



Create and manage volumes for Amazon FSx for ONTAP

Cloud Manager

Julia
October 04, 2021

Table of Contents

- Create and manage volumes for Amazon FSx for ONTAP 1
 - Creating volumes 1
 - Mounting volumes 5
 - Editing volumes 6
 - Cloning the volume 6
 - Managing Snapshot copies 6
 - Changing the tiering policy 6
 - Replicating and syncing data 7
 - Deleting volumes 7
 - Removing FSx for ONTAP from the workspace 7
 - Deleting the FSx for ONTAP working environment 8

Create and manage volumes for Amazon FSx for ONTAP

After you set up your working environment, you can create and manage FSx for ONTAP volumes, clones, and snapshots, change tiering policies, and remove or delete FSx for ONTAP.

Creating volumes

You can create and edit NFS and CIFS volumes in a new or existing FSx for ONTAP working environment. Volumes created using ONTAP CLI will also be visible in your FSx for ONTAP working environment.

Before you begin

You need:

- An active [Connector in AWS](#).

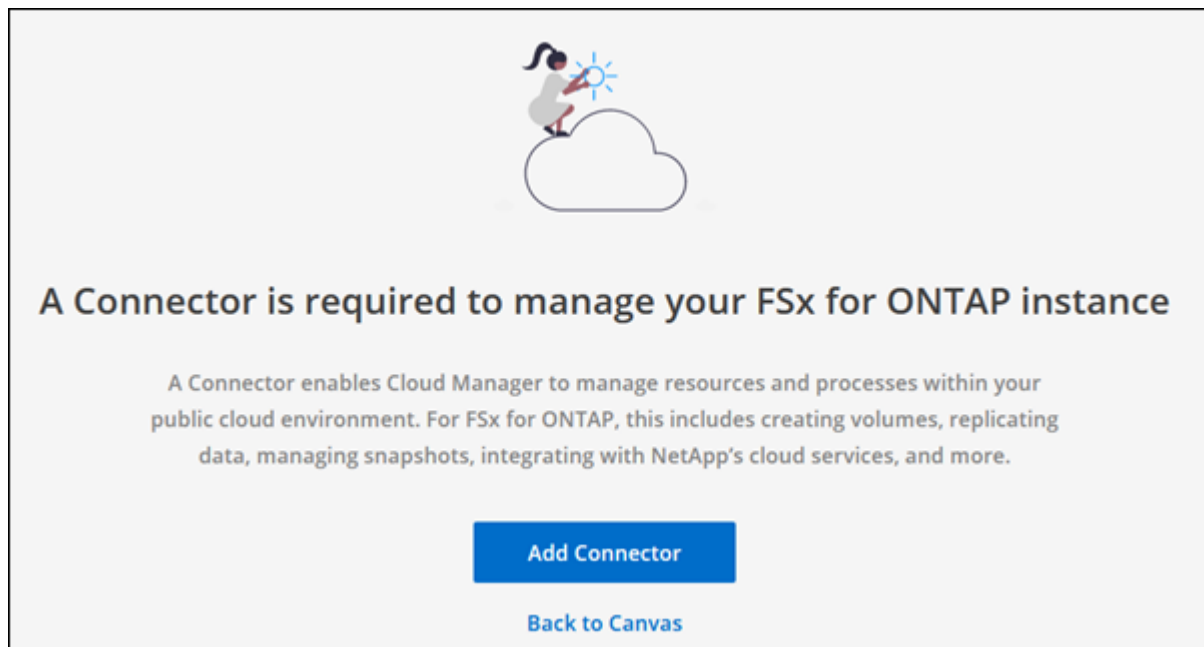


You do not need a Connector in AWS to remove or delete a working environment.

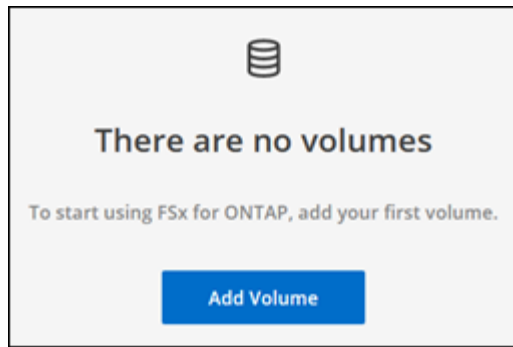
- If you want to use SMB, you must have set up DNS and Active Directory.

Steps

1. Open the FSx for ONTAP working environment.
2. If you don't have a Connector enabled, you'll be prompted to add one.



3. Click the **Volumes** tab
4. Click **Add Volume**.



5. **Volume Details and Protection:**

- a. Enter a name for your new volume.
- b. Enter the volume size. Note that the volume size will grow with usage.
- c. Select a snapshot policy. By default, a snapshot is taken every hour (keeping the last six copies), every day (keeping the last two copies), and every week (keeping the last two copies).
- d. Click **Next**.

A light gray rectangular form titled "Volume Details & Protection" at the top center. It contains three main sections: 1. "Volume Name" with a text input field containing "myfsxvol" and an information icon (i) to its right. 2. "Size (GiB)" with a numeric input field containing "3" and an information icon (i) to its right. 3. "Snapshot Policy" with a dropdown menu showing "default" and a downward arrow. Below the dropdown, the text "default policy" is shown with an information icon (i).

6. **Protocol:** Select the an NFS or CIFS volume protocol.

- a. For NFS:
 - Select an Access Control policy.
 - Select the NFS versions.
 - Select a Custom Export Policy. Click the information icon for valid value criteria.

☒ Details & Protection
 ☒ 2 Protocol
 ☐ 3 Usage Profile & Tiering Policy
 ☐ 4 Review

Volume Protocol

Select the volume's protocol: ☒ **NFS Protocol** ☐ CIFS Protocol

Access Control

Custom_export_policy

Select NFS Version

☒ NFSv3 ☒ NFSv4

Custom Export Policy ⓘ

10.20.0.0/16

b. For CIFS:

- Enter a Share Name.
- Enter users or groups separated by a semicolon.
- Select the permission level for the volume.

☒ Details & Protection
 ☒ 2 Protocol
 ☐ 3 Usage Profile & Tiering Policy
 ☐ 4 Review

Volume Protocol

Select the volume's protocol: ☐ NFS Protocol ☒ **CIFS Protocol**

Share Name

<Volume name>_share

Users/Groups ⓘ

Everyone;

Permissions

Full Control



If this is the first CIFS volume for this working environment, you will be prompted to configure CIFS connectivity using an *Active Directory* or *Workgroup* setup.

- If you select an Active Directory setup, you'll need to provide the following configuration information.

Field	Description
DNS Primary IP Address	The IP addresses of the DNS servers that provides name resolution for the CIFS server. The listed DNS server must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select Enable NTP Server Configuration to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details.

- If you select a Workgroup setup, enter the server and workgroup name for a workgroup configured for CIFS.

c. Click **Next**.

7. Usage Profile and Tiering:

- By default, **Storage Efficiency** is disabled. You can change this setting to enable deduplication and compression.
- By default, **Tiering Policy** is set to **Snapshot Only**. You can select a different tiering policy based on your needs.
- Click **Next**.

Usage Profile & Tiering Policy

Usage Profile

Storage Efficiency

☐ Enabled - Deduplication, compression and compaction
 ☒ Disabled - No Efficiency

Tiering data to object storage

Tiering policy

☐ Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
 ☒ Snapshot Only - Tiers cold Snapshot copies to object storage.
 ☐ None - Data tiering is disabled.
 ☐ All - Immediately tiers all data (not including metadata) to object storage.

- Review:** Review your volume configuration. Click **Previous** to change settings or click **Add** to create the volume.

Result

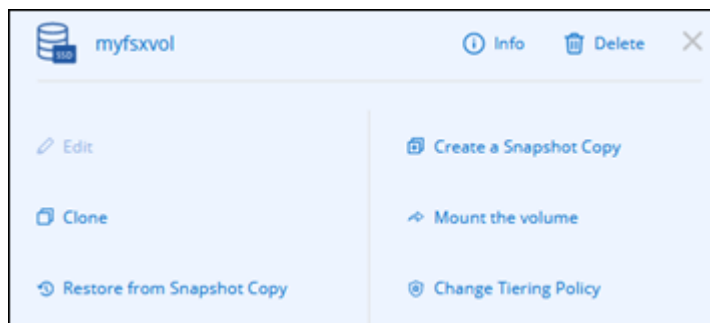
The new volume is added to the working environment.

Mounting volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

Steps

- Open the working environment.
- Open the volume menu and select **Mount the volume**.



- Follow the instructions to mount the volume.

Editing volumes

After you create a volume, you can modify it at any time.

Steps

1. Open the working environment.
2. Open the volume menu and select **Edit**.
 - a. For NFS, you can modify the size and tags.
 - b. For CIFS, you can modify the share name, users, permissions, and Snapshot policy as needed.
3. Click **Apply**.

Cloning the volume

After you create a volume, you can create a new read-write volume from a new Snapshot.

Steps

1. Open the working environment.
2. Open the volume menu and select **Clone**.
3. Enter a name for the cloned volume.
4. Click **Clone**.

Managing Snapshot copies

Snapshot copies provide a point-in-time copy of your volume. Create Snapshot copies and restore the data to a new volume.

Steps

1. Open the working environment.
2. Open the volume menu and choose one of the available options to manage Snapshot copies:
 - **Create a Snapshot copy**
 - **Restore from a Snapshot copy**
3. Follow the prompts to complete the selected action.

Changing the tiering policy

Change the tiering policy for the volume.

Steps

1. Open the working environment.
2. Open the volume menu and select **Change Tiering policy**.
3. Select a new volume tiering policy and click **Change**.

Replicating and syncing data

You can replicate data between storage environments using Cloud Manager. To configure FSx for ONTAP replication, see [replicating data between systems](#).

You can create sync relationships using Cloud Sync in Cloud Manager. To configure sync relationships, see [create sync relationships](#).

Deleting volumes

Delete the volumes that you no longer need.

Before you begin

You cannot delete a volume that was previously part of a SnapMirror relationship using Cloud Manager. SnapMirror volumes must be deleted using the AWS Management Console or CLI.

Steps

1. Open the working environment.
2. Open the volume menu and select **Delete**.
3. Enter the working environment name and confirm that you want to delete the volume. It can take up to an hour before the volume is completely removed from Cloud Manager.



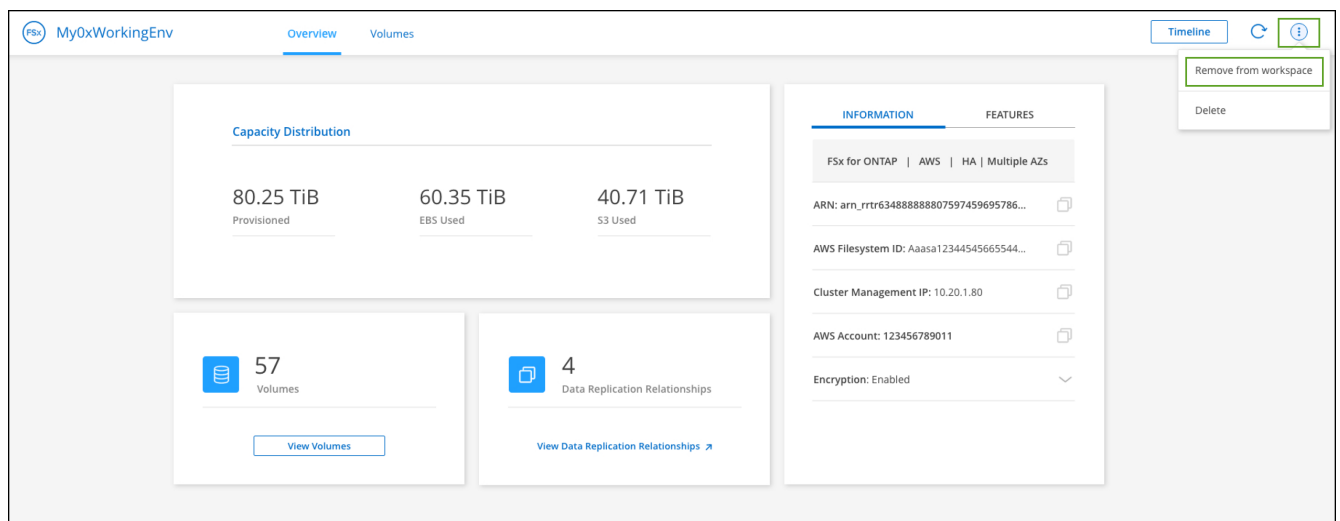
If you try to delete a cloned volume, you will receive an error.

Removing FSx for ONTAP from the workspace

You can remove FSx for ONTAP from Cloud Manager without deleting your FSx for ONTAP account or volumes. You can add the FSx for ONTAP working environment back to Cloud Manager at any time.

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed with removing the working environment.
2. At the top right of the page, select the actions menu and click **Remove from workspace**.



3. Click **Remove** to remove FSx for ONTAP from Cloud Manager.

Deleting the FSx for ONTAP working environment

You can delete the FSx for ONTAP from Cloud Manager.

Before you begin

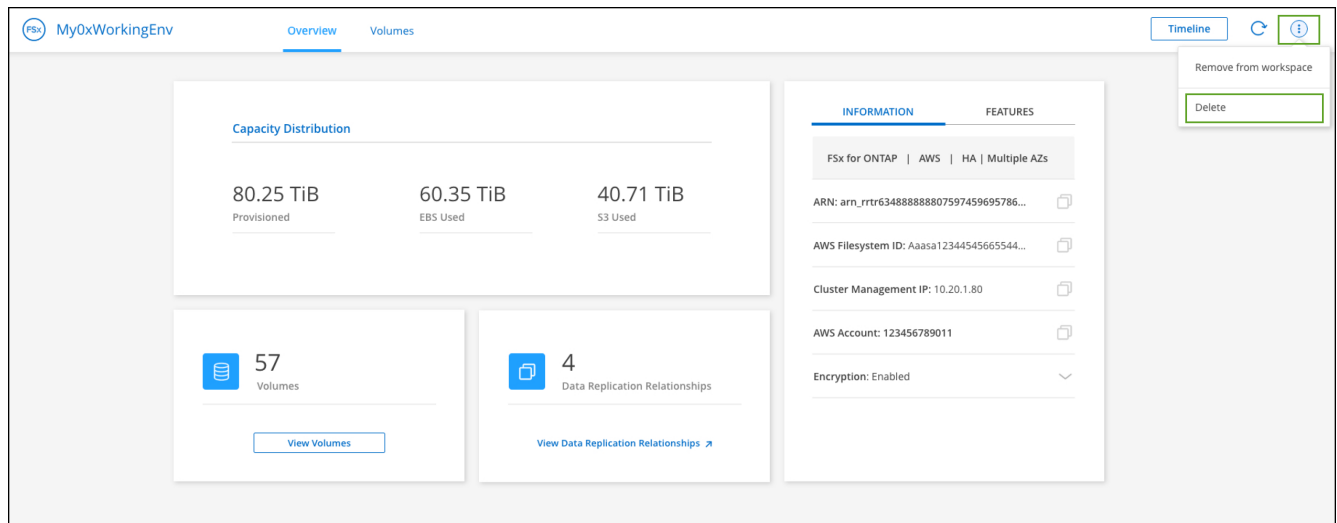
- You must delete all volumes associated with the file system.
- You cannot delete a working environment that contains failed volumes. Failed volumes must be deleted using the AWS Management Console or CLI prior to deleting FSx for ONTAP files system.



This action will delete all resources associated with the working environment. This action cannot be undone.

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed to deleting the working environment.
2. At the top right of the page, select the actions menu and click **Delete**.



3. Enter the name of the working environment and click **Delete**.

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.