Restore from ONTAP backups

NetApp Backup and Recovery

NetApp
February 11, 2026

Table of Contents

Restore from ONTAP backups . . . 1

Restore ONTAP data from backup files with NetApp Backup and Recovery . . . 1

The Restore Dashboard . . . 1

Comparing Browse & Restore and Search & Restore . . . 2

Restore from ONTAP backups using Search & Restore . . . 2

Search & Restore supported systems and object storage providers . . . 3

Search & Restore prerequisites . . . 4

Search & Restore process . . . 6

Enable the Indexed Catalog for each system . . . 6

Restore volumes, folders, and files using Search & Restore . . . 8

Restore ONTAP data using Browse & Restore . . . 9

Browse & Restore supported systems and object storage providers . . . 10

Restore volumes using Browse & Restore . . . 11

Restore folders and files using Browse & Restore . . . 13

Restore from ONTAP backups

Restore ONTAP data from backup files with NetApp Backup and Recovery

Backups of your ONTAP volume data are stored as snapshots, on replicated volumes, or in object storage. You can restore data from any of these locations at a specific point in time. With NetApp Backup and Recovery, you can restore an entire volume, a folder, or individual files as needed.

To switch to and from NetApp Backup and Recovery workloads, refer to Switch to different NetApp Backup and Recovery workloads.

- You can restore a **volume** (as a new volume) to the original system, to a different system that's using the same cloud account, or to an on-premises ONTAP system.
- You can restore a **folder** to a volume in the original system, to a volume in a different system that's using the same cloud account, or to a volume on an on-premises ONTAP system.
- You can restore **files** to a volume in the original system, to a volume in a different system that's using the same cloud account, or to a volume on an on-premises ONTAP system.

You need a valid NetApp Backup and Recovery license to restore data to a production system.

To summarize, these are the valid flows you can use to restore volume data to an ONTAP system:

- Backup file → restored volume
- Replicated volume → restored volume
- Snapshot → restored volume

If the restore operation does not complete, wait until the Job Monitor shows "Failed" before you retry the restore operation.

For limitations related to restoring ONTAP data, see Backup and restore limitations for ONTAP volumes.

The Restore Dashboard

You use the Restore Dashboard to perform volume, folder, and file restore operations. To access the Restore Dashboard, select **Backup and recovery** from the Console menu, and then select the **Restore** tab. You can also select ⋮ > **View Restore Dashboard** from the Backup and recovery service from the Services panel.

NetApp Backup and Recovery must already be activated for at least one system and initial backup files must exist.

The Restore Dashboard provides two different ways to restore data from backup files: **Browse & Restore** and **Search & Restore**.

Comparing Browse & Restore and Search & Restore

In broad terms, *Browse & Restore* is typically better when you need to restore a specific volume, folder, or file from the last week or month — and you know the name and location of the file, and the date when it was last in good shape. *Search & Restore* is typically better when you need to restore a volume, folder, or file, but you don’t remember the exact name, or the volume in which it resides, or the date when it was last in good shape.

This table provides a feature comparison of the two methods.

Browse & Restore	Search & Restore
Browse through a folder-style structure to find the volume, folder, or file within a single backup file.	Search for a volume, folder, or file across **all backup files** by partial or full volume name, partial or full folder/file name, size range, and additional search filters.
Does not handle file recovery if the file has been deleted or renamed, and the user doesn’t know the original file name	Handles newly created/deleted/renamed directories and newly created/deleted/renamed files
Quick restore is supported.	Quick restore is not supported.

This table provides a list of valid restore operations based on the location where your backup files reside.

Backup Type	Browse & Restore			Search & Restore		
	Restore volume	**Restore files**	**Restore folder**	**Restore volume**	**Restore files**	**Restore folder**
Snapshot	Yes	No	No	Yes	Yes	Yes
Replicated volume	Yes	No	No	Yes	Yes	Yes
Backup file	Yes	Yes	Yes	Yes	Yes	Yes

Before you use either restore method, configure your environment to meet the resource requirements. See the following sections for details.

See the requirements and restore steps for the type of restore operation you want to use:

- Restore volumes using Browse & Restore
- Restore folders and files using Browse & Restore
- Restore volumes, folders, and files using Search & Restore

Restore from ONTAP backups using Search & Restore

You can use Search & Restore to recover volumes, folders, or files from ONTAP backup files. Search & Restore enables you to search across all backups (including local snapshots, replicated volumes, and object storage) without needing exact system, volume, or file names.

Restoring from local snapshots or replicated volumes is typically faster and less expensive than restoring from object storage.

When restoring a full volume, NetApp Backup and Recovery creates a new volume using the backup data. You can restore to the original system, another system within the same cloud account, or an on-premises ONTAP system. Folders and files can be restored to their original location, a different volume in the same system, another system in the same cloud account, or an on-premises system.

Restore capabilities depend on your ONTAP version:

- **Folders:** Using ONTAP 9.13.0 or greater, you can restore folders with all files and sub-folders; with earlier versions, you can restore only files in the folder.
- **Archival Storage:** Restoring from archival storage (available with ONTAP 9.10.1 or greater) is slower and might incur additional costs.
- **Destination Cluster Requirements:**
  - Volume restore: ONTAP 9.10.1 or greater
  - File restore: ONTAP 9.11.1 or greater
  - Google Archive and StorageGRID: ONTAP 9.12.1 or greater
  - Folder restore: ONTAP 9.13.1 or greater

Learn more about restoring from AWS archival storage.
Learn more about restoring from Azure archival storage.
Learn more about restoring from Google archival storage.

- If the backup file in object storage has been configured with DataLock & Ransomware protection, then folder-level restore is supported only if the ONTAP version is 9.13.1 or greater. If you are using an earlier version of ONTAP, you can restore the entire volume from the backup file and then access the folder and files you need.
- If the backup file in object storage resides in archival storage, then folder-level restore is supported only if the ONTAP version is 9.13.1 or greater. If you are using an earlier version of ONTAP, you can restore the folder from a newer backup file that has not been archived, or you can restore the entire volume from the archived backup and then access the folder and files you need.
- The "High" restore priority is not supported when restoring data from Azure archival storage to StorageGRID systems.
- Restoring folders is not currently supported from volumes in ONTAP S3 object storage.

Before you start, you should have some idea of the name or location of the volume or file you want to restore.

Search & Restore supported systems and object storage providers

You can restore ONTAP data from a backup file that resides in a secondary system (a replicated volume) or in object storage (a backup file) to the following systems. Snapshots reside on the source system and can be restored only to that same system.

Note: You can restore volumes and files from any type of backup file, but you can restore a folder only from backup files in object storage at this time.

Backup File Location		Destination system
Object Store (Backup)	**Secondary System (Replication)**	

Backup File Location		Destination system
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	Cloud Volumes ONTAP in Google On-premises ONTAP system
NetApp StorageGRID	On-premises ONTAP system Cloud Volumes ONTAP	On-premises ONTAP system
ONTAP S3	On-premises ONTAP system Cloud Volumes ONTAP	On-premises ONTAP system

For Search & Restore, the Console agent can be installed in the following locations:

- For Amazon S3, the Console agent can be deployed in AWS or in your premises
- For Azure Blob, the Console agent can be deployed in Azure or in your premises
- For Google Cloud Storage, the Console agent must be deployed in your Google Cloud Platform VPC
- For StorageGRID, the Console agent must be deployed in your premises; with or without internet access
- For ONTAP S3, the Console agent can be deployed in your premises (with or without internet access) or in a cloud provider environment

Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

Search & Restore prerequisites

Ensure your environment meets these requirements before enabling Search & Restore:

- Cluster requirements:
  - The ONTAP version must be 9.8 or greater.
  - The storage VM (SVM) on which the volume resides must have a configured data LIF.
  - NFS must be enabled on the volume (both NFS and SMB/CIFS volumes are supported).
  - The SnapDiff RPC Server must be activated on the SVM. The Console does this automatically when you enable Indexing on the system. (SnapDiff is the technology that quickly identifies the file and directory differences between snapshots.)
- NetApp recommends mounting a separate volume on the Console agent to increase resiliency of Search & Restore. For instructions, refer to mount the volume to reindex the catalog.

Legacy Search & Restore prerequisites (using Indexed Catalog v1)

The following are the requirements for Search & Restore when using legacy indexing:

- AWS requirements:
  - Specific Amazon Athena, AWS Glue, and AWS S3 permissions must be added to the user role that provides the Console with permissions. Make sure all the permissions are configured correctly.

    Note that if you were already using NetApp Backup and Recovery with a Console agent you configured in the past, you'll need to add the Athena and Glue permissions to the Console user role now. They are required for Search & Restore.

- Azure requirements:
  - You must register the Azure Synapse Analytics Resource Provider (called "Microsoft.Synapse") with your Subscription. See how to register this resource provider for your subscription. You must be the Subscription **Owner** or **Contributor** to register the resource provider.
  - Specific Azure Synapse Workspace and Data Lake Storage Account permissions must be added to the user role that provides the Console with permissions. Make sure all the permissions are configured correctly.

    Note that if you were already using NetApp Backup and Recovery with a Console agent you configured in the past, you'll need to add the Azure Synapse Workspace and Data Lake Storage Account permissions to the Console user role now. They are required for Search & Restore.
  - The Console agent must be configured **without** a proxy server for HTTP communication to the internet. If you have configured an HTTP proxy server for your Console agent, you can't use Search & Restore functionality.
- Google Cloud requirements:
  - Specific Google BigQuery permissions must be added to the user role that provides the NetApp Console with permissions. Make sure all the permissions are configured correctly.

    If you were already using NetApp Backup and Recovery with a Console agent you configured in the past, you'll need to add the BigQuery permissions to the Console user role now. They are required for Search & Restore.
- StorageGRID and ONTAP S3 requirements:

  Depending on your configuration, there are 2 ways that Search & Restore is implemented:

  - If there are no cloud provider credentials in your account, then the Indexed Catalog information is stored on the Console agent.

    For information about the Indexed Catalog v2, see the section below about how to enable the Indexed Catalog.
  - If you are using a Console agent in a private (dark) site, then the Indexed Catalog information is stored on the Console agent (requires Console agent version 3.9.25 or greater).
  - If you have AWS credentials or Azure credentials in the account, then the Indexed Catalog is stored at the cloud provider, just like with a Console agent deployed in the cloud. (If you have both credentials, AWS is selected by default.)

    Even though you are using an on-premises Console agent, the cloud provider requirements must be met for both Console agent permissions and cloud provider resources. See the AWS and

Azure requirements above when using this implementation.

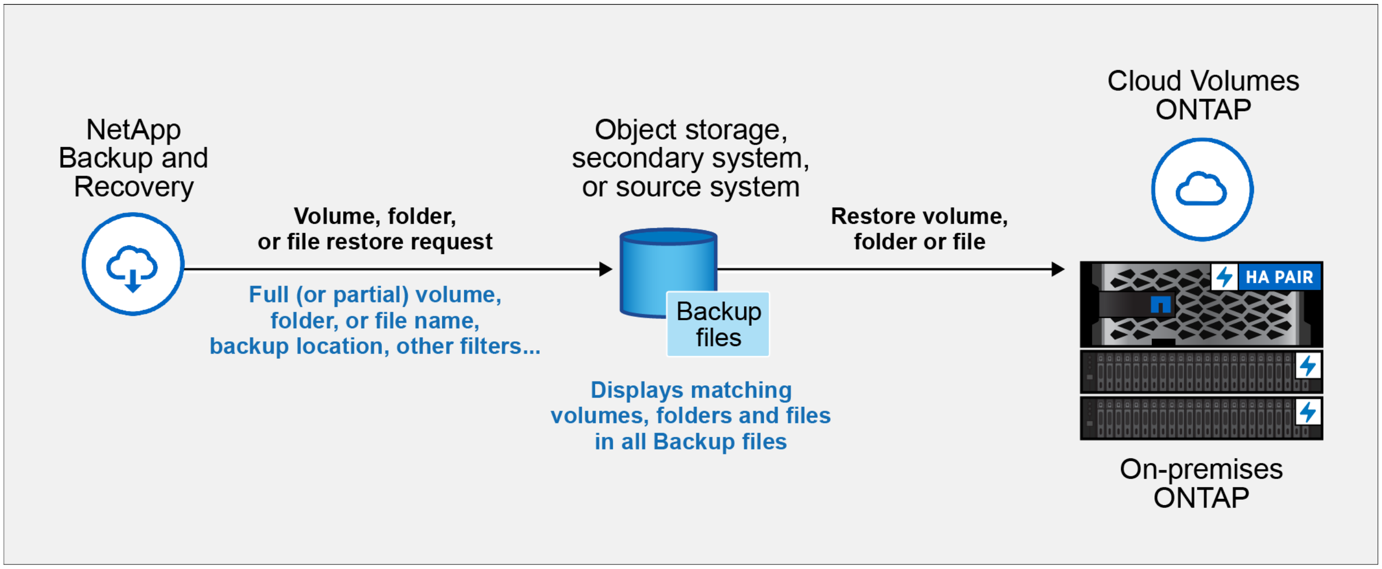
Search & Restore process

The process goes like this:

1. Before you can use Search & Restore, you need to enable "Indexing" on each source system from which you'll want to restore volume data. This allows the Indexed Catalog to track the backup files for every volume.
2. When you want to restore a volume or files from a volume backup, under *Search & Restore*, select **Search & Restore**.
3. Enter the search criteria for a volume, folder, or file by partial or full volume name, partial or full file name, backup location, size range, creation date range, other search filters, and select **Search**.

   The Search Results page displays all the locations that have a file or volume that matches your search criteria.

4. Select **View All Backups** for the location you want to use to restore the volume or file, and then select **Restore** on the actual backup file you want to use.
5. Select the location where you want the volume, folder, or file(s) to be restored and select **Restore**.
6. The volume, folder, or file(s) are restored.


NetApp Backup and Recovery
Volume, folder, or file restore request
Full (or partial) volume, folder, or file name, backup location, other filters...
Object storage, secondary system, or source system
Backup files
Displays matching volumes, folders and files in all Backup files
Restore volume, folder or file
Cloud Volumes ONTAP
HA PAIR
On-premises ONTAP

You only need to know a partial name and NetApp Backup and Recovery searches through all backup files that match your search.

Enable the Indexed Catalog for each system

Before you can use Search & Restore, you need to enable "Indexing" on each source system from which you're planning to restore volumes or files. This allows the Indexed Catalog to track every volume and every backup file - making your searches very quick and efficient.

The Indexed Catalog is a database that stores metadata about all the volumes and backup files in your system. It is used by the Search & Restore functionality to quickly find the backup files that contain the data you want to restore.

Indexed Catalog features

NetApp Backup and Recovery does not provision a separate bucket when you use the Indexed Catalog. Instead, for backups stored in AWS, Azure, Google Cloud Platform, StorageGRID, or ONTAP S3, the service provisions space on the Console agent or on the cloud provider environment.

The Indexed Catalog supports the following:

- Global search efficiency in less than 3 minutes
- Up to 5 billion files
- Up to 5000 volumes per cluster
- Up to 100K snapshots per volume
- Maximum time for baseline indexing is less than 7 days. The actual time will vary depending on your environment.

Steps to enable Indexing for a system:

If Indexing has already been enabled for your system, go to the next section to restore your data.

You will first need to mount a separate volume to hold catalog files. This prevents data loss if the size of the files that hold the snapshots becomes too large. This is not required on every cluster; you can mount any one volume from any of the clusters in your environment. If you don’t do this, indexing might not function correctly.

For the mounted volume, use the following sizing guidance:

- Use a NetApp NFS volume
- Recommended AFF storage with 300 MB/s disk throughput. Less throughput will impact search and other operations.
- Enable NetApp snapshots to secure the catalog metadata in addition to the catalog backup zip files
- 50 GB per 1 billion files
- 20 GB for the catalog data with additional space for zip file creation and temporary files

Step to mount the volume to reindex the catalog

1. Mount the volume to `/opt/application/netapp/cbs` by entering the following command, where:
   - `volume name` is the volume on the cluster where the catalog files will be stored
   - `/opt/application/netapp/cbs` is the path where it is being mounted

   ```
   mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
   ```

   Example:

   ```
   mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
   ```

Steps to enable the index

1. Do one of the following:
   - If no systems have been indexed, on the Restore Dashboard under *Search & Restore*, select **Enable**

Indexing for systems.

    - If at least one system has already been indexed, on the Restore Dashboard under *Search & Restore*, select **Indexing Settings**.

2. Select **Enable Indexing** for the system.

Result

After all the services are provisioned and the Indexed Catalog has been activated, the system is shown as "Active".

Depending on the size of the volumes in the system, and the number of backup files in all 3 backup locations, the initial indexing process could take up to an hour. After that it is transparently updated hourly with incremental changes to stay current.

Restore volumes, folders, and files using Search & Restore

After you have enabled Indexing for your system, you can restore volumes, folders, and files using Search & Restore. This allows you to use a broad range of filters to find the exact file or volume that you want to restore from all backup files.

Steps

1. From the Console menu, select **Protection > Backup and recovery**.
2. Select the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Search & Restore* section, select **Search & Restore**.
4. From the *Search & Restore* section, select **Search & Restore**.
5. From the Search & Restore page:
    a. In the *Search bar*, enter a full or partial volume name, folder name, or file name.
    b. Select the type of resource: **Volumes**, **Files**, **Folders**, or **All**.
    c. In the *Filter by* area, select the filter criteria. For example, you can select the system where the data resides and the file type, for example a .JPEG file. Or you can select the type of Backup Location if you want to search for results only within available snapshots or backup files in object storage.
6. Select **Search** and the Search Results area displays all the resources that have a file, folder, or volume that matches your search.
7. Locate the resource that has the data you want to restore and select **View All Backups** to display all the backup files that contain the matching volume, folder, or file.
8. Locate the backup file that you want to use to restore the data and select **Restore**.

    Note that the results identify local volume snapshots and remote Replicated volumes that contain the file in your search. You can choose to restore from the cloud backup file, from the snapshot, or from the Replicated volume.

9. Select the destination location where you want the volume, folder, or file(s) to be restored and select **Restore**.
    - For volumes, you can select the original destination system or you can select an alternate system. When restoring a FlexGroup volume you'll need to choose multiple aggregates.
    - For folders, you can restore to the original location or you can select an alternate location; including the system, volume, and folder.
    - For files, you can restore to the original location or you can select an alternate location; including the

system, volume, and folder. When selecting the original location, you can choose to overwrite the source file(s) or to create new file(s).

If you select an on-premises ONTAP system and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:

- When restoring from Amazon S3, select the IPspace in the ONTAP cluster where the destination volume will reside, enter the access key and secret key for the user you created to give the ONTAP cluster access to the S3 bucket, and optionally choose a private VPC endpoint for secure data transfer. See details about these requirements.
- When restoring from Azure Blob, select the IPspace in the ONTAP cluster where the destination volume will reside, and optionally choose a private endpoint for secure data transfer by selecting the VNet and Subnet. See details about these requirements.
- When restoring from Google Cloud Storage, select the IPspace in the ONTAP cluster where the destination volume will reside, and the Access Key and Secret Key to access the object storage. See details about these requirements.
- When restoring from StorageGRID, enter the FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with StorageGRID, enter the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume resides. See details about these requirements.
- When restoring from ONTAP S3, enter the FQDN of the ONTAP S3 server and the port that ONTAP should use for HTTPS communication with ONTAP S3, select the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume will reside. See details about these requirements.

Results

The volume, folder, or file(s) are restored and you are returned to the Restore Dashboard so you can review the progress of the restore operation. You can also select the **Job Monitoring** tab to see the restore progress. See Job monitor page.

Restore ONTAP data using Browse & Restore

With NetApp Backup and Recovery, restore ONTAP data using Browse & Restore. Before restoring, note the source volume name, source system and SVM, and backup file date. You can restore ONTAP data from a snapshot, a replicated volume, or from backups stored in object storage.

Restore capabilities depend on your ONTAP version:

- **Folders:** Using ONTAP 9.13.0 or greater, you can restore folders with all files and sub-folders; with earlier versions, you can restore only files in the folder.
- **Archival Storage:** Restoring from archival storage (available with ONTAP 9.10.1 or greater) is slower and might incur additional costs.
- **Destination Cluster Requirements:**
  - Volume restore: ONTAP 9.10.1 or greater
  - File restore: ONTAP 9.11.1 or greater
  - Google Archive and StorageGRID: ONTAP 9.12.1 or greater
  - Folder restore: ONTAP 9.13.1 or greater

Learn more about restoring from AWS archival storage.
Learn more about restoring from Azure archival storage.
Learn more about restoring from Google archival storage.

> The High priority isn’t supported when restoring data from Azure archival storage to StorageGRID systems.

Browse & Restore supported systems and object storage providers

You can restore ONTAP data from a backup file that resides in a secondary system (a replicated volume) or in object storage (a backup file) to the following systems. Snapshots reside on the source system and can be restored only to that same system.

Note: You can restore a volume from any type of backup file, but you can restore a folder or individual files only from a backup file in object storage at this time.

From Object Store (Backup)	From Primary (Snapshot)	From Secondary System (Replication)	To Destination system
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Azure Blob
Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system
Cloud Volumes ONTAP in Google On-premises ONTAP system	NetApp StorageGRID	On-premises ONTAP system	On-premises ONTAP system Cloud Volumes ONTAP
To on-premises ONTAP system	ONTAP S3	On-premises ONTAP system	On-premises ONTAP system Cloud Volumes ONTAP

For Browse & Restore, the Console agent can be installed in the following locations:

- For Amazon S3, the Console agent can be deployed in AWS or in your premises
- For Azure Blob, the Console agent can be deployed in Azure or in your premises
- For Google Cloud Storage, the Console agent must be deployed in your Google Cloud Platform VPC
- For StorageGRID, the Console agent must be deployed in your premises; with or without internet access
- For ONTAP S3, the Console agent can be deployed in your premises (with or without internet access) or in a cloud provider environment

Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

> If the ONTAP version on your system is less than 9.13.1, then you can’t restore folders or files if the backup file has been configured with DataLock & Ransomware. In this case, you can restore the entire volume from the backup file and then access the files you need.

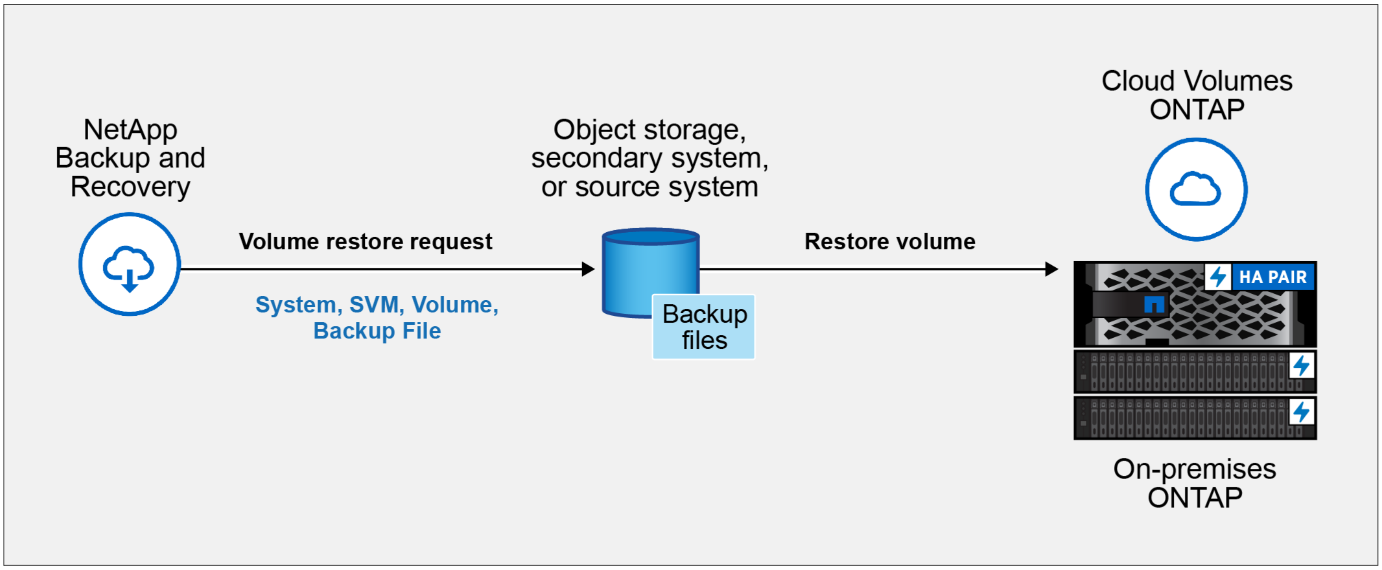
Restore volumes using Browse & Restore

When you restore a volume from a backup file, NetApp Backup and Recovery creates a *new* volume using the data from the backup. When using a backup from object storage, you can restore the data to a volume in the original system, to a different system that's located in the same cloud account as the source system, or to an on-premises ONTAP system.

When restoring a cloud backup to a Cloud Volumes ONTAP system using ONTAP 9.13.0 or greater or to an on-premises ONTAP system running ONTAP 9.14.1, you'll have the option to perform a *quick restore* operation. The quick restore is ideal for disaster recovery situations where you need to provide access to a volume as soon as possible. A quick restore restores the metadata from the backup file to a volume instead of restoring the entire backup file. Quick restore is not recommended for performance or latency-sensitive applications, and it is not supported with backups in archived storage.

> ⓘ Quick restore is supported for FlexGroup volumes only if the source system from which the cloud backup was created was running ONTAP 9.12.1 or greater. And it is supported for SnapLock volumes only if the source system was running ONTAP 9.11.0 or greater.

When restoring from a replicated volume, you can restore the volume to the original system or to a Cloud Volumes ONTAP or on-premises ONTAP system.


NetApp Backup and Recovery
Volume restore request
System, SVM, Volume, Backup File
Object storage, secondary system, or source system
Backup files
Restore volume
Cloud Volumes ONTAP
HA PAIR
On-premises ONTAP

You need the source system name, storage VM, volume name, and backup file date to restore a volume.

Steps

1. From the Console menu, select **Protection > Backup and recovery**.
2. Select the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, select **Restore Volume**.
4. In the *Select Source* page, navigate to the backup file for the volume you want to restore. Select the **system**, the **Volume**, and the **Backup** file that has the date/time stamp from which you want to restore.

   The **Location** column shows whether the backup file (Snapshot) is **Local** (a snapshot on the source system), **Secondary** (a replicated volume on a secondary ONTAP system), or **Object Storage** (a backup file in object storage). Choose the file that you want to restore.

5. Select **Next**.

Note that if you select a backup file in object storage, and Ransomware Resilience is active for that backup (if you enabled DataLock and Ransomware Resilience in the backup policy), then you are prompted to run an additional ransomware scan on the backup file before restoring the data. We recommend that you scan the backup file for ransomware. (You'll incur extra egress costs from your cloud provider to access the contents of the backup file.)

6. In the *Select Destination* page, select the **system** where you want to restore the volume.
7. When restoring a backup file from object storage, if you select an on-premises ONTAP system and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:
   - When restoring from Amazon S3, select the IPspace in the ONTAP cluster where the destination volume will reside, enter the access key and secret key for the user you created to give the ONTAP cluster access to the S3 bucket, and optionally choose a private VPC endpoint for secure data transfer.
   - When restoring from Azure Blob, select the IPspace in the ONTAP cluster where the destination volume will reside, select the Azure Subscription to access the object storage, and optionally choose a private endpoint for secure data transfer by selecting the VNet and Subnet.
   - When restoring from Google Cloud Storage, select the Google Cloud Project and the Access Key and Secret Key to access the object storage, the region where the backups are stored, and the IPspace in the ONTAP cluster where the destination volume will reside.
   - When restoring from StorageGRID, enter the FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with StorageGRID, select the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume will reside.
   - When restoring from ONTAP S3, enter the FQDN of the ONTAP S3 server and the port that ONTAP should use for HTTPS communication with ONTAP S3, select the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume will reside.
8. Enter the name you want to use for the restored volume, and select the Storage VM and Aggregate where the volume will reside. When restoring a FlexGroup volume you'll need to select multiple aggregates. By default, **<source_volume_name>_restore** is used as the volume name.

   When restoring a backup from object storage to a Cloud Volumes ONTAP system using ONTAP 9.13.0 or greater or to an on-premises ONTAP system running ONTAP 9.14.1, you'll have the option to perform a *quick restore* operation.

   And if you are restoring the volume from a backup file that resides in an archival storage tier (available starting with ONTAP 9.10.1), then you can select the Restore Priority.

   Learn more about restoring from AWS archival storage.
   Learn more about restoring from Azure archival storage.
   Learn more about restoring from Google archival storage. Backup files in the Google Archive storage tier are restored almost immediately, and require no Restore Priority.
9. Select **Next** to choose whether you want to do a Normal restore or a Quick Restore process:
   - **Normal restore**: Use normal restore on volumes that require high performance. Volumes will not be available until the restore process is complete.
   - **Quick restore**: Restored volumes and data will be available immediately. Do not use this on volumes that require high performance because during the quick restore process, access to the data might be slower than usual.
10. Select **Restore** and you return to the Restore Dashboard so you can review the progress of the restore

operation.

Result

NetApp Backup and Recovery creates a new volume based on the backup you selected.

Note that restoring a volume from a backup file that resides in archival storage can take many minutes or hours depending on the archive tier and the restore priority. You can select the **Job Monitoring** tab to see the restore progress.

Restore folders and files using Browse & Restore

If you need to restore only a few files from an ONTAP volume backup, you can choose to restore a folder or individual files instead of restoring the entire volume. You can restore folders and files to an existing volume in the original system, or to a different system that's using the same cloud account. You can also restore folders and files to a volume on an on-premises ONTAP system.

> ⓘ You can restore a folder or individual files only from a backup file in object storage at this time. Restoring files and folders is not currently supported from a local snapshot or from a backup file that resides in a secondary system (a replicated volume).

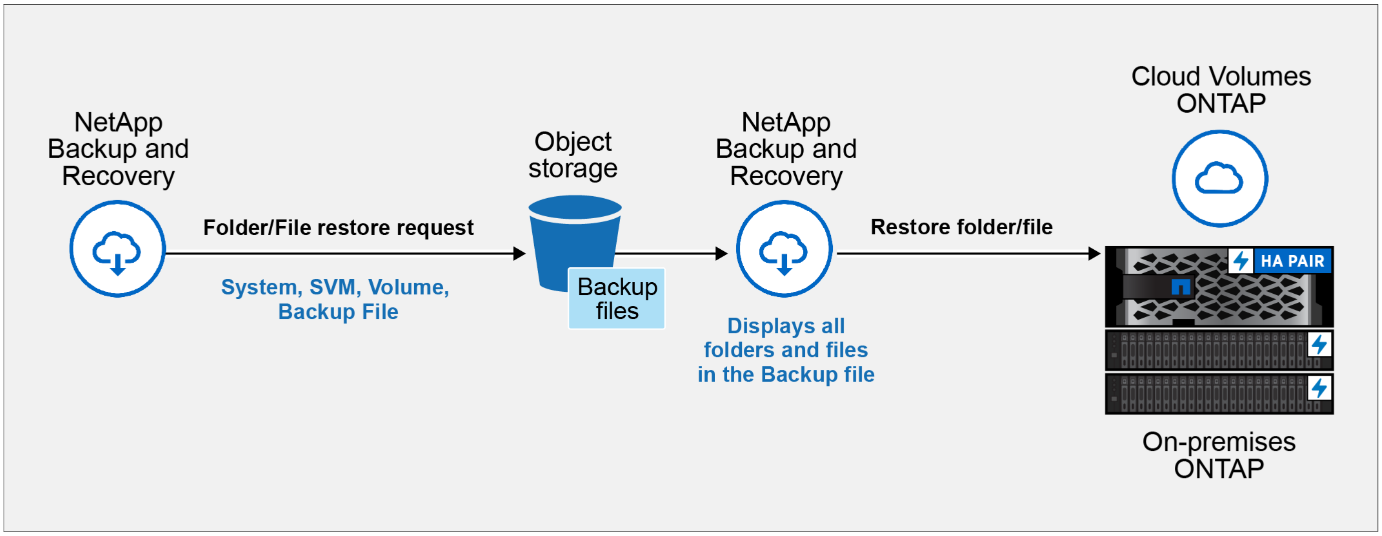
If you select multiple files, they are restored to the same destination volume. To restore files to different volumes, run the process multiple times.

When using ONTAP 9.13.0 or greater, you can restore a folder along with all files and sub-folders within it. When using a version of ONTAP before 9.13.0, only files from that folder are restored - no sub-folders, or files in sub-folders, are restored.

> ⓘ
>
> - If the backup file has been configured with DataLock & Ransomware protection, then folder-level restore is supported only if the ONTAP version is 9.13.1 or greater. If you are using an earlier version of ONTAP, you can restore the entire volume from the backup file and then access the folder and files you need.
> - If the backup file resides in archival storage, then folder-level restore is supported only if the ONTAP version is 9.13.1 or greater. If you are using an earlier version of ONTAP, you can restore the folder from a newer backup file that has not been archived, or you can restore the entire volume from the archived backup and then access the folder and files you need.
> - With ONTAP 9.15.1, you can restore FlexGroup folders using the "Browse and restore" option. This feature is in a Technology Preview mode.
>
>   You can test it using a special flag described in the NetApp Backup and Recovery July 2024 Release blog.

Restore folders and files

Follow these steps to restore folders or files to a volume from an ONTAP volume backup. You should know the name of the volume and the date of the backup file that you want to use to restore the folder or file(s). This functionality uses Live Browsing so that you can view the list of directories and files within each backup file.


NetApp Backup and Recovery
Folder/File restore request
System, SVM, Volume, Backup File
Object storage
Backup files
NetApp Backup and Recovery
Displays all folders and files in the Backup file
Restore folder/file
Cloud Volumes ONTAP
HA PAIR
On-premises ONTAP

Before you begin

- The ONTAP version must be 9.6 or greater to perform *file* restore operations.
- The ONTAP version must be 9.11.1 or greater to perform *folder* restore operations. ONTAP version 9.13.1 is required if the data is in archival storage, or if the backup file is using DataLock and Ransomware protection.
- The ONTAP version must be 9.15.1 p2 or greater to restore FlexGroup directories using the Browse and restore option.

Steps

1. From the Console menu, select **Protection > Backup and recovery**.
2. Select the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, select **Restore Files or Folder**.
4. In the *Select Source* page, navigate to the backup file for the volume that contains the folder or files you want to restore. Select the **system**, the **Volume**, and the **Backup** that has the date/time stamp from which you want to restore files.
5. Select **Next** and the list of folders and files from the volume backup are displayed.

   If you are restoring folders or files from a backup file that resides in an archival storage tier, then you can select the Restore Priority.

   Learn more about restoring from AWS archival storage.
   Learn more about restoring from Azure archival storage.
   Learn more about restoring from Google archival storage. Backup files in the Google Archive storage tier are restored almost immediately, and require no Restore Priority.

   And if Ransomware Resilience is active for the backup file (if you enabled DataLock and Ransomware Resilience in the backup policy), then you are prompted to run an additional ransomware scan on the backup file before restoring the data. We recommend that you scan the backup file for ransomware. (You'll incur extra egress costs from your cloud provider to access the contents of the backup file.)

6. In the *Select Items* page, select the folder or file(s) that you want to restore and select **Continue**. To assist you in finding the item:
   - You can select the folder or file name if you see it.
   - You can select the search icon and enter the name of the folder or file to navigate directly to the item.

- You can navigate down levels in folders using the Down arrow at the end of the row to find specific files.

  As you select files they are added to the left side of the page so you can see the files that you have already chosen. You can remove a file from this list if needed by selecting the **x** next to the file name.

7. In the *Select Destination* page, select the **system** where you want to restore the items.

   If you select an on-premises cluster and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:

   - When restoring from Amazon S3, enter the IPspace in the ONTAP cluster where the destination volume resides, and the AWS Access Key and Secret Key needed to access the object storage. You can also select a Private Link Configuration for the connection to the cluster.
   - When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volume resides. You can also select a Private Endpoint Configuration for the connection to the cluster.
   - When restoring from Google Cloud Storage, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the Access Key and Secret Key needed to access the object storage.
   - When restoring from StorageGRID, enter the FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with StorageGRID, enter the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume resides.

8. Then select the **Volume** and the **Folder** where you want to restore the folder or file(s).

   You have a few options for the location when restoring folders and file(s).

   - When you have chosen **Select Target Folder**, as shown above:
     - You can select any folder.
     - You can hover over a folder and click at the end of the row to drill down into subfolders, and then select a folder.
   - If you have selected the same destination system and Volume as where the source folder/file was located, you can select **Maintain Source Folder Path** to restore the folder, or file(s), to the same folder where they existed in the source structure. All the same folders and sub-folders must already exist; folders are not created. When restoring files to their original location, you can choose to overwrite the source file(s) or to create new file(s).

9. Select **Restore** to return to the Restore Dashboard and review the progress of the restore operation.

Copyright information

Trademark information