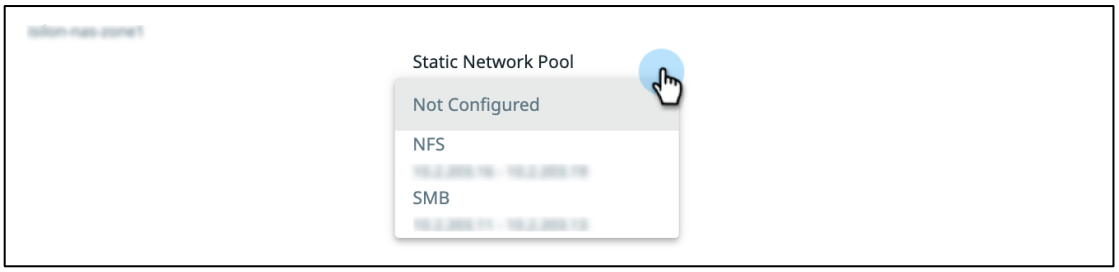
1. Log in to Cohesity and navigate to **Data Protection** > **Sources.**
2. Select the registered Isilon source, click the 3 dots on the right and click **Configure**.



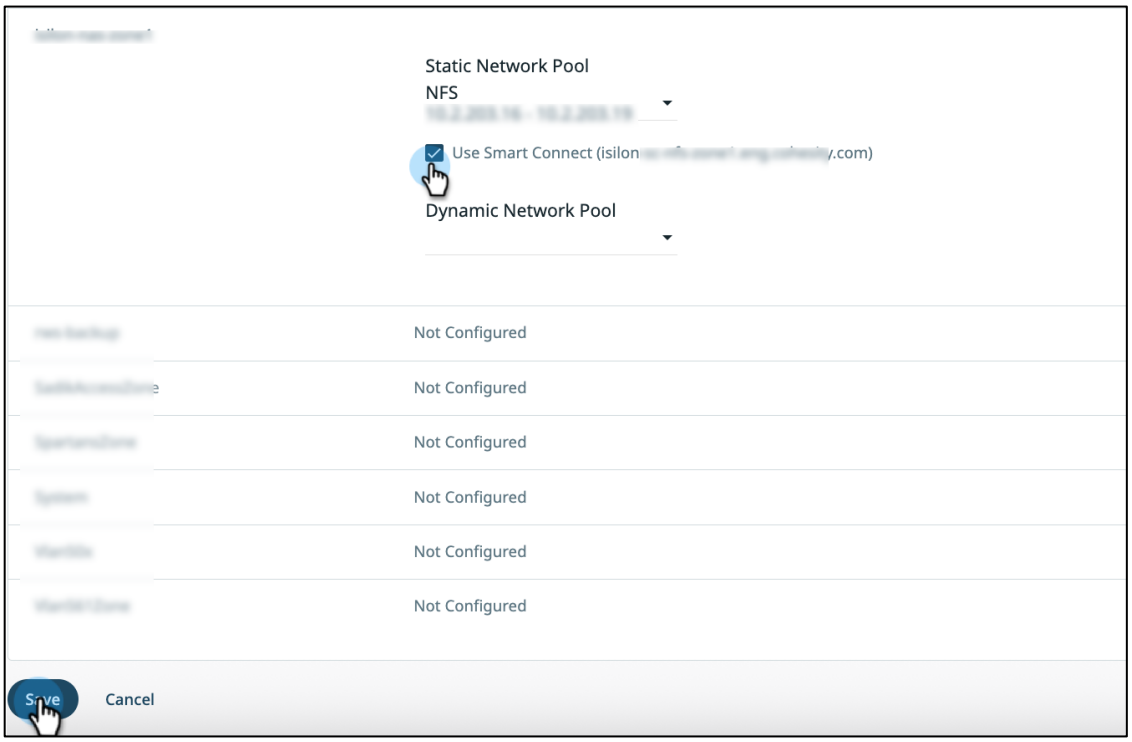
3. On the Configure Isilon Source page, select the access zone on which you intend to configure Smart Connect.



4. From the **Static Network Pool**, select the required pre-configured pool.



5. Enable the "**Use Smart Connect**" option and click **save**.



Your Isilon NAS cluster is now a registered source on Cohesity. To protect it, create a Cohesity Protection Group below.

Choose a Cohesity Protection Policy

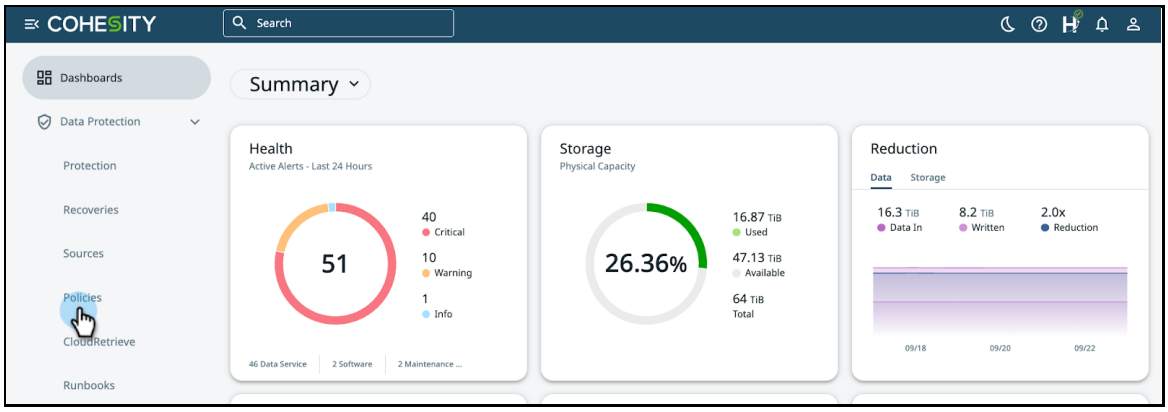
In Cohesity, Protection Groups use Protection Policies. Protection Policies reflect business needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs), while a Protection Group defines operational requirements, such as which source objects 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.

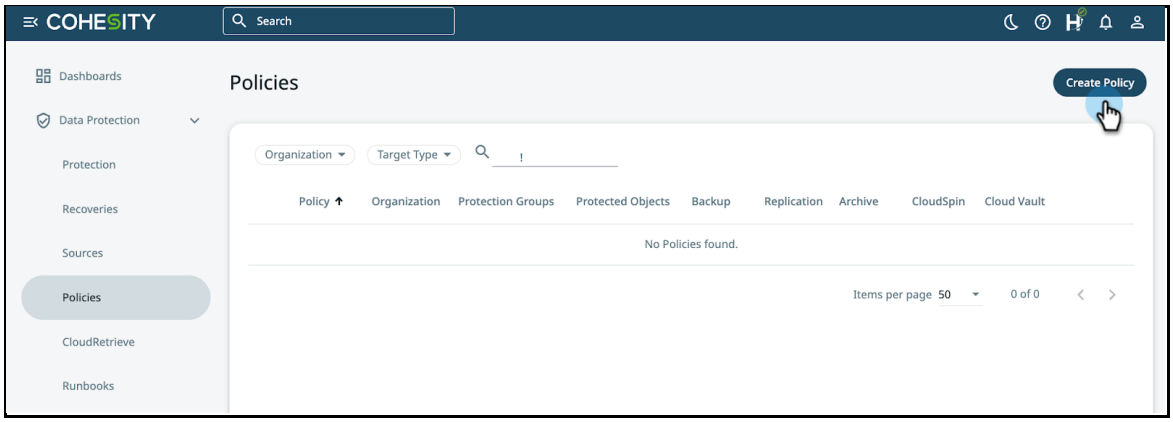
NOTE: See our recommendations for protecting Isilon NAS data in Best Practices below.

To create a custom Protection Policy:

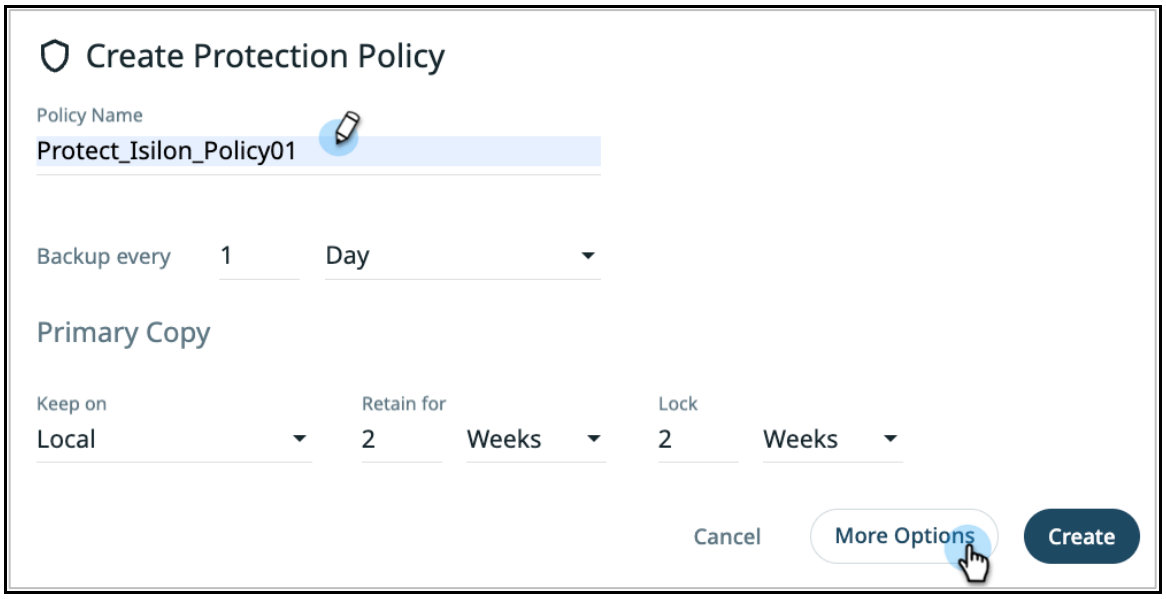
1. Log in to Cohesity and navigate to **Data Protection** > **Policies**.



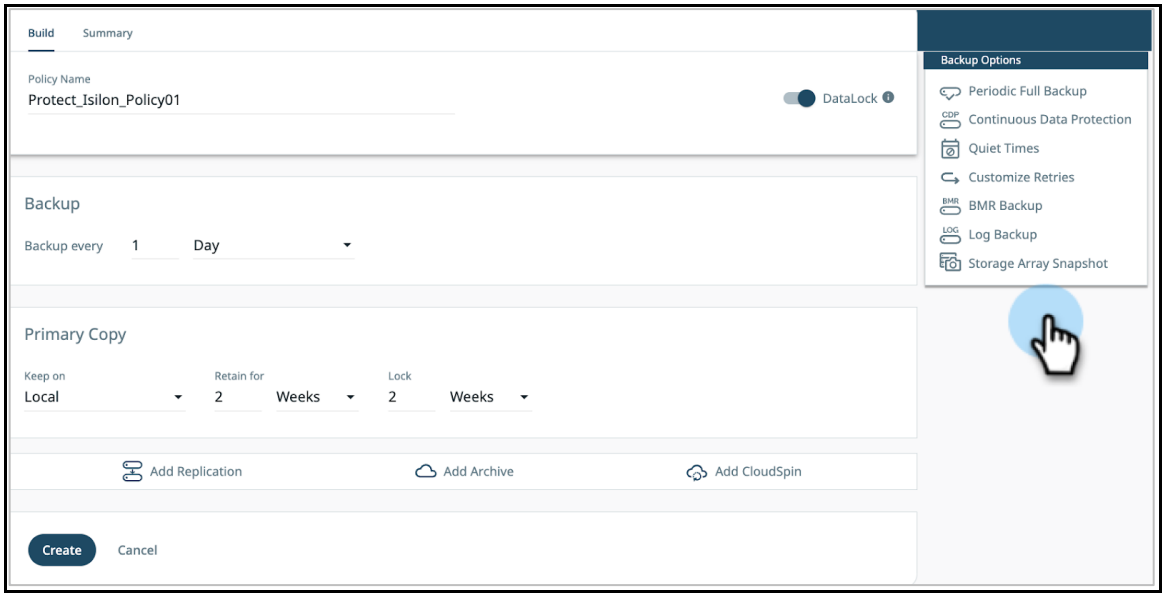
2. Click **Create Policy** located at the top right of the page.



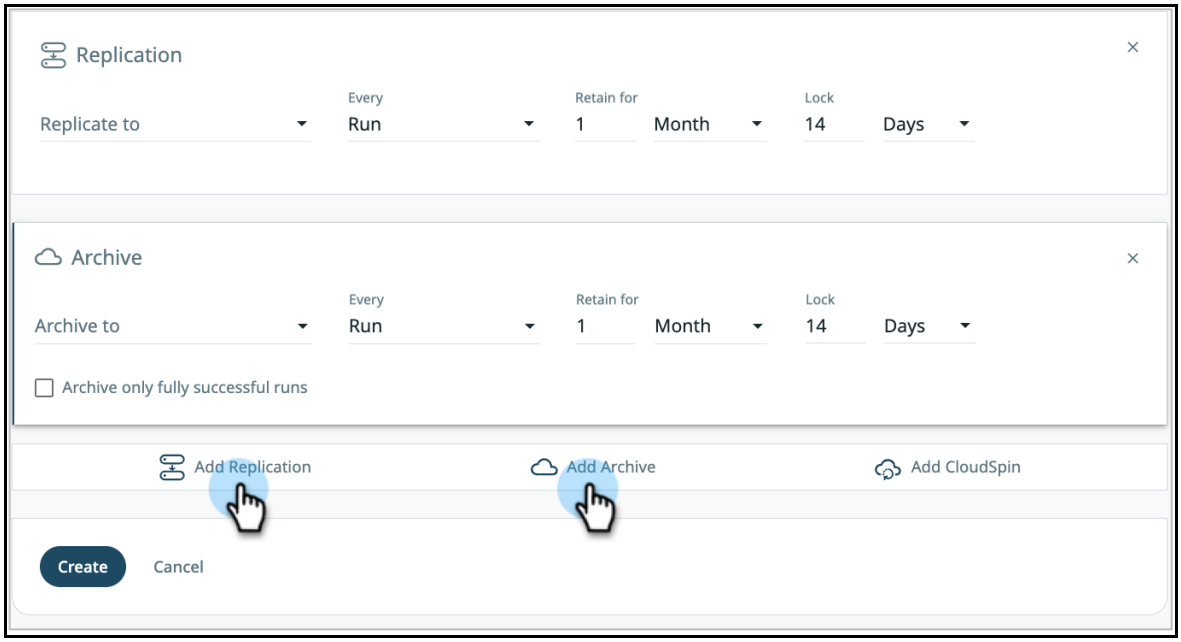
3. In the **Create Protection Policy** modal, enter a **Policy Name** and select the backup interval and retention times for the **Scheduled Backup**. Click **More Options** to configure the advanced settings.



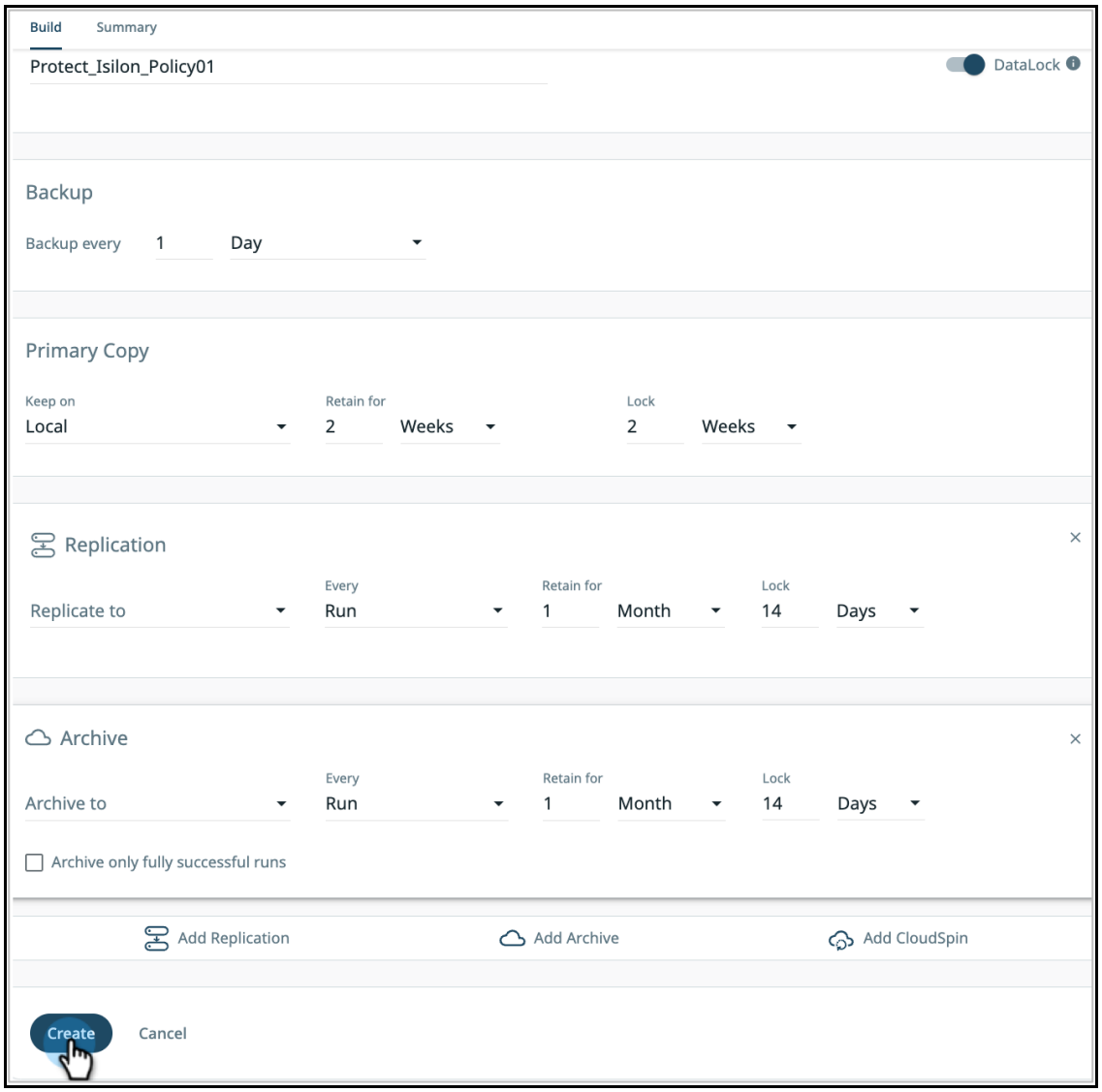
4. In the **Create Protection Policy** form, you can edit the **Retry Options**. If required, from the floating menu on the right, you can add **Periodic Full Backup, Define Quiet Times**, and more. When you do, you can configure the options for each as you add them.



5. If required, add **Replication** or **Archive** for your backed up Isilon 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.

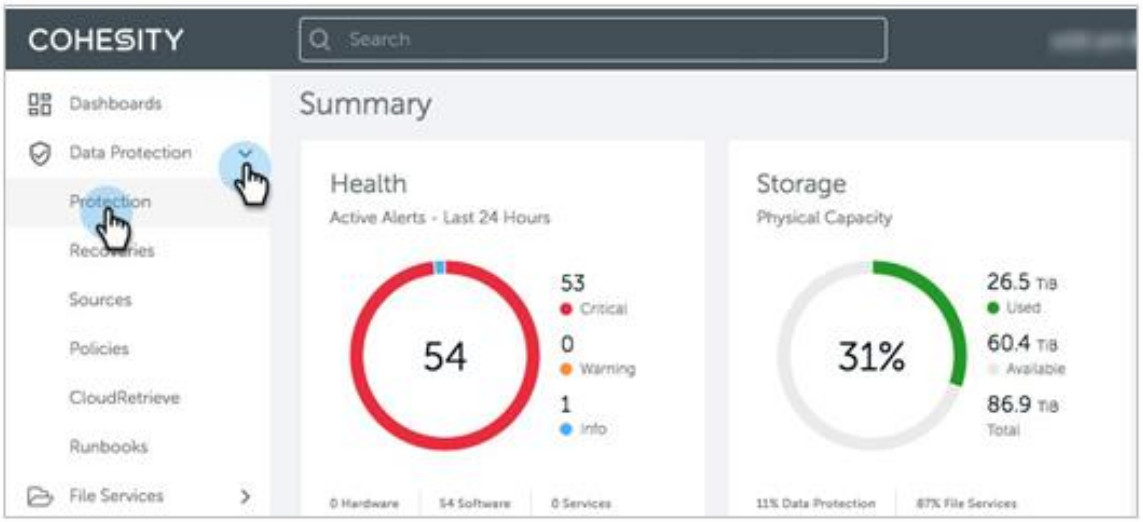
Create a Cohesity Protection Group

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.

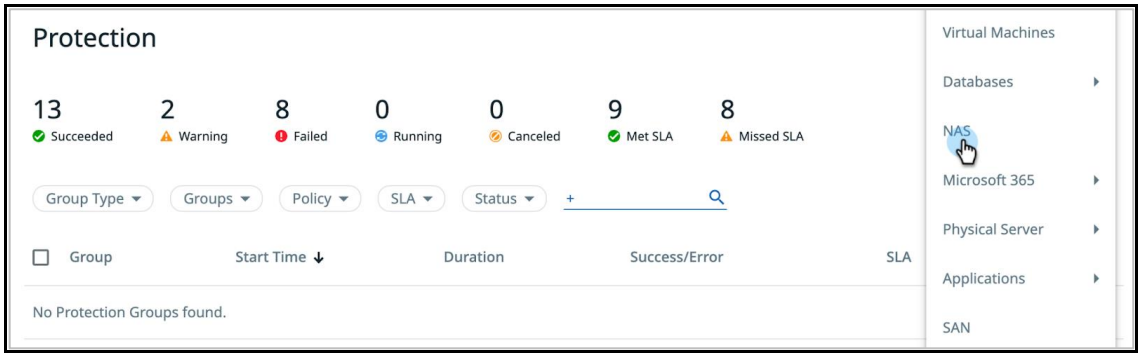
Multiple Protection Groups can use the same Protection Policy, but each Group can have only one Policy.

To create a Protection Group:

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

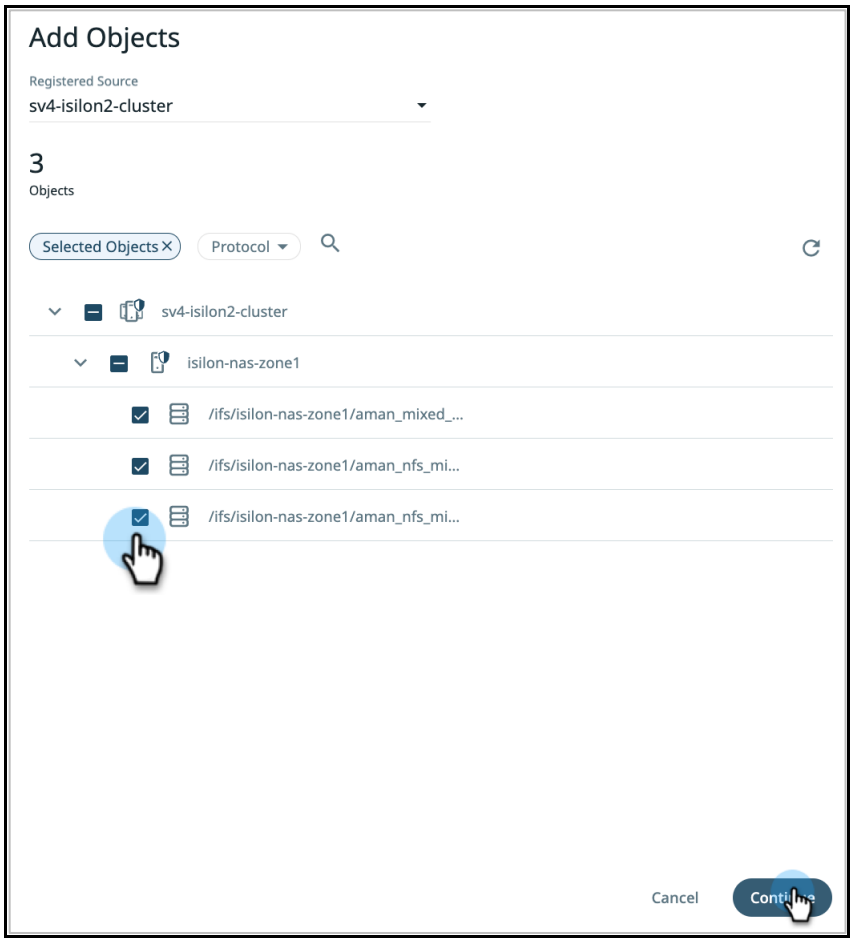


2. Click **Protect** on the top-right of the page and then select **NAS**.

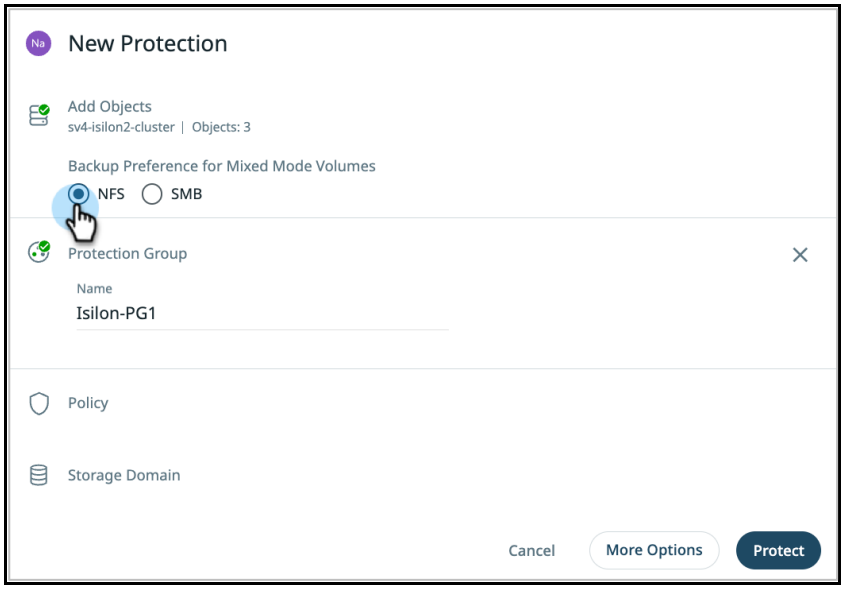


3. In the **New Protection** form, under **Source**, select the Isilon cluster you registered earlier, select the objects you wish to protect, and then click **Continue**.

> **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.

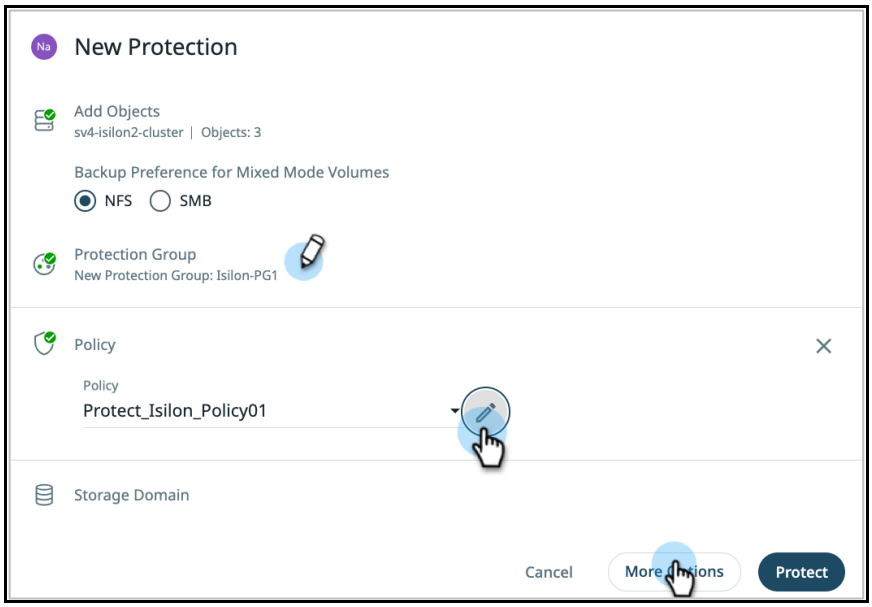


4. If the selected volumes include both NFS exports and SMB shares, select **Backup Preference for Mixed Mode Volumes**.

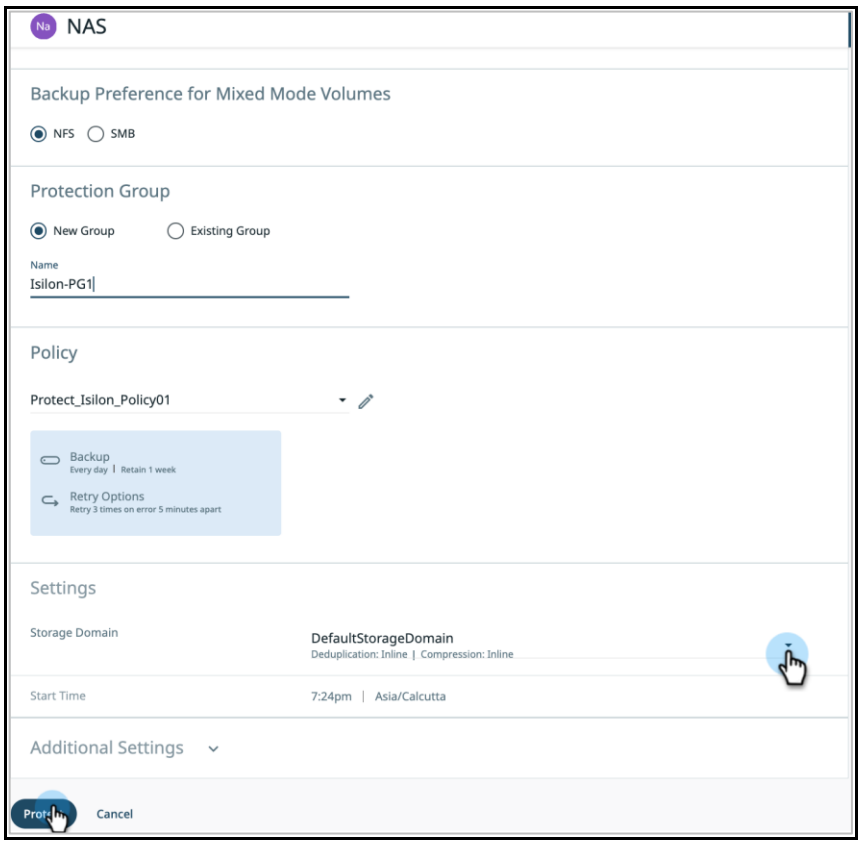


NOTE: For Isilon mixed volumes, Cohesity will back up both NFS POSIX ACLs and SMB access control lists (ACLs).

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



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



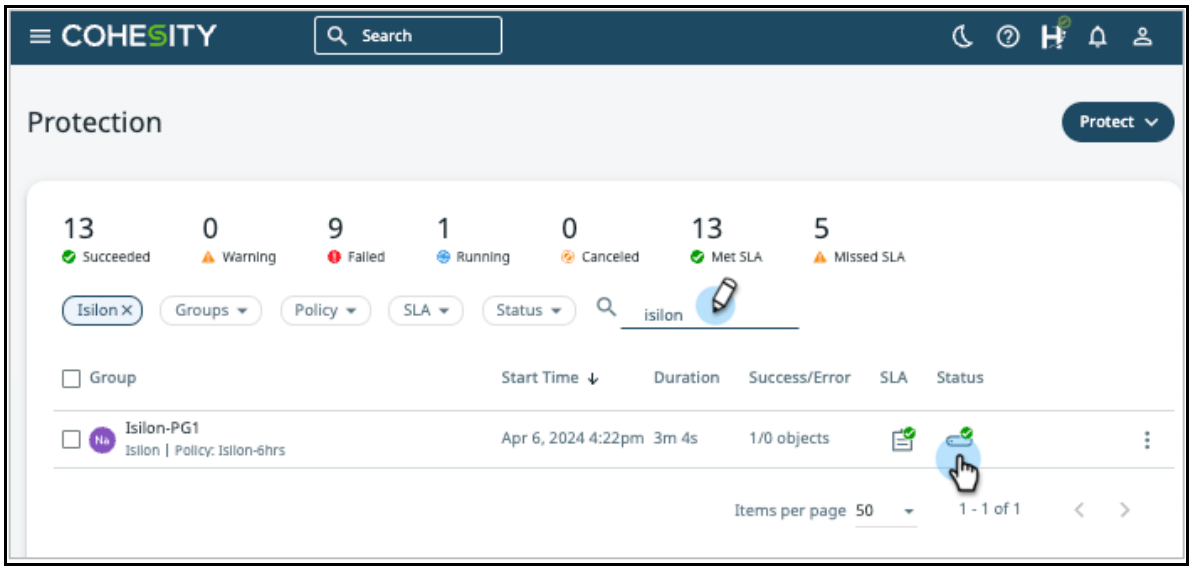
Your new Protection Group is now active and running.

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 Isilon Nas below.

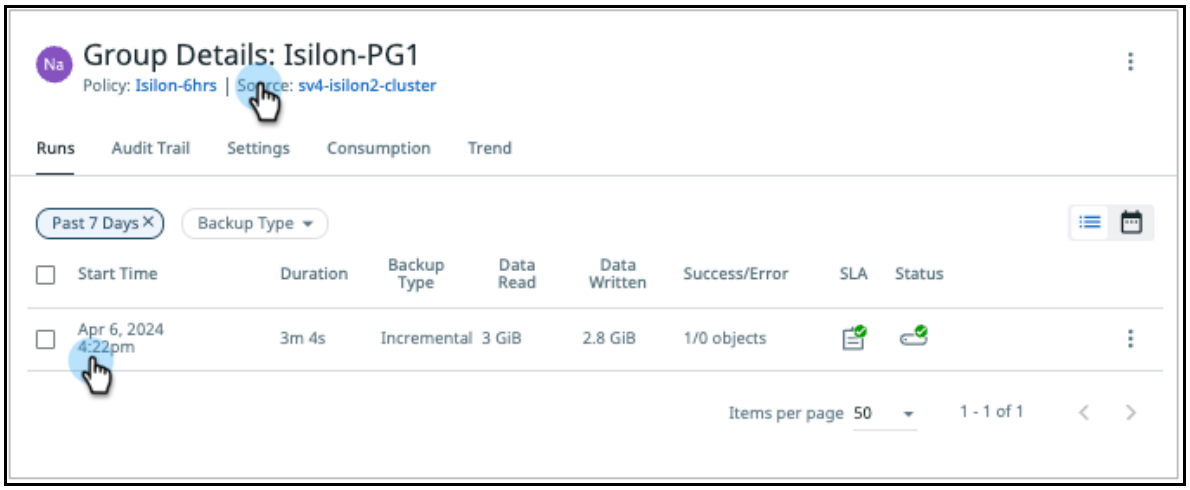
Check the Status of Your Protection Group

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

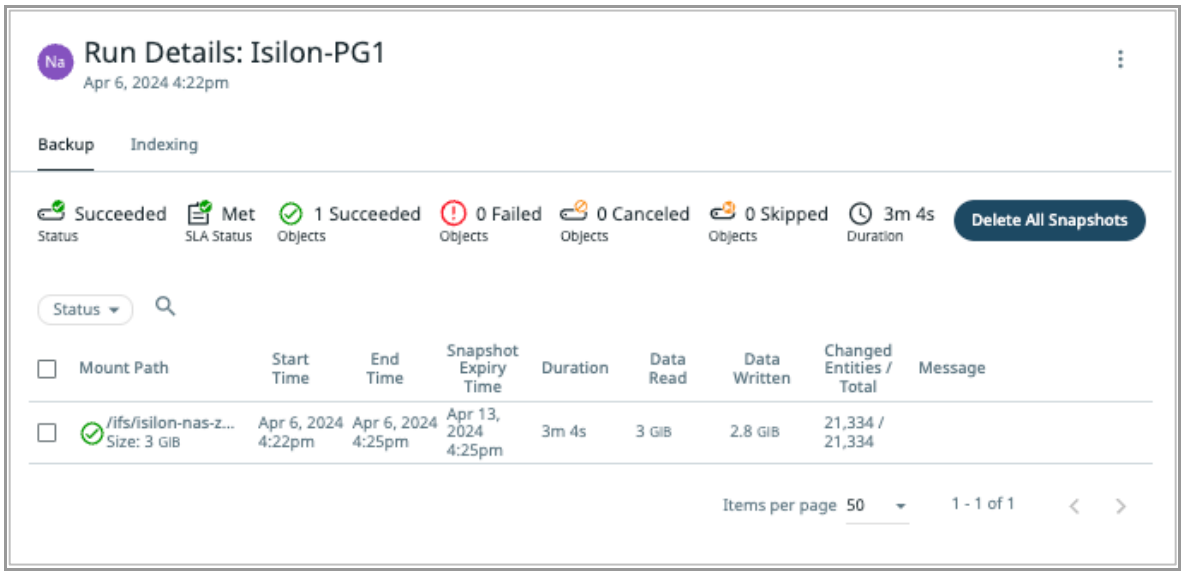
1. Navigate to **Data Protection** > **Protection**.
2. Enter a search term to find the Protection Group and click the **Status** column in that row to see its status details.



3. Click on the Protection Group name to view the Job runs.



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



Understanding Cohesity's Isilon Recovery Approach

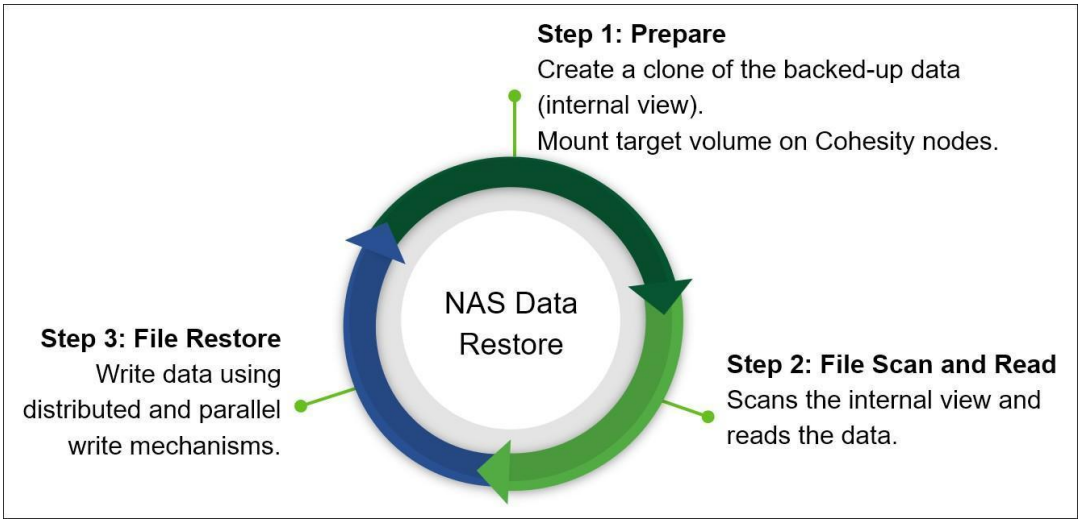
Isilon data recovery is essentially the rebuilding of Isilon data that is lost due to unfortunate incidents such as media or storage failure, application failure, data corruption due to power interruption, or data deletion due to human errors. Cohesity DataProtect offers efficient data recovery options 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 Isilon data from snapshots of storage volumes created earlier by a Protection Group. Restoring data for Isilon 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 Dell EMC Isilon cluster is backed up with Cohesity DataProtect, you can start a recovery task that restores specific Isilon 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 10: 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.

> **NOTE**: Before the write operation begins, the user account used to register the Isilon NAS device with Cohesity is checked for permission on the target. If permissions are not in place, the recovery task fails.

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

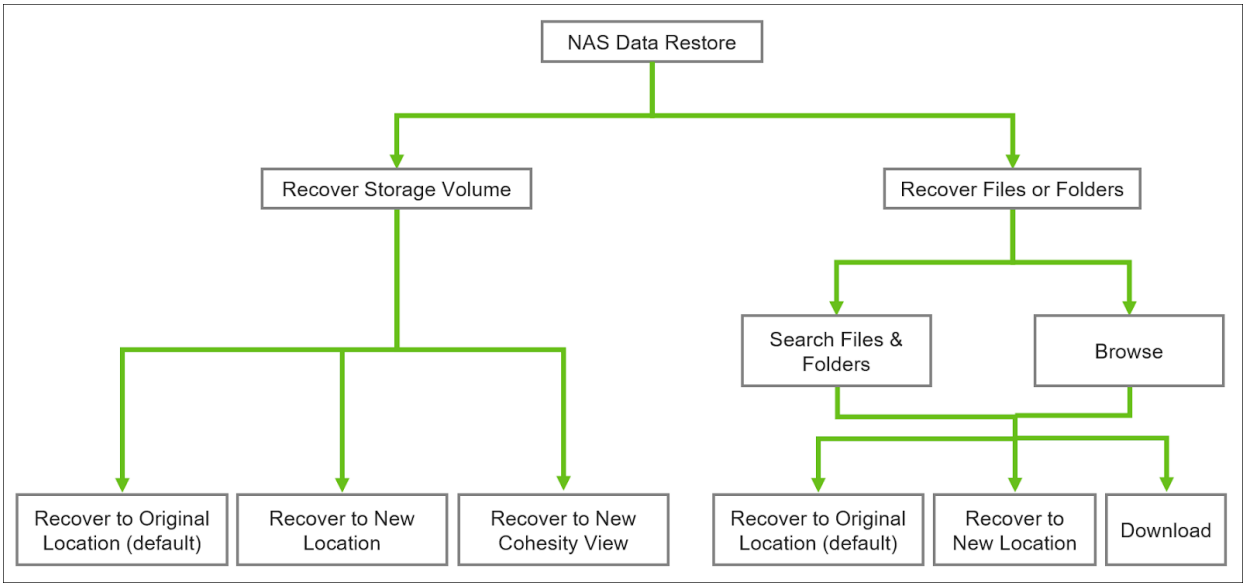
Recover Isilon Data with Cohesity DataProtect

Cohesity DataProtect offers two levels of recovery granularity for Isilon 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 11 illustrates the phases and choices you encounter in a typical NAS data restore workflow.

Figure 11: NAS Data Recovery Decision Tree



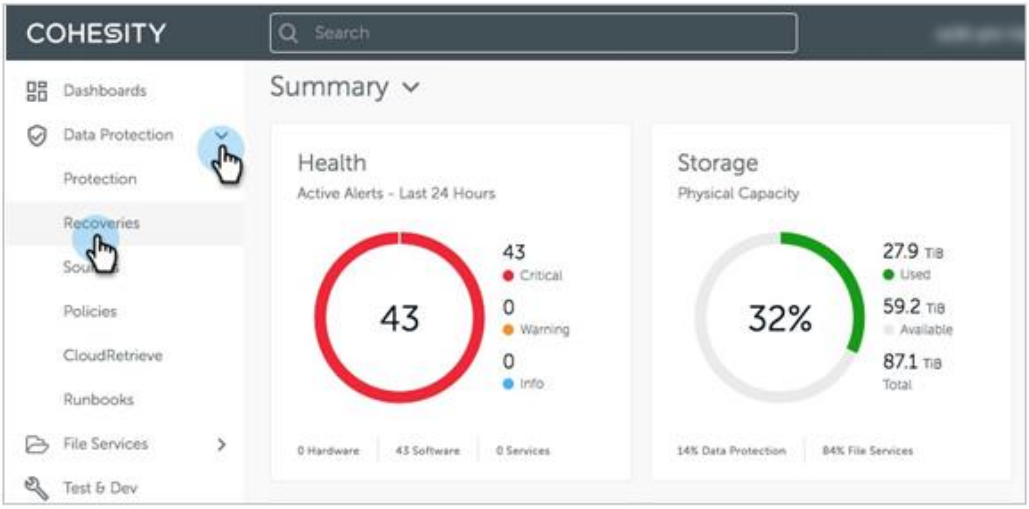
Recover Storage Volume

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

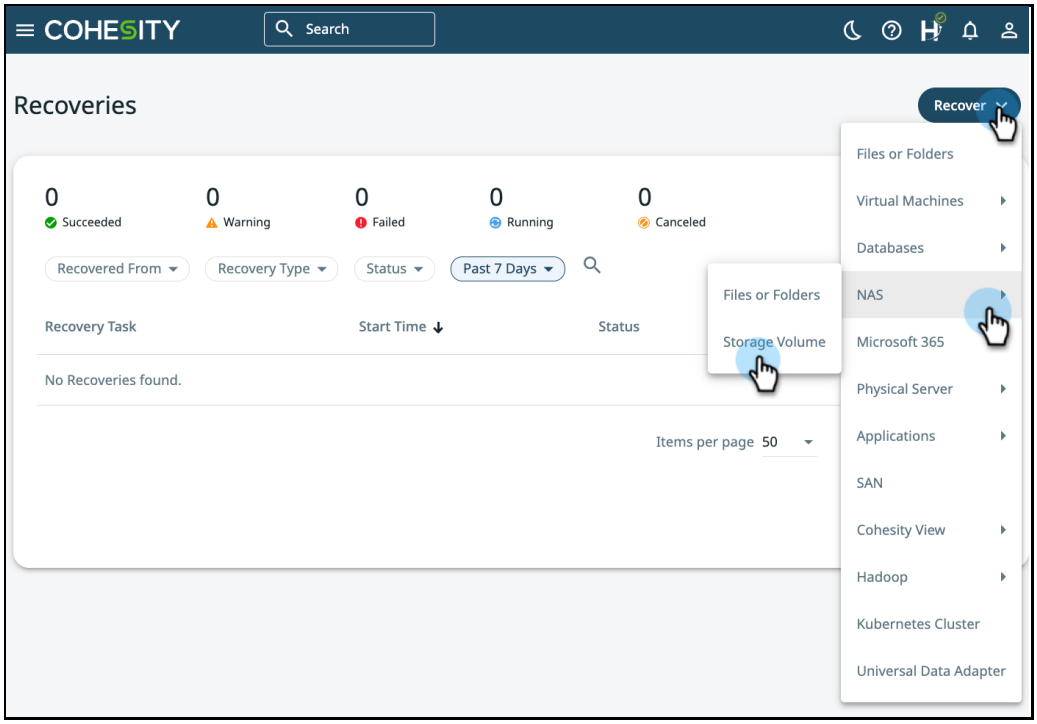
NOTE: Before recovering storage volumes, ensure that snapshots of those volumes exist in the Protection Groups on your Cohesity cluster.

To recover an Isilon storage volume:

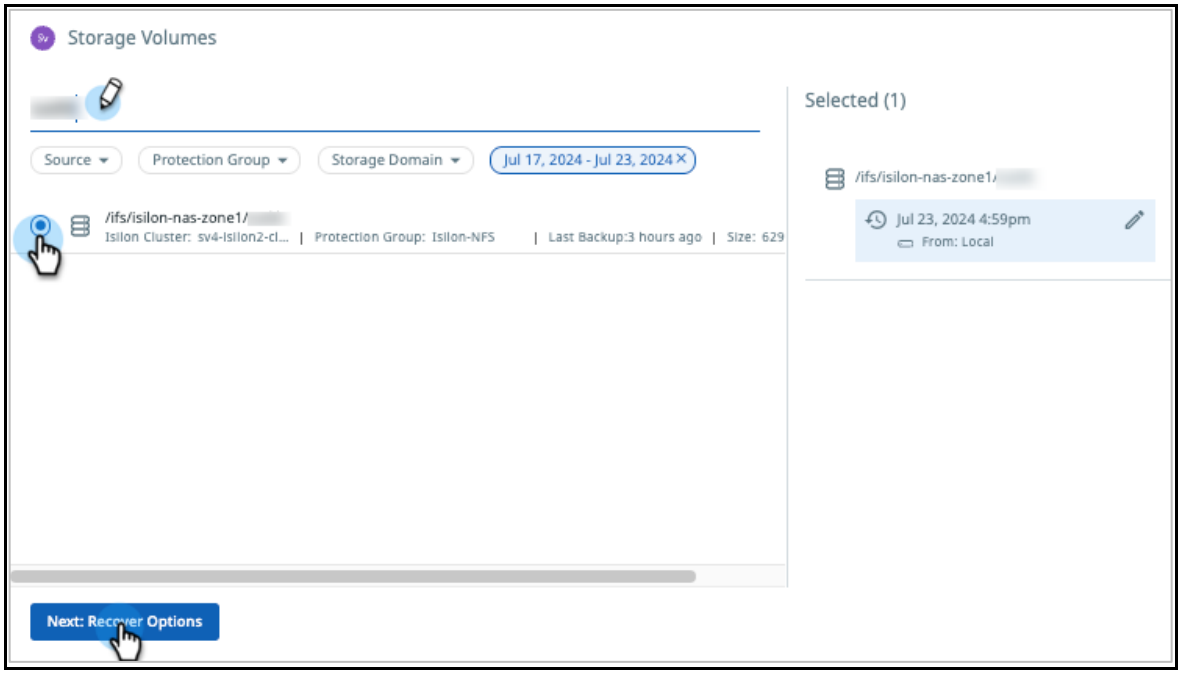
1. Log in to Cohesity and navigate to **Data Protection** > **Recoveries**.



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 Isilon 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 an Isilon volume to its original NAS target, select **Original Location**. Edit the **Recovery Options** as necessary and click **Recover**.

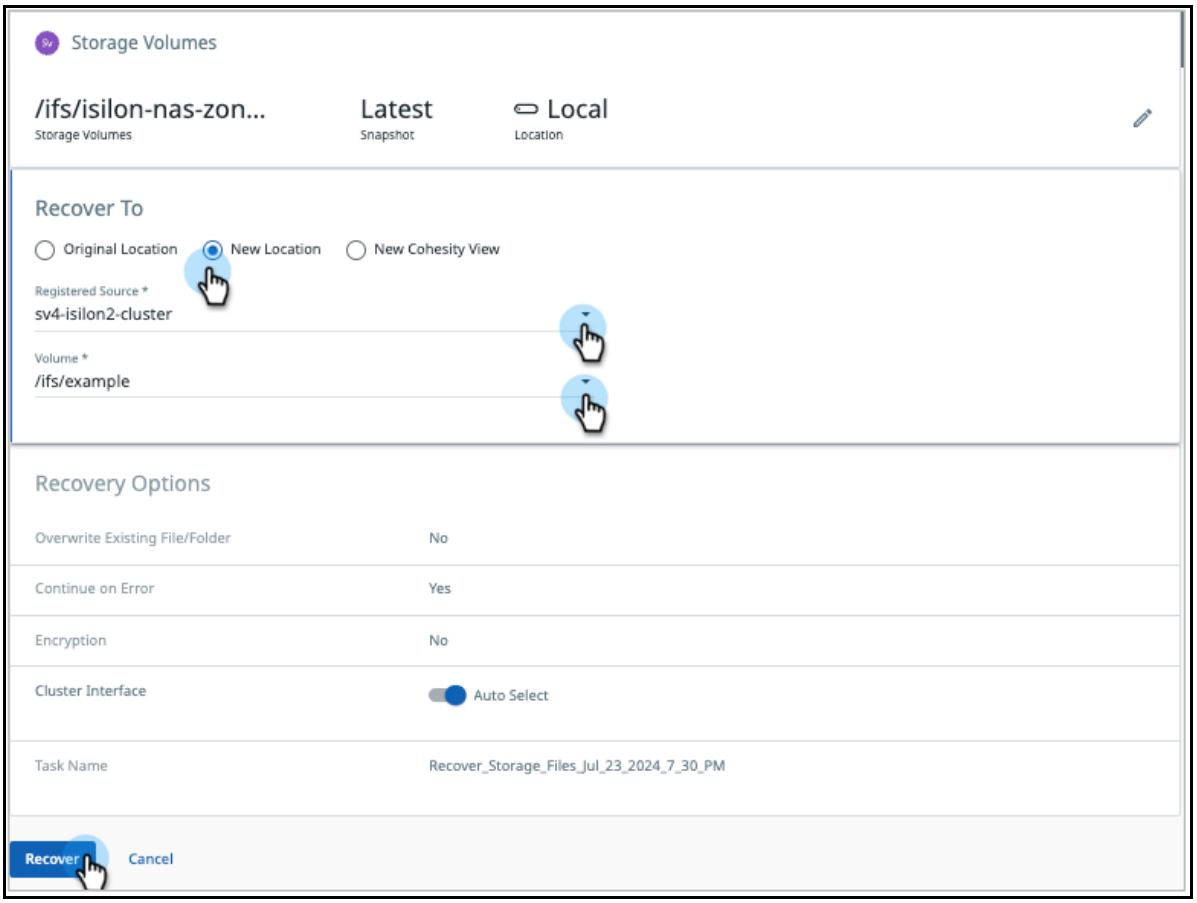
Refer to Recover Storage Volumes to the Original Location in the online Help for details on the Recovery Options.

Recover to a New NAS Location

If some of your source data becomes unavailable or you need to migrate it, you can recover it to a new NAS location. With this option, you can restore your Isilon device's 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 must be registered as a source in Cohesity.

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



Refer to 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.

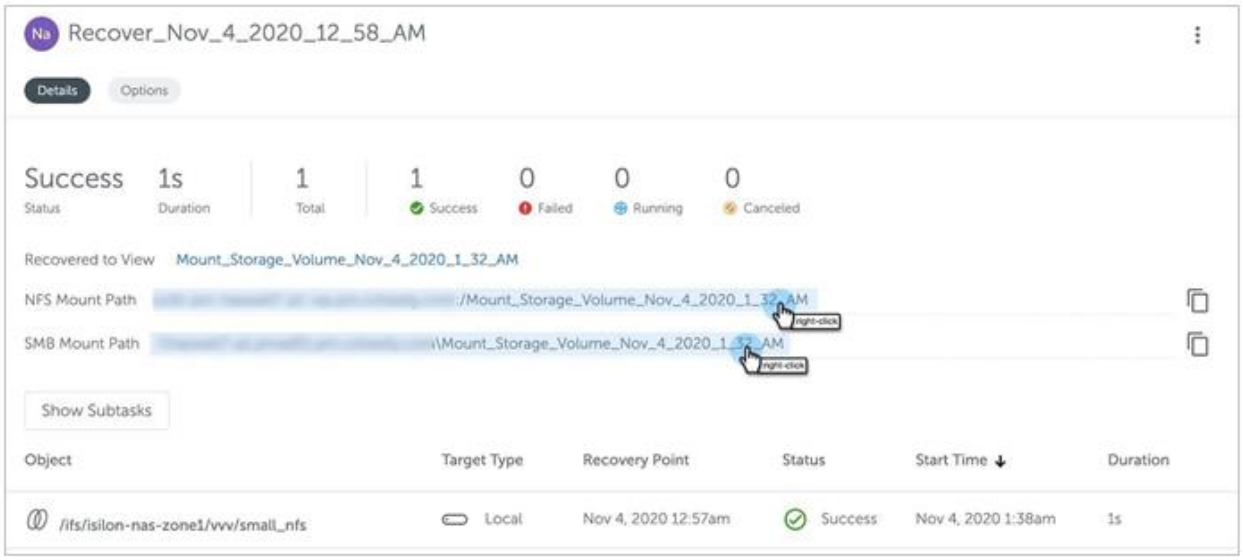
To recover the Isilon volume to a Cohesity View, select **New Cohesity View**, edit the automatically assigned **Name** for the new View if necessary, and select the most QoS Policy that is most appropriate for the workload. Edit the **Recovery Options** as necessary and click **Recover**.

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**.
- This workflow is not supported for NAS backups performed using the NFS4.1 protocol.

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 12: 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 Isilon 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.

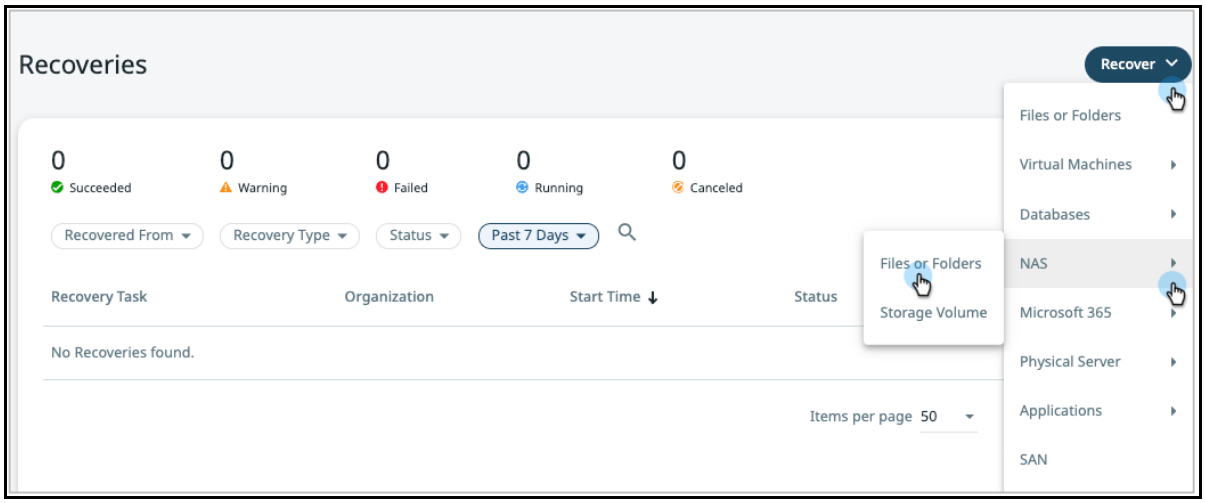
> **NOTE**: Before you try to recover files or folders, ensure that snapshots of these files and folders appear on the Cohesity cluster in a Protection Group.

To recover files and folders from Isilon 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

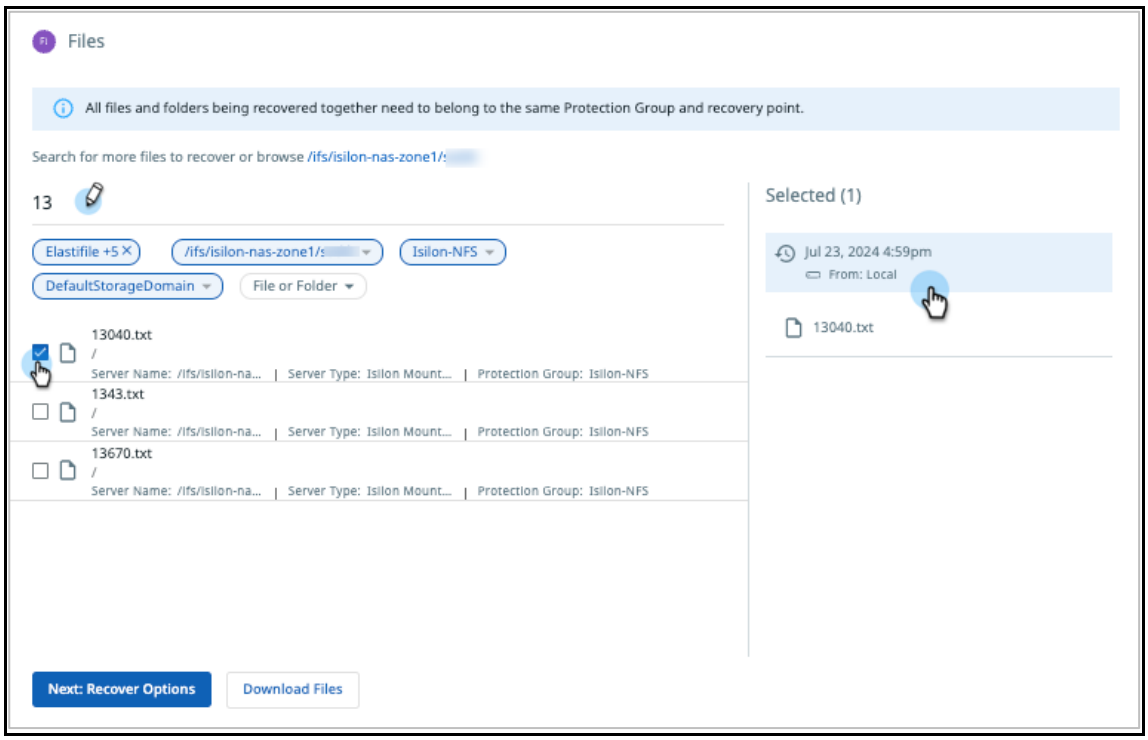
The Files or Folders search option allows you to search and recover files using file or folder names from any backup available on Cohesity.

NOTE:

- To 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:

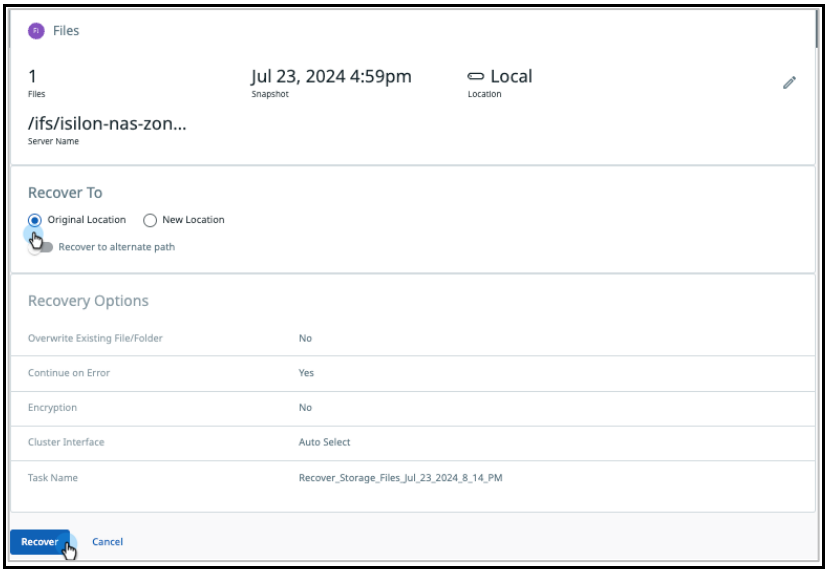
1. Enter the full or partial file name or path and select the file from the search results. By default, the latest snapshot is selected. To recover from a different recovery point, click the **Edit** pencil icon in the right pane under **Selected** and choose the snapshot you need.



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:

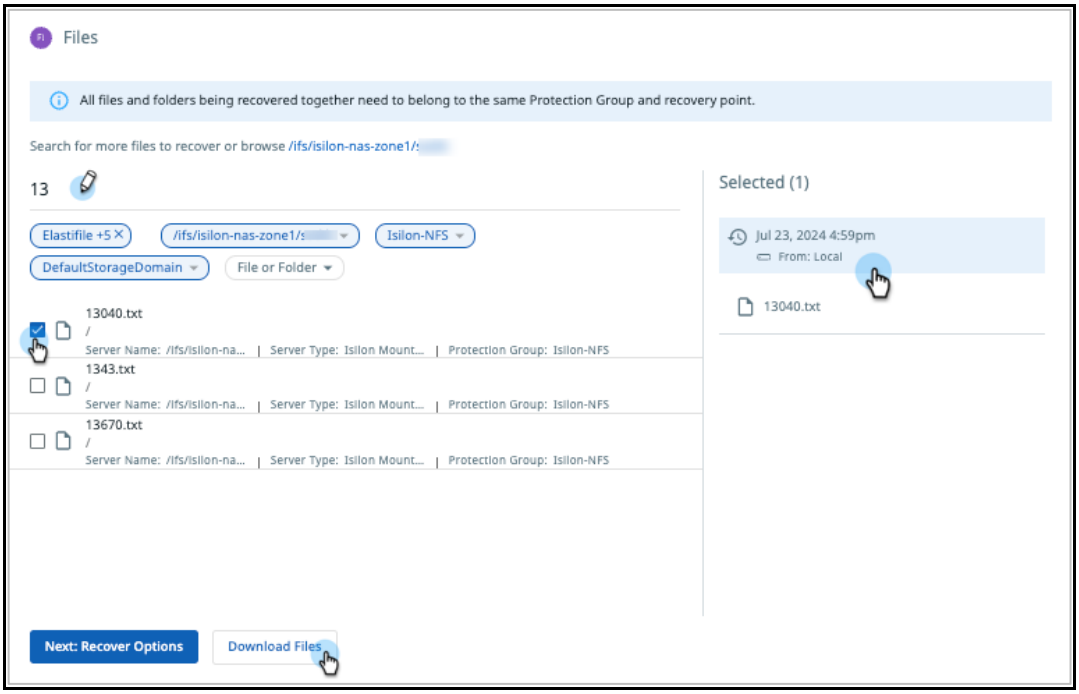
   a. Next: Recover Options. On the Files page, select Original Location or enter a New Location and click **Recover**.



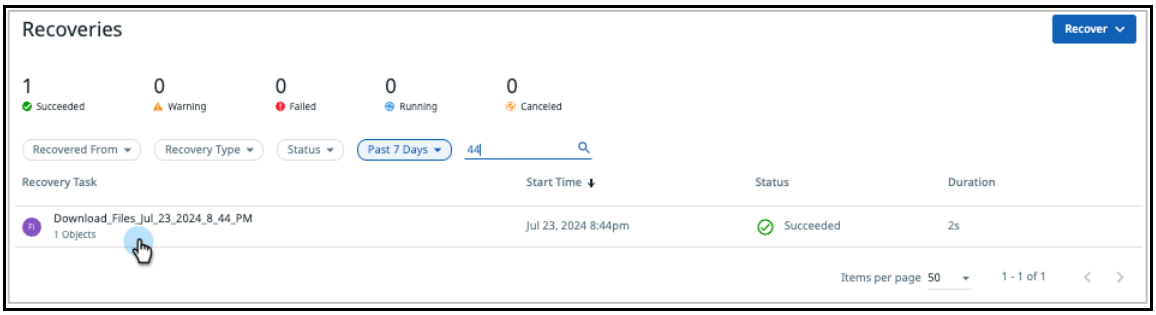
NOTE:

- 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.

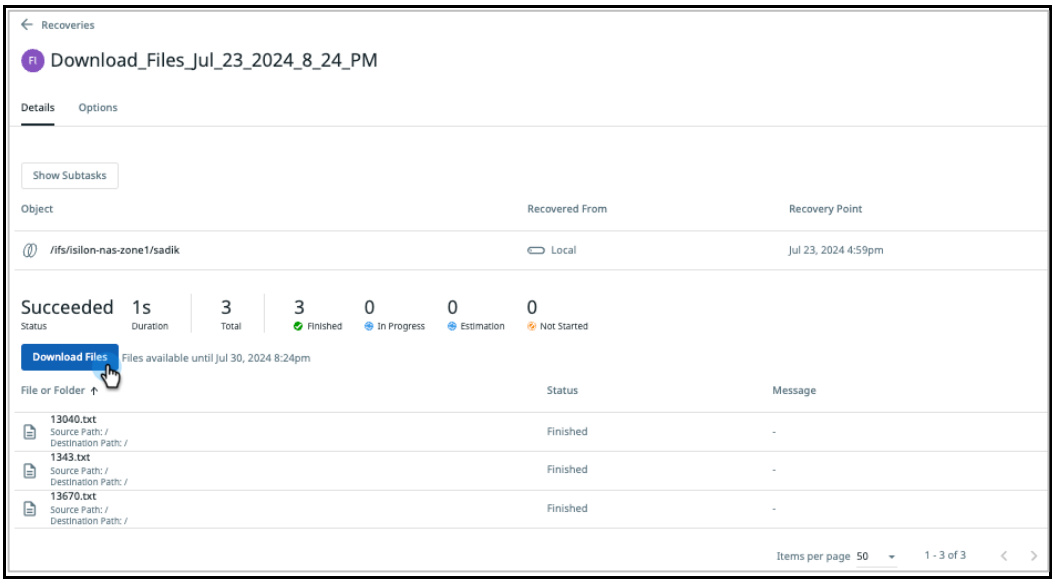
   b. **Download Files**. If you are recovering a single file, this option downloads the file to your browser's download folder.



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.



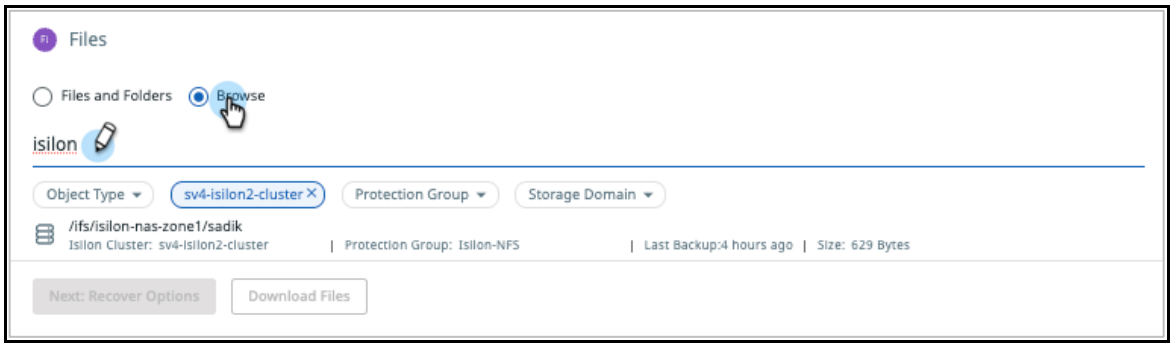
For details on Cohesity DataProtect's actions in each file recovery use case, see Appendix A: Restore Write Behavior for more details.

Browse

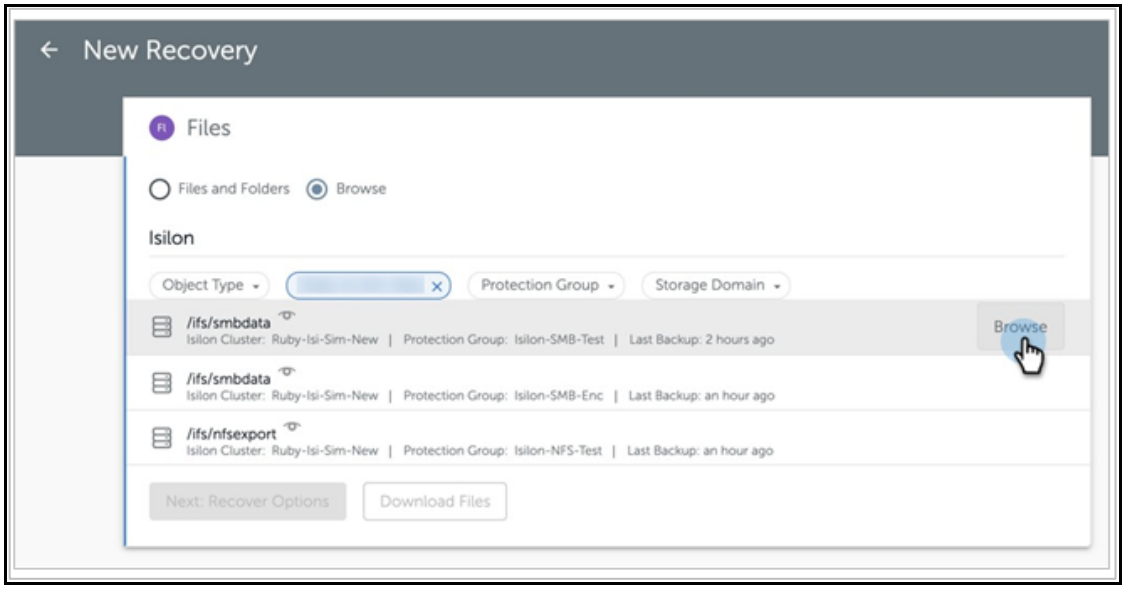
The **Browse** option allows you to search and recover files using the name of the server or Protection Group from any backup available on Cohesity.

To browse by server or Protection Group name:

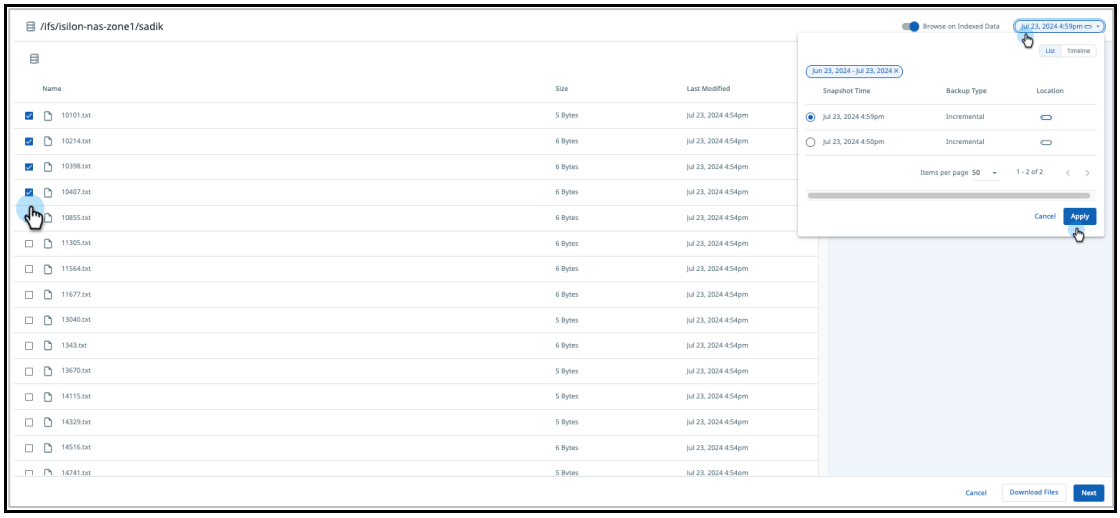
1. In the **Files** form, select **Browse** and enter the full or partial name of the server or Protection Group. Use the **Object Type**, **Source**, **Protection Group**, and/or **Storage Domain** filters to further narrow your results as needed.



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**.

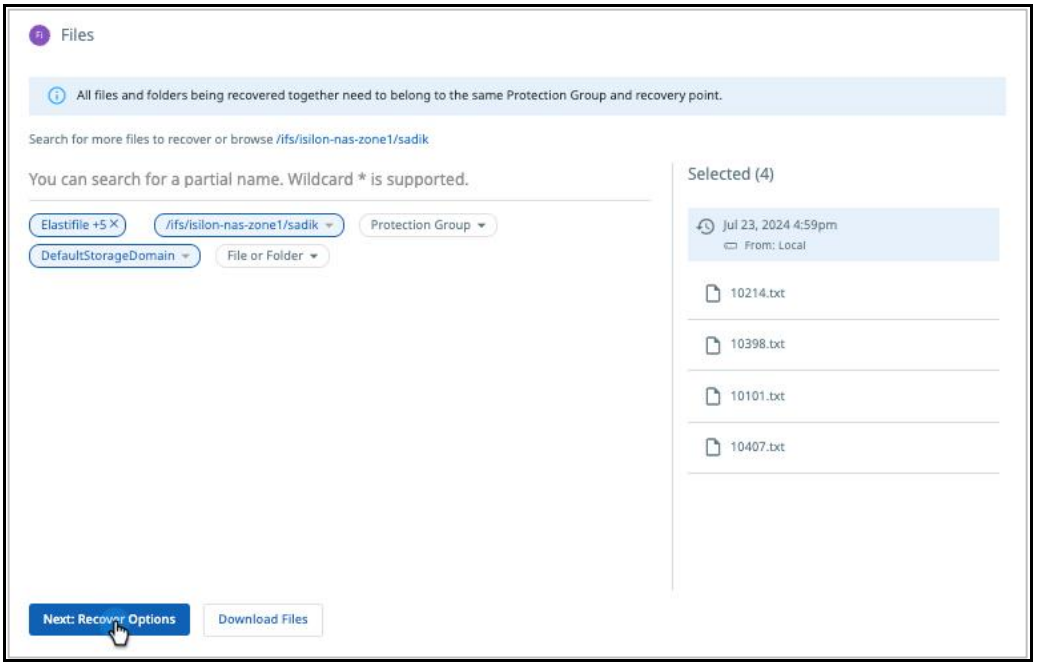


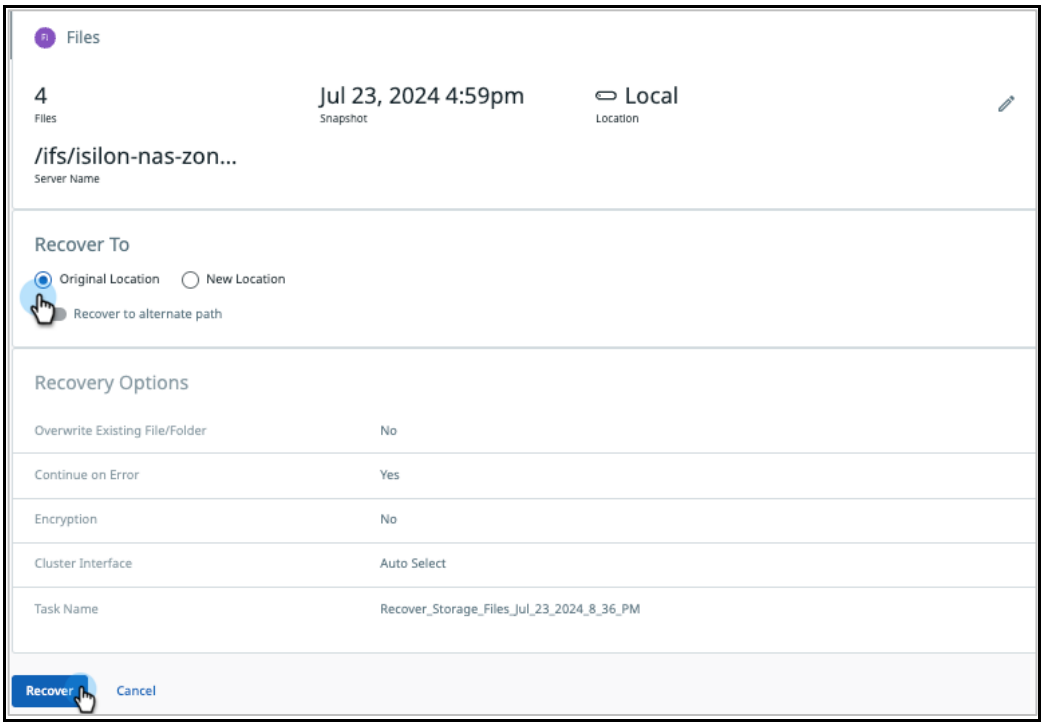
NOTE:

- 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. 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**.

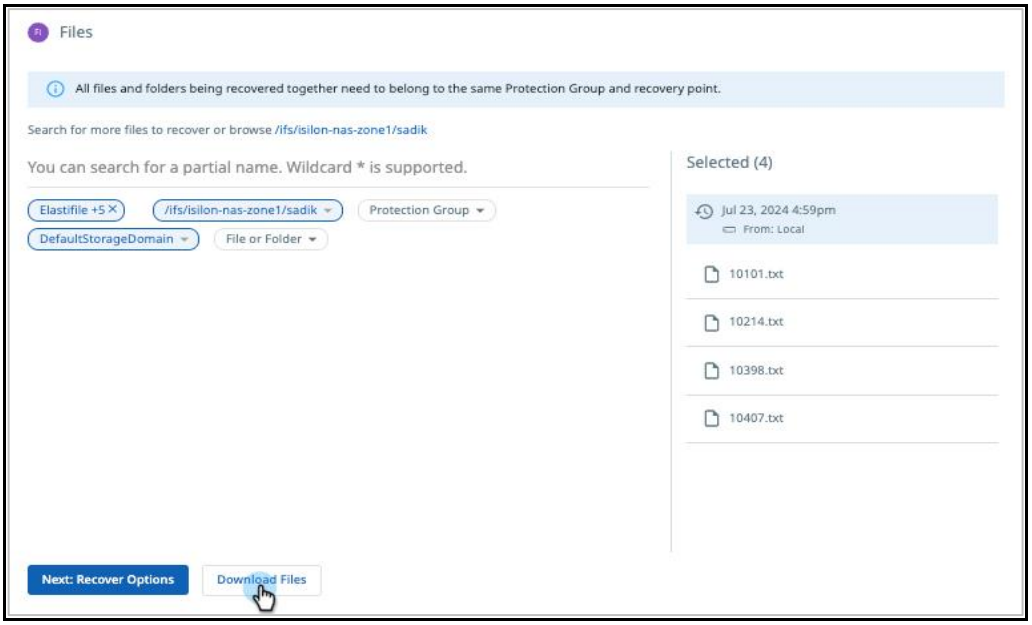




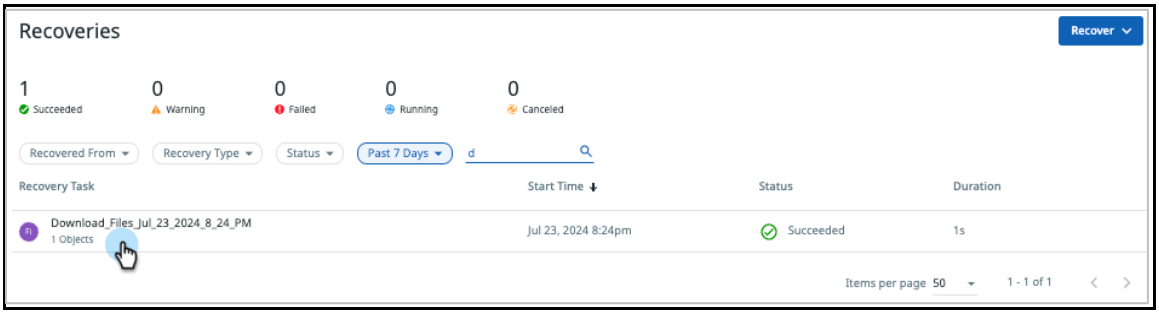
NOTE:

- To recover files or folders to an alternate path in the original NAS source, enable **Recover to 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.

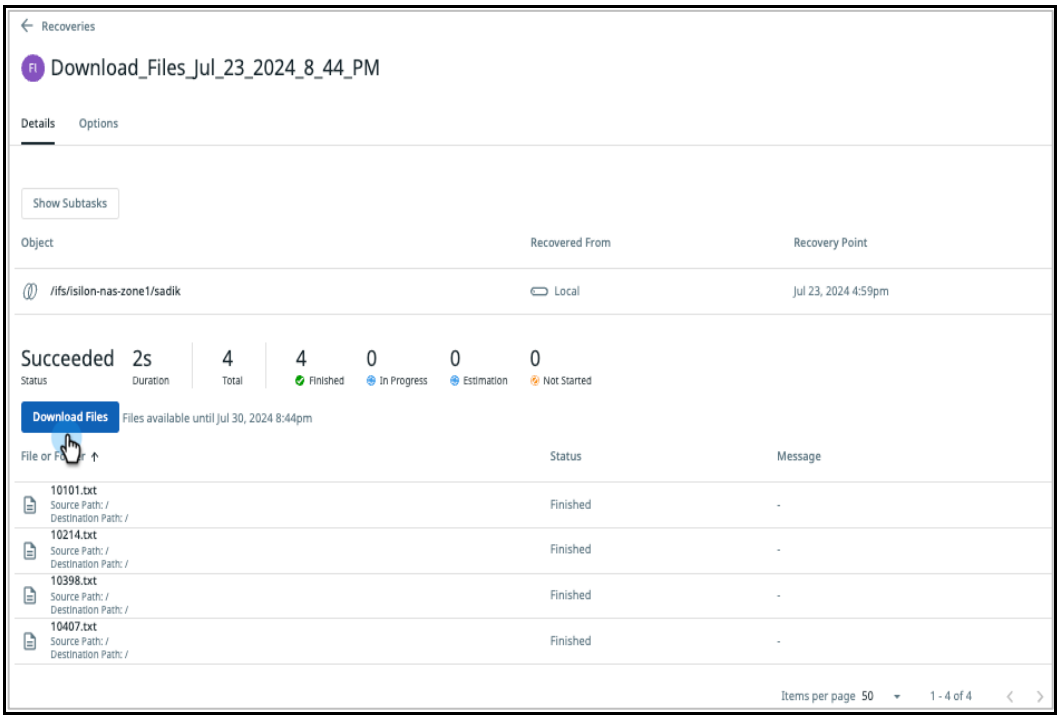
b. **Download Files**. If you are recovering a single file, this option downloads the file to your browser's download folder.



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.

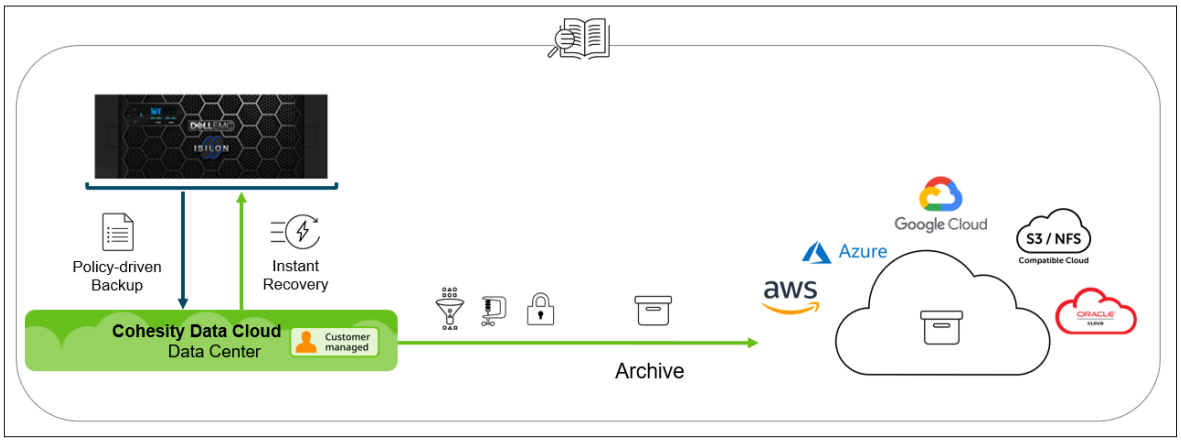
Use CloudArchive for Long-term Retention

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



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

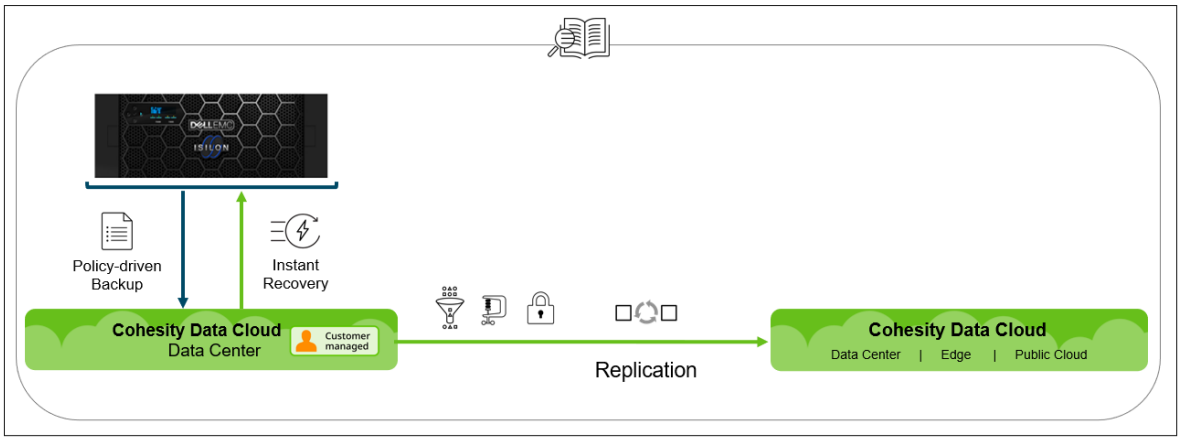
- **Replication** provides a simple way to store and retrieve data in the event of major business disruptions, such as natural disasters and IT failures.
- **CloudRetrieve** works with CloudArchive to restore your data to an alternate Cohesity cluster.

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 14: Replicate Backups to Other Cohesity Clusters



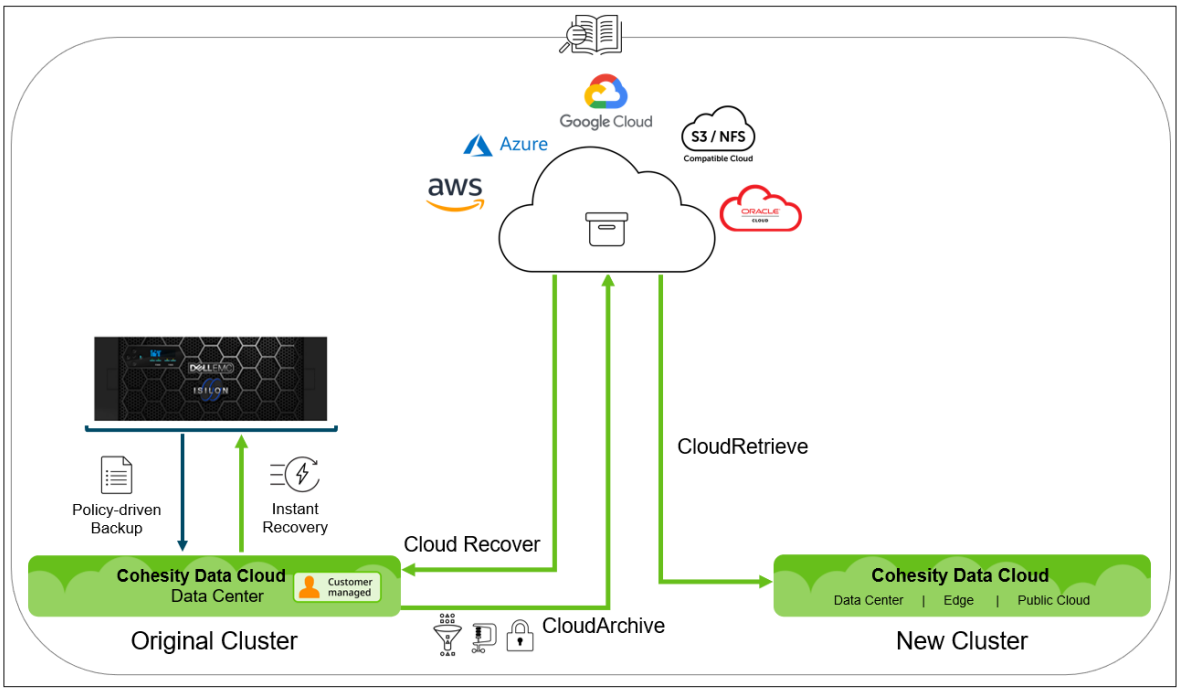
For more, see About Replication in the online Help.

Access Your Cloud-stored Data

Once the data is archived, Isilon 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 15: 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 Isilon NAS

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

1. To leverage the Isilon Changelist for faster incremental backups if the Protection Group has fewer objects selected. Enable Use Isilon Changelist option in the Protection Group.
2. When a Protection Group contains many objects, using this built-in CFT can be faster than vendor-native CFT, which is limited to only one Changelist call at a time. With built-in CFT, Cohesity runs all the above processes in parallel with all objects in the Protection Group and Protection Groups.
3. To be able to recover at granular levels later, enable Indexing when you create a NAS Protection Group.
4. 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.
5. Avoid adding the same shares to multiple Protection Groups.
6. Filter IP to include or exclude the IP addresses for the cluster to make sure backup / recovery does not fail with connectivity issues.

Appendix A: Restore Write Behavior

During recovery from your Isilon 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 Isilon 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 Isilon NAS Files or Folders restore operations, the recovery task:

1. If Recover to Original Location is disabled, creates the “/tmp/Recover-Files_<TimeStamp>” directory structure on the target and performs the recovery under that directory.
2. Writes recovered files in the format:
   `__ch_<InternalViewID>_<SubTaskID>_<FileName>`

   NOTE: Folders are written the same as source names.
3. 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 Isilon backups, the restore operations behave differently depending on the restore location, target volume, and the “Overwrite Existing File/Folder” option.

Table 5: 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, which enables you to search results even when you are searching 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.

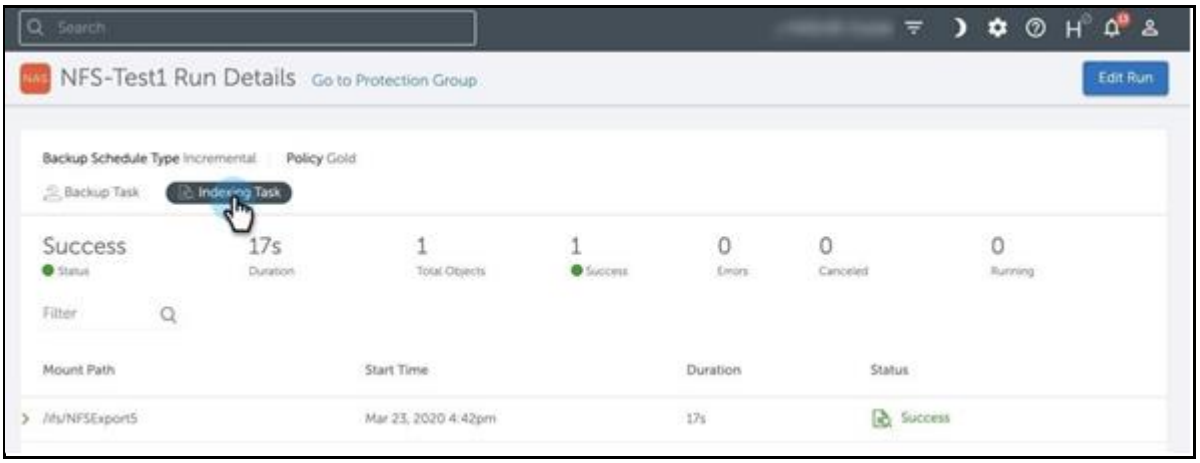
Once indexing is enabled in the Protection Group, everything in the protected SMB/NFS share is indexed by default. However, because indexing is resource-intensive, we recommend that you exclude the files and directories where file-level recovery is not required, such as scratch spaces, binaries, temp 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 completes successfully, the Protection Group starts indexing the backup metadata. You can track the progress of the **Indexing Task** in the Protection Run Details.

Figure 16: Click a Completed Protection Run for Indexing Task 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: “BackupAdmin” Role and Access Zones

The Isilon user account used on Cohesity to back up SMB data needs at least read access on the SMB share to be able to back up the Isilon data.

Provide Access to System Zone SMB Shares

To provide access to the Isilon SMB shares (/ifs or other shares) on the System Zone, assign the Isilon user to the built-in **BackupAdmin** role within Isilon. This will grant access to the default /ifs share (or other shares on the System Zone) to back up and restore Isilon data.

Provide Access to Non-System Zone SMB Shares

By default, the **BackupAdmin** role does not exist in the Non-System Zone. To provide access to the Isilon SMB shares on Non-System Zones, create the **BackupAdmin** role and assign the **ISI_PRIV_IFS_BACKUP** and **ISI_PRIV_IFS_RESTORE** privileges to the role. Once the role is created, assign the Isilon user to the newly created **BackupAdmin** role within Isilon.

Commands to create the **BackupAdmin** role on Isilon for a non-system zone:

```
#isi auth roles create BackupAdmin --zone=<zonename>
#isi auth roles modify BackupAdmin --zone=<zonename>
--add-priv=ISI_PRIV_IFS_BACKUP --add-user=<domain\username>
#isi auth roles modify BackupAdmin --zone=<zonename>
--add-priv=ISI_PRIV_IFS_RESTORE --add-user=<domain\username>
```

Example

```
isi auth roles create DebBackupAdmin --zone=SpartansZone
isi auth roles modify DebBackupAdmin --zone=SpartansZone --add-
priv=ISI_PRIV_IFS_BACKUP --add-user=debjeet
isi auth roles modify DebBackupAdmin --zone=SpartansZone --add-
priv=ISI_PRIV_IFS_RESTORE
```

NOTE: If the user is a local user, domain name is not required. ISI_PRIV_IFS_RESTORE privilege is created in read only mode in the non-system Access zone.

Provide Access at the SMB Share Level

If providing access at the zone level is not desirable, then you can grant access at the SMB share level.

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:

- Adaikkappan Arumugam, Product Solutions
- Amandeep Gautam, Cohesity Engineering
- Rich Kuhn, Product Solutions

Document Version History

VERSION	DATE	DOCUMENT HISTORY
3.6	May 2025	Added SmartConnect section
3.5	April 2025	Updated the “Prerequisites” section.
3.4	Nov 2024	Revamped Entire Document
3.3	May 2024	Minor Updates
3.2	June 2023	Rebranding updates
3.1	Mar 2022	Minor update
3.0	Dec 2020	Feature update
2.0	Apr 2020	Major update
1.0	Dec 2019	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 42 of the Fortune 100.

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