Restoring data from backup files

Cloud Manager

Tom Onacki, Aksel Davis

February 17, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_restore_backups.html on February 28, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Restoring data from backup files

Backups are stored in an object store in your cloud account so that you can restore data from a specific point in time. You can restore an entire volume from a saved backup file, or if you only need to restore a few files, you can restore up to 8 individual files (at one time) from a saved backup file.

You can restore an entire volume to the same working environment, to a different working environment that’s using the same cloud account, or to an on-premises ONTAP system. See Restoring a volume from a backup.

You can restore files to a volume in the same working environment, to a volume in a different working environment that’s using the same cloud account, or to a volume on an on-premises ONTAP system. See Restoring files from a backup.

Supported working environments and object storage providers

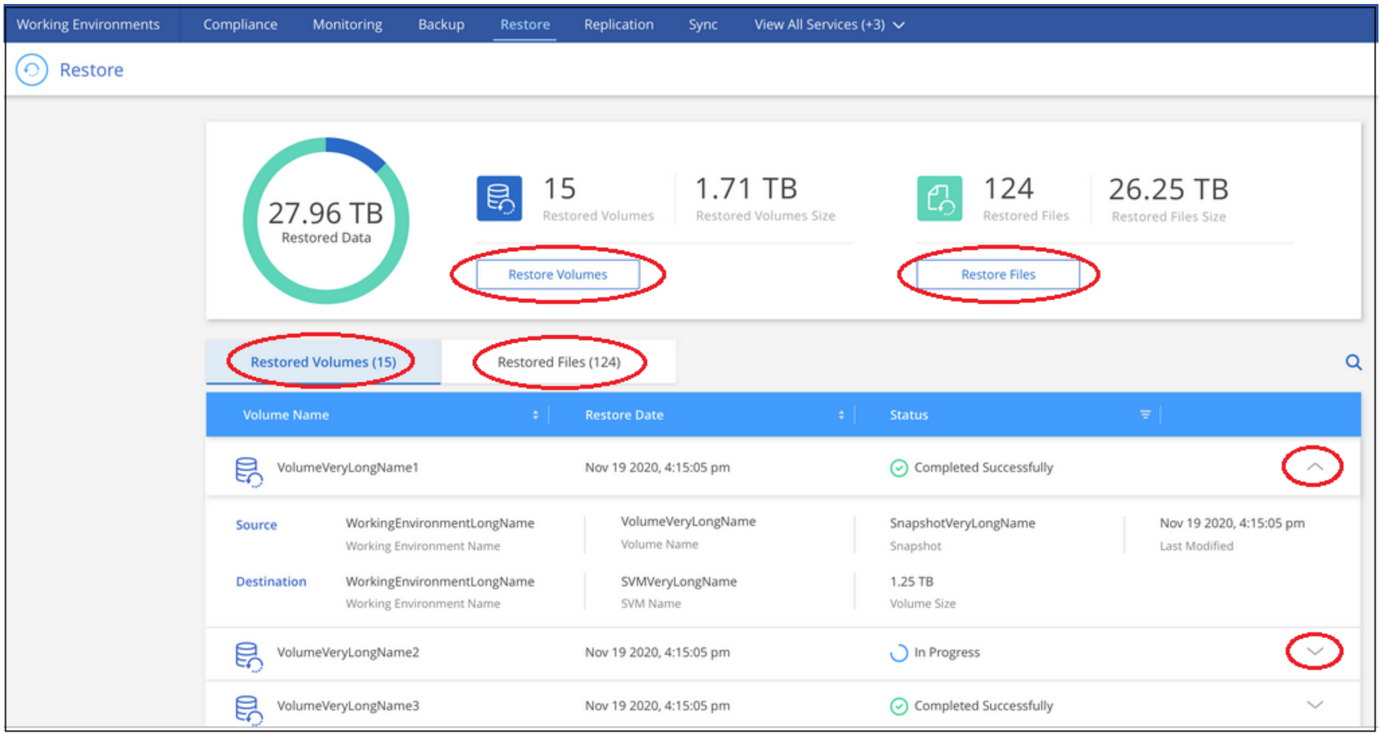
You can restore a volume, or individual files, from a backup file to the following working environments:

Backup File Location	Destination Working Environment	
	Volume Restore	**File Restore**
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	

The Restore Dashboard

You access the Restore Dashboard by clicking the **Restore** tab from the top of Cloud Manager, or you can click the **Activate** or **Enable** button for the Restore service from the Services panel.

> ℹ The Cloud Backup service must already be activated for at least one working environment.



Volume Name	Restore Date	Status
VolumeVeryLongName1	Nov 19 2020, 4:15:05 pm	Completed Successfully
VolumeVeryLongName2	Nov 19 2020, 4:15:05 pm	In Progress
VolumeVeryLongName3	Nov 19 2020, 4:15:05 pm	Completed Successfully

Source	WorkingEnvironmentLongName Working Environment Name	VolumeVeryLongName Volume Name	SnapshotVeryLongName Snapshot	Nov 19 2020, 4:15:05 pm Last Modified
Destination	WorkingEnvironmentLongName Working Environment Name	SVMVeryLongName SVM Name	1.25 TB Volume Size	

The Restore Dashboard provides buttons for you to restore volumes and files. Clicking the *Restore Volumes* or *Restore Files* buttons starts a wizard that walks you through the steps to restore that data.

The dashboard also provides a list of all the volumes and all the files you have restored in case you need a history of previous restore actions. You can expand the row for each restored volume or file to view the details about the source and destination locations for the volume or file.

Restoring a volume from a backup file

When you restore a volume from a backup file, Cloud Manager creates a *new* volume using the data from the backup. You can restore the data to a volume in the same working environment or to a different working environment that's located in the same cloud account as the source working environment. You can also restore files to an on-premises ONTAP system.

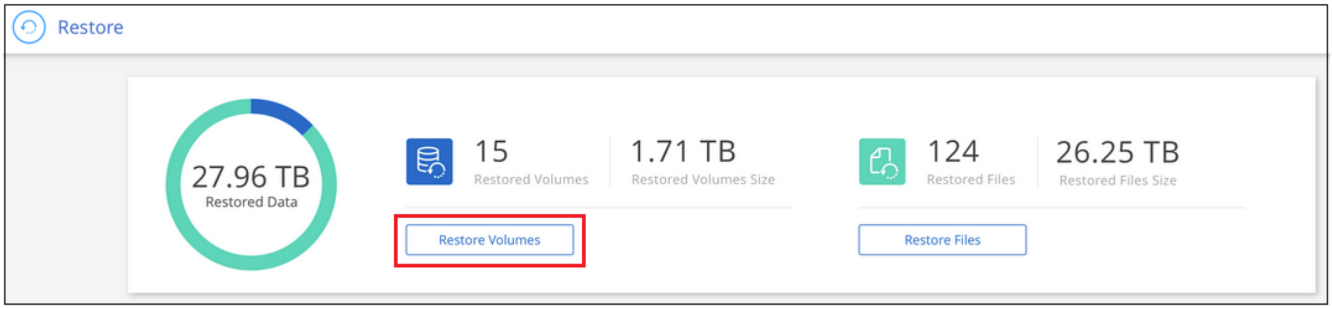
You should know the name of the volume you want to restore and the date of the backup file you want to use to create the newly restored volume.

Steps

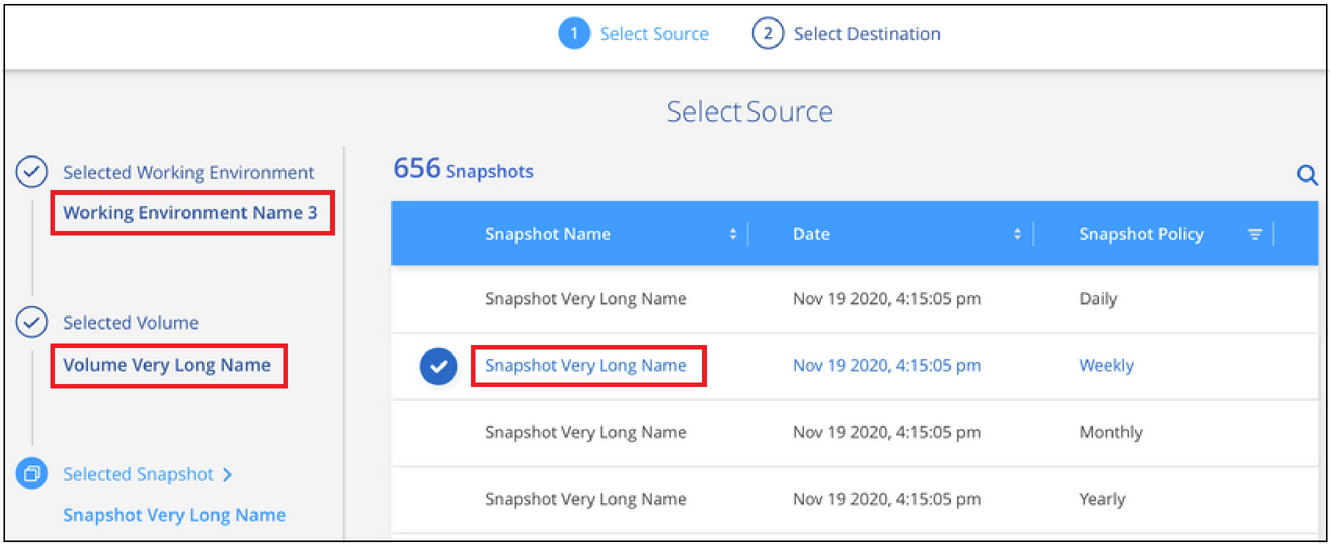
1. Select the **Restore** tab.

   The Restore Dashboard appears.

2. Click **Restore Volumes**.



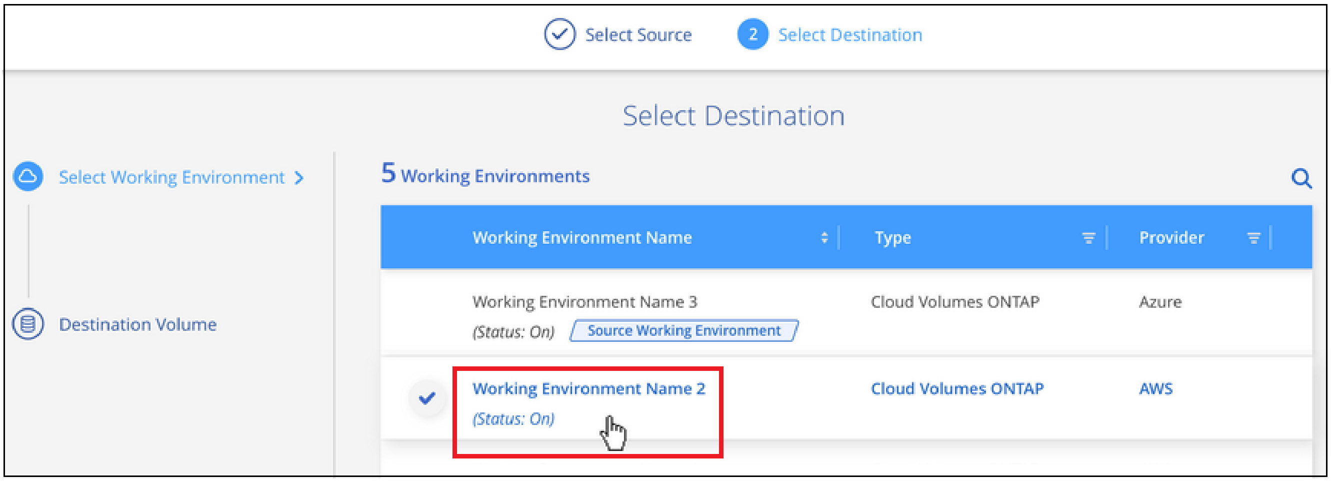
3. In the *Select Source* page, navigate to the backup file (snapshot) for the volume you want to restore. Select the **Working Environment**, the **Volume**, and the **Snapshot** that has the date/time stamp that you want to restore.



	Snapshot Name	Date	Snapshot Policy
	Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Daily
✓	Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Weekly
	Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Monthly
	Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Yearly

4. Click **Continue**.

5. In the *Select Destination* page, select the **Working Environment** where you want to restore the volume.



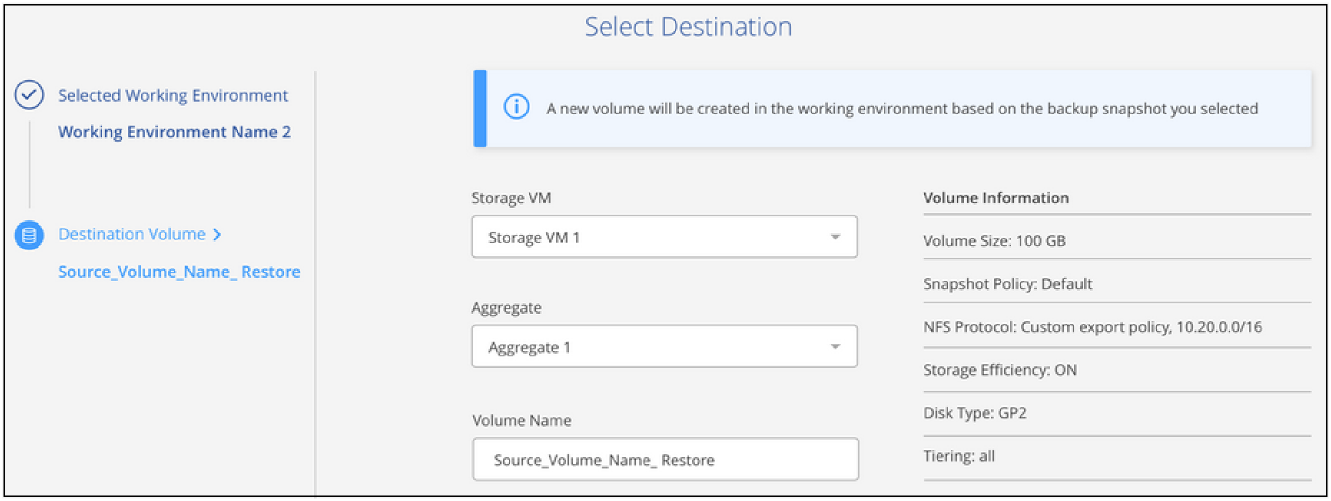
	Working Environment Name	Type	Provider
	Working Environment Name 3 (Status: On) Source Working Environment	Cloud Volumes ONTAP	Azure
✓	Working Environment Name 2 (Status: On)	Cloud Volumes ONTAP	AWS

6. 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, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the AWS Access Key and Secret Key needed to access the object storage.

    - When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volumes reside.
    - 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.

7. Select the Storage VM where the volume will reside and enter the name you want to use for the restored volume. By default, **<source_volume_name>_Restore** is used as the volume name.



Select Destination

Selected Working Environment
Working Environment Name 2

Destination Volume >
Source_Volume_Name_ Restore

A new volume will be created in the working environment based on the backup snapshot you selected

Storage VM: Storage VM 1

Aggregate: Aggregate 1

Volume Name: Source_Volume_Name_ Restore

Volume Information
Volume Size: 100 GB
Snapshot Policy: Default
NFS Protocol: Custom export policy, 10.20.0.0/16
Storage Efficiency: ON
Disk Type: GP2
Tiering: all

   You can select the Aggregate that the volume will use for its' capacity when restoring a volume to an on-prem ONTAP system.

8. Click **Restore** and you are returned to the Restore Dashboard so you can review the progress of the restore operation.

Result

Cloud Manager creates a new volume based on the backup you selected. You can manage this new volume as required.

Restoring files from a backup

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

You can restore up to 8 files at a time from a volume in a backup file. All the files are restored to the same destination volume that you choose. If you need to restore more than 8 files you can run the restore process a second time.

Restoring individual files from a backup file uses a separate Restore instance/virtual machine.

File Restore process

The process goes like this:

1. When you want to restore one or more files from a volume, click the Restore tab, click **Restore Files**, and select the backup file in which the file (or files) reside.

2. The Restore instance starts up and displays the folders and files that exist within the backup file.

   Note: The Restore instance is deployed in your cloud providers' environment the first time you restore a file.

3. Choose the file (or files) that you want to restore from that backup.
4. Select the location where you want the file(s) to be restored (the working environment, volume, and folder), and click **Restore**.
5. The file(s) are restored, and then the Restore instance is shut down to save costs after a period of inactivity.

Details

Costs

See this topic for the cost of the Cloud Backup service and the Restore instance.

Instance type

- In AWS, the Restore instance runs on an m5n.xlarge instance with 4 CPUs, 16 GiB Memory, and EBS Only instance storage. In regions where m5n.xlarge instance isn’t available, Restore runs on an m5.xlarge instance instead.
- In Azure, the Restore virtual machine runs on a Standard_D4s_v3 VM with 4 CPUs, 16 GiB Memory, and a 32 GB disk.

The instance is named *Cloud-Restore-Instance* with your Account ID concatenated to it. For example: *Cloud-Restore-Instance-MyAccount*.

Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before Cloud Restore is deployed.

AWS permissions required

When using file Restore with AWS, the IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest Cloud Manager policy as described in AWS requirements.

Additionally, the following permissions are needed in the policy for file restore:

```
"Action": [
  "ec2:DescribeInstanceTypeOfferings",
  "ec2:startInstances",
  "ec2:stopInstances",
  "ec2:terminateInstances"
],
```

Enable outbound internet access

Cloud Restore requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the instance has outbound internet access to contact the following endpoints. When you deploy Cloud Restore in the cloud, it is located in the same subnet as the Connector.

Review the appropriate table depending on whether you are deploying Cloud Restore in AWS or Azure.

Required endpoints for AWS deployments:

Endpoints	Purpose
http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/	CentOS package for the Cloud Restore Instance AMI.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance image repository.

Required endpoints for Azure deployments:

Endpoints	Purpose
http://olcentgbl.trafficmanager.net https://olcentgbl.trafficmanager.net	Provides CentOS packages for the Cloud Restore virtual machine.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance image repository.

Restoring a single file from a backup file

Follow these steps to restore up to 8 files from a volume backup to a volume. You should know the name of the volume and the date of the backup file that you want to use to restore the file, or files. This functionality uses Live Browsing so that you can view the list of directories and files within the backup file.

Note that the wording in the UI calls each backup file a "snapshot" because backup files are created using NetApp Snapshot technology.

The following video shows a quick walkthrough of restoring a single file:

[] | *https://img.youtube.com/vi/ROAY6gPL9N0/maxresdefault.jpg*

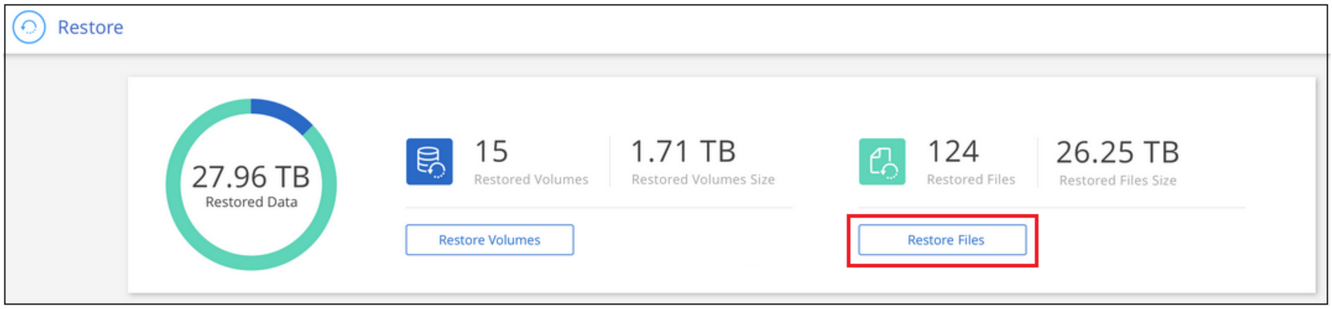
> ℹ The ONTAP version must be 9.6 or greater in your source and destination ONTAP systems.

Steps

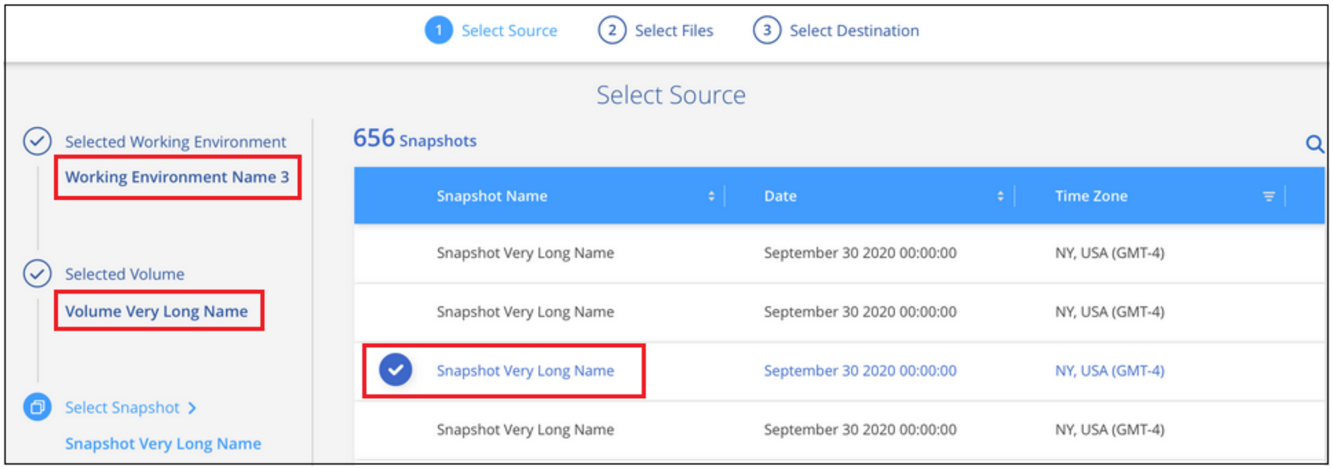
1. Click the **Restore** tab.

   The Restore Dashboard appears.

2. Click the **Restore Files** button.



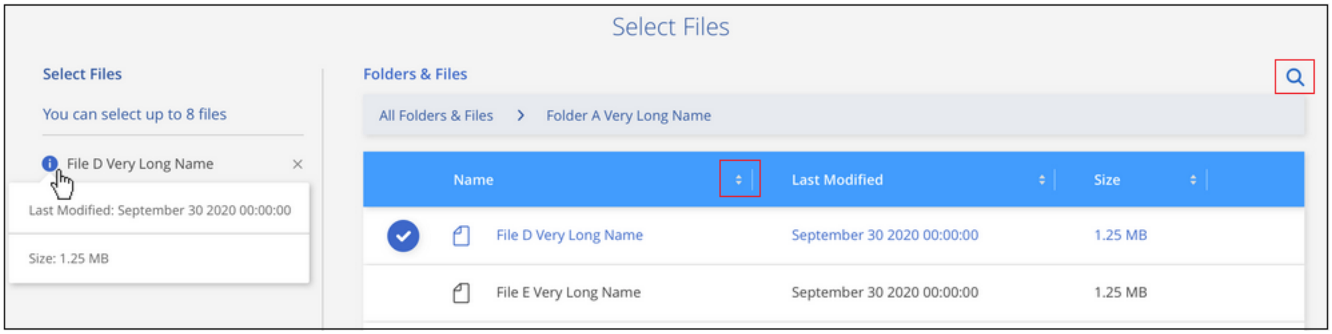
3. In the *Select Source* page, navigate to the backup file (snapshot) for the volume that contains the files you want to restore. Select the **Working Environment**, the **Volume**, and the **Snapshot** that has the date/time stamp from which you want to restore files.



Snapshot Name	Date	Time Zone
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)
✓ Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)

4. Click **Continue** and the Restore instance is started. After a few minutes the Restore instance displays the list of folders and files from the volume snapshot.

   Note: The Restore instance is deployed in your cloud providers' environment the first time you restore a file, so this step could take a few minutes longer the first time.

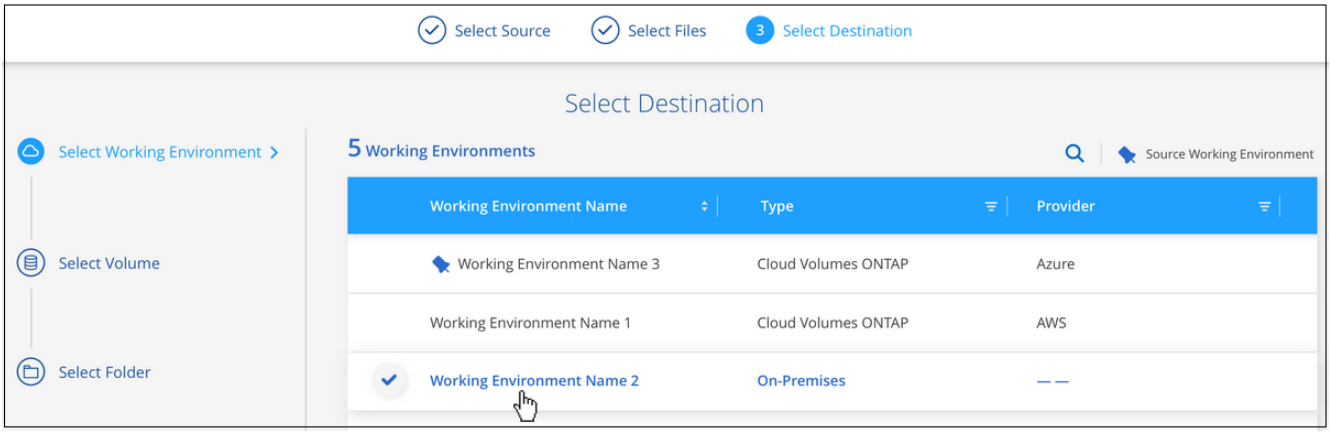

Select Files
Select Files
You can select up to 8 files
File D Very Long Name ×
Last Modified: September 30 2020 00:00:00
Size: 1.25 MB
Folders & Files
All Folders & Files > Folder A Very Long Name

Name	Last Modified	Size
✓ File D Very Long Name	September 30 2020 00:00:00	1.25 MB
File E Very Long Name	September 30 2020 00:00:00	1.25 MB

5. In the *Select Files* page, select the file or files that you want to restore and click **Continue**.
   - You can click the search icon and enter the name of the file to navigate directly to the file.
   - You can click the file name if you see it.
   - You can navigate down levels in folders using the ❯ button at the end of the row to find the file.

     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 clicking the **x** next to the file name.

6. In the *Select Destination* page, select the **Working Environment** where you want to restore the files.

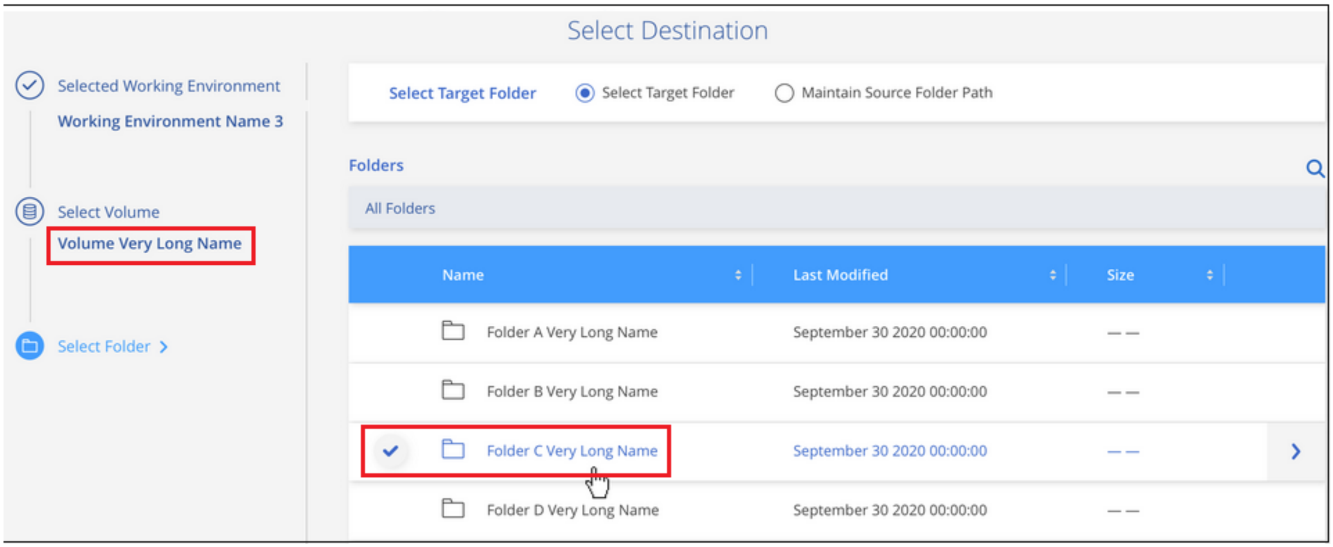


Working Environment Name	Type	Provider
Working Environment Name 3	Cloud Volumes ONTAP	Azure
Working Environment Name 1	Cloud Volumes ONTAP	AWS
✓ Working Environment Name 2	On-Premises	— —

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 volumes reside, and the AWS Access Key and Secret Key needed to access the object storage.
- When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volumes reside.

7. Then select the **Volume** and the **Folder** where you want to restore the files.



Name	Last Modified	Size
Folder A Very Long Name	September 30 2020 00:00:00	— —
Folder B Very Long Name	September 30 2020 00:00:00	— —
✓ Folder C Very Long Name	September 30 2020 00:00:00	— —
Folder D Very Long Name	September 30 2020 00:00:00	— —

You have a few options for the location when restoring files.

- 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 Working Environment and Volume as where the source file was located (as identified by the ◆ icon), you can select **Maintain Source Folder Path** to restore the file, or all files, 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.

8. Click **Restore** and you are returned to the Restore Dashboard so you can review the progress of the restore operation.

The Restore instance is shut down after a certain period of inactivity to save you money so that you incur costs only when it is active.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.