



Amazon FSx for ONTAP

Cloud Manager

NetApp
February 25, 2022

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_fsx_aws.html on February 25, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Amazon FSx for ONTAP 1
 - Learn about Amazon FSx for ONTAP 1
 - Get started with Amazon FSx for ONTAP 2
 - Set up permissions for FSx for ONTAP 2
 - Create and manage an Amazon FSx for ONTAP working environment 5
 - Create and manage volumes for Amazon FSx for ONTAP 13

Amazon FSx for ONTAP

Learn about Amazon FSx for ONTAP

[Amazon FSx for ONTAP](#) is a fully managed service allowing customers to launch and run file systems powered by NetApp's ONTAP storage operating system. FSx for ONTAP provides the same features, performance, and administrative capabilities NetApp customers use on premises, with the simplicity, agility, security, and scalability of a native AWS service.

Features

- No need to configure or manage storage devices, software, or backups.
- Support for CIFS, NFSv3, NFSv4.x, and SMB v2.0 - v3.1.1 protocols.
- Low cost, virtually unlimited data storage capacity using available Infrequently Accessed (IA) storage tier.
- Certified to run on latency-sensitive applications including Oracle RAC.
- Choice of bundled and pay-as-you-go pricing.

Additional features in Cloud Manager

- Using a Connector in AWS and Cloud Manager, you can create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as Data Sense and Cloud Sync.
- Using Artificial Intelligence (AI) driven technology, Cloud Data Sense can help you understand data context and identify sensitive data that resides in your FSx for ONTAP accounts. [Learn more](#).
- Using NetApp Cloud Sync, you can automate data migration to any target in the cloud or on premises. [Learn more](#)

Cost

Your FSx for ONTAP account is maintained by AWS and not by Cloud Manager. [Amazon FSx for ONTAP getting started guide](#)

There is an additional cost associated with using the Connector in AWS and the optional data services such as Cloud Sync and Data Sense.

Supported regions

[View supported Amazon regions.](#)

Getting help

Amazon FSx for ONTAP is an AWS first-party solution. For questions or technical support issues associated with your AWS FSx file system, infrastructure or any AWS solution using this service, use the Support Center in your AWS console to open a support case to AWS. Select the "FSx for ONTAP" service and appropriate category. Provide the remaining information required to create your AWS support case.

For general questions specific to Cloud Manager or Cloud Manager micro-services, you can start with the in-line Cloud Manager chat.

For technical support issues specific to Cloud Manager or micro-services within, you can open a NetApp support ticket using your Cloud Manager account level serial number. You will need to register your Cloud Manager serial number to activate support.

Limitations

- Cloud Manager can replicate data only from on-premises or Cloud Volumes ONTAP to FSx for ONTAP.
- At this time iSCSI volumes can be created using the ONTAP CLI, ONTAP API, or Cloud Manager API.

Get started with Amazon FSx for ONTAP

Get started with Amazon FSx for ONTAP in a few steps.

You can get started with FSx for ONTAP in just a few steps.

1

Create an FSx for ONTAP working environment

You must create an Amazon FSx for ONTAP working environment before adding volumes. You will need an AWS access key and secret key for an [IAM user with FSx for ONTAP permissions](#).

2

Create a Connector

You must have a [Connector for AWS](#) to open the FSx for ONTAP working environment, create volumes, or perform other actions. When a Connector is required, Cloud Manager will prompt you if one is not already added.

3

Add volumes

You can create FSx for ONTAP volumes using Cloud Manager.

4

Manage your volumes

Use Cloud Manager to manage your volumes and configure additional services such as replication, Cloud Sync, and Data Sense.

Related links

- [Creating a Connector from Cloud Manager](#)
- [Launching a Connector from the AWS Marketplace](#)
- [Installing the Connector software on a Linux host](#)

Set up permissions for FSx for ONTAP

To create or manage an Amazon FSx for ONTAP working environment, you need an AWS access key and secret key for an IAM user with FSx for ONTAP permissions. These permissions are different from the permissions required to create a Connector in AWS.

To grant FSx for ONTAP permissions to a user, you need to create a new IAM policy or edit an exiting policy.

You can then attach the policy to a user or user group.

Create a new policy

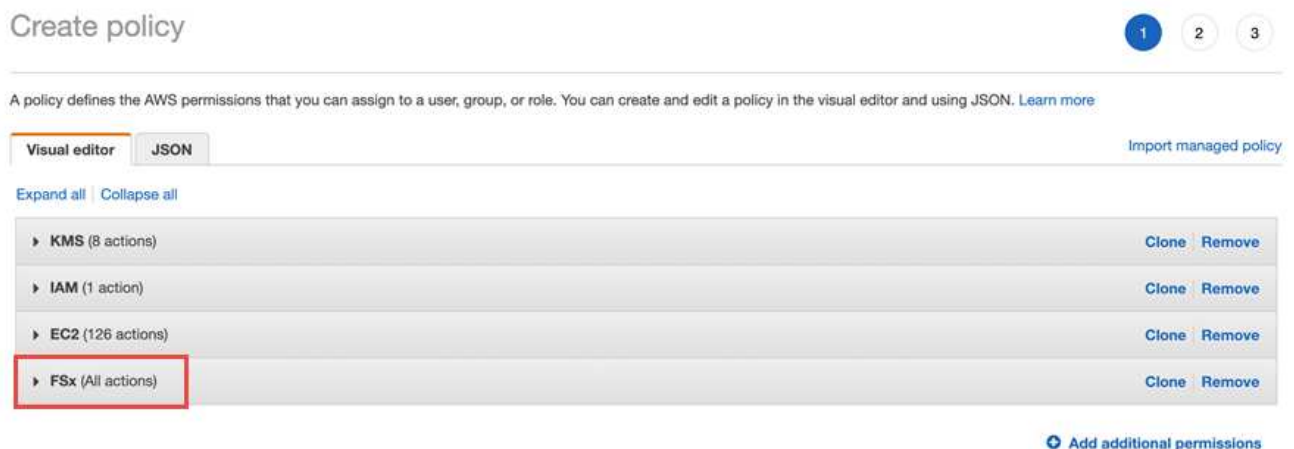
You can create a new IAM policy for FSx for ONTAP.

Steps

1. From the AWS IAM console, Click **Create Policy**.
2. Using the JSON editor, paste the following policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "kms:Describe*",
        "kms:List*",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

3. Open the Visual Editor tab to confirm the correct configuration. Click **Next: Tags**.



4. Optionally, add any tags to help you organize your policies. Click **Next: Review**.
5. Confirm your policy configuration and click **Create Policy**.

6. Type a name and description for your policy and click **Create Policy**.

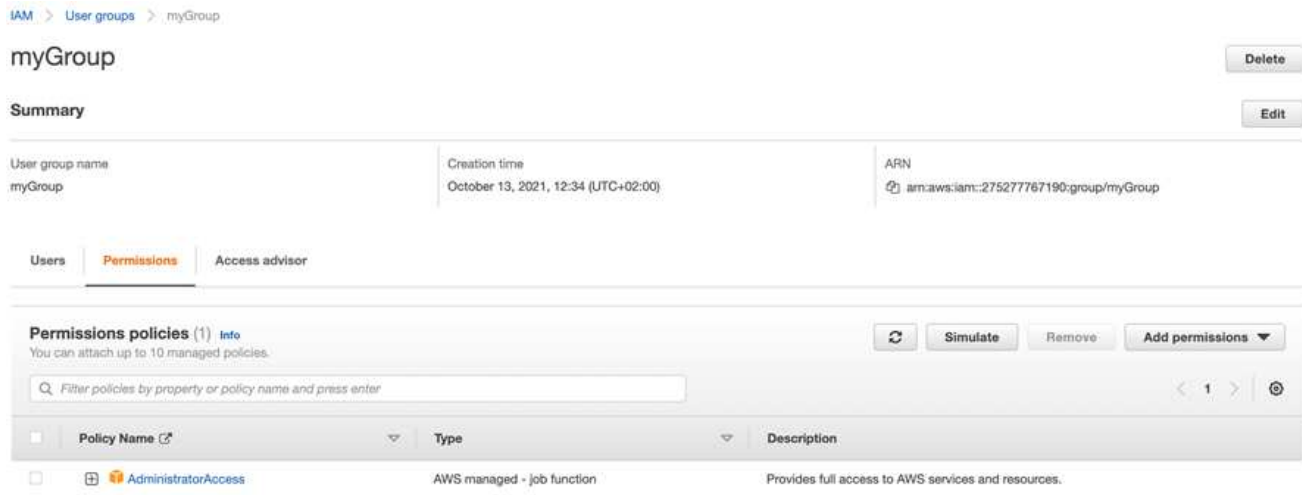
For more details on creating an IAM policy, see [AWS Documentation: Creating IAM Policies](#).

Edit an existing policy

If you have an existing IAM policy, you can edit it to add permissions for FSx for ONTAP.

Steps

1. From the AWS IAM console, select the policy you want to edit.



2. Edit the policy to include the following actions for FSx for ONTAP:

```
"Action": [
    "fsx:*",
    "ec2:Describe*",
    "ec2:CreateTags",
    "kms:Describe*",
    "kms:List*",
    "iam:CreateServiceLinkedRole"
```

Attach the policy

After creating or editing a policy to enable FSx for ONTAP, attach it to an IAM user group or directly to a specific IAM user.

For detailed instructions on creating and managing AWS users and groups, see:

- [AWS Documentation: Creating an IAM user in your AWS account](#)
- [AWS Documentation: Creating IAM user groups](#)

Related links

- [AWS credentials and permissions](#)
- [Create a Connector in AWS](#)
- [Managing AWS credentials for Cloud Manager](#)
- [What Cloud Manager does with AWS permissions](#)

Create and manage an Amazon FSx for ONTAP working environment

Using Cloud Manager you can create and manage FSx for ONTAP working environments to add and manage volumes and additional data services.

Create an Amazon FSx for ONTAP working environment

The first step is to create an FSx for ONTAP working environment. If you already created an FSx for ONTAP file system in the AWS Management Console, you can [discover it using Cloud Manager](#).

Before you begin

Before creating your FSx for ONTAP working environment in Cloud Manager, you will need:

- An AWS access key and secret key for an IAM user with the [required FSx for ONTAP permissions](#).
- The region and VPN information for where you will create the FSx for ONTAP instance.

Steps

1. In Cloud Manager, add a new Working Environment, select the location **Amazon Web Services**, and click **Next**.
2. Select **Amazon FSx for ONTAP** and click **Next**.

Add Working Environment

Choose a Location

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-Premises

Choose Type

Cloud Volumes ONTAP
Single Node

Cloud Volumes ONTAP HA
High Availability

Amazon FSx for ONTAP
High Availability

Kubernetes Cluster
Managed

If you want to discover an existing Amazon FSx for ONTAP in AWS, [Click Here](#)

Next

3. You can select existing FSx for ONTAP credentials or create new credentials using your AWS access key and secret key. Click to verify your IAM user policy adheres to [FSx for ONTAP requirements](#).
4. Provide information about your FSx for ONTAP instance:
 - a. Enter the working environment name you want to use.
 - b. Optionally, you can create tags by clicking the plus sign and entering a tag name and value.
 - c. Enter and confirm the ONTAP Cluster password you want to use.
 - d. Select the option to use the same password for your SVM user or set a different password.
 - e. Click **Next**.

Add FSx for ONTAP

Details and Credentials

Details

Working Environment Name

myfsxenvironment

Tags

Optional

+ Add Tags

Credentials

User Name

fsxadmin

ONTAP Cluster Password

.....

Confirm ONTAP Cluster Password

.....

☒ Use the same password for SVM user (vsadmin)

Previous

Next

5. Provide region and VPC information:

- Select a region and VPC with subnets in at least two Availability Zones so each node is in a dedicated Availability Zone.
- Accept the default security group or select a different one. [AWS security groups](#) control inbound and outbound traffic. These are configured by your AWS admin and are associated with your [AWS elastic network interface \(ENI\)](#).
- Select an Availability Zone and subnet for each node.
- Click **Next**.

- Leave *CIDR Range* empty and click **Next** to automatically set an available range. Optionally, you can use [AWS Transit Gateway](#) to manually configure a range.

- Select route tables that include routes to the floating IP addresses. If you have just one route table for the subnets in your VPC (the main route table), Cloud Manager automatically adds the floating IP addresses to that route table. Click **Next** to continue.

Add FSx for ONTAP
Route Tables

Select the route tables that should include routes to the floating IP addresses. This enables client access to volumes. Clients associated with unselected route tables won't have access to volumes.

[Learn More](#)

2 Route table


<input type="checkbox"/>	Name	Main	ID	Associate with Subnets	Tags	
<input checked="" type="checkbox"/>	VPC4QA	Yes	rtb-0880ec9d aeb55d630	2 Subnets	2	⌵
<input type="checkbox"/>	No tag name	No	rtb-0e0c7d9e a4cf05d66	1 Subnet	1	⌵

Notice: The main route table is the default for the VPC

Previous
Next

8. Accept the default AWS master key or click **Change Key** to select a different AWS Customer Master Key (CMK). For more information on CMK, see [Setting up the AWS KMS](#). Click **Next** to continue.

Add FSx for ONTAP
Data Encryption


AWS Managed Encryption

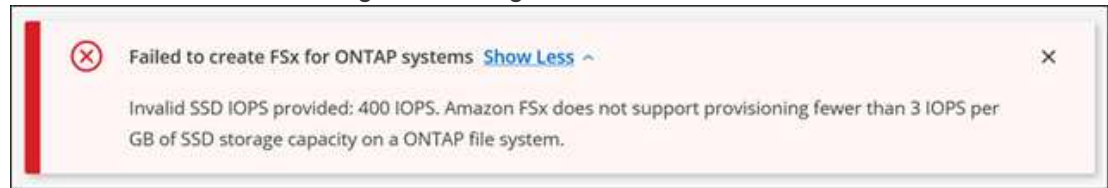
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/fsx [Change Key](#)

Previous
Next

9. Configure your storage:
 - a. Select the throughput, capacity, and unit.
 - b. You can optionally specify an IOPS value. If you don't specify an IOPS value, Cloud Manager will set a default value based on 3 IOPS per GiB of the total capacity entered. For example, if you enter 2000 GiB for the total capacity and no value for the IOPS, the effective IOPS value will be set to 6000.

If you specify an IOPS value that does not meet the minimum requirements, you'll receive an error when adding the working environment.



c. Click **Next**.

Add FSx for ONTAP

Storage Configuration

SSD Disk Properties

Throughput: 512 MBps

Capacity: 3

Unit: TIB

IOPS Value: 400

Optional ⓘ

Notice: The current version of FSx does not allow changing the capacity after creation. Also, note that the capacity drives the cost of the service.

Previous Next

10. Review your configuration:

- Click the tabs to review your ONTAP properties, provider properties, and networking configuration.
- Click **Previous** to make changes to any settings.
- Click **Add** to accept the settings and create your Working Environment.

Review

myfsxenvironment
 FSx for ONTAP | HA | Multiple AZs

Overview

ONTAP Properties	Provider Properties	Networking
HA Deployment Model	Multiple Availability Zone	
Capacity	3 TiB	
Throughput	512 MBps	

Previous
Add

Result

Cloud Manager displays your FSx for ONTAP configuration on the Canvas page.



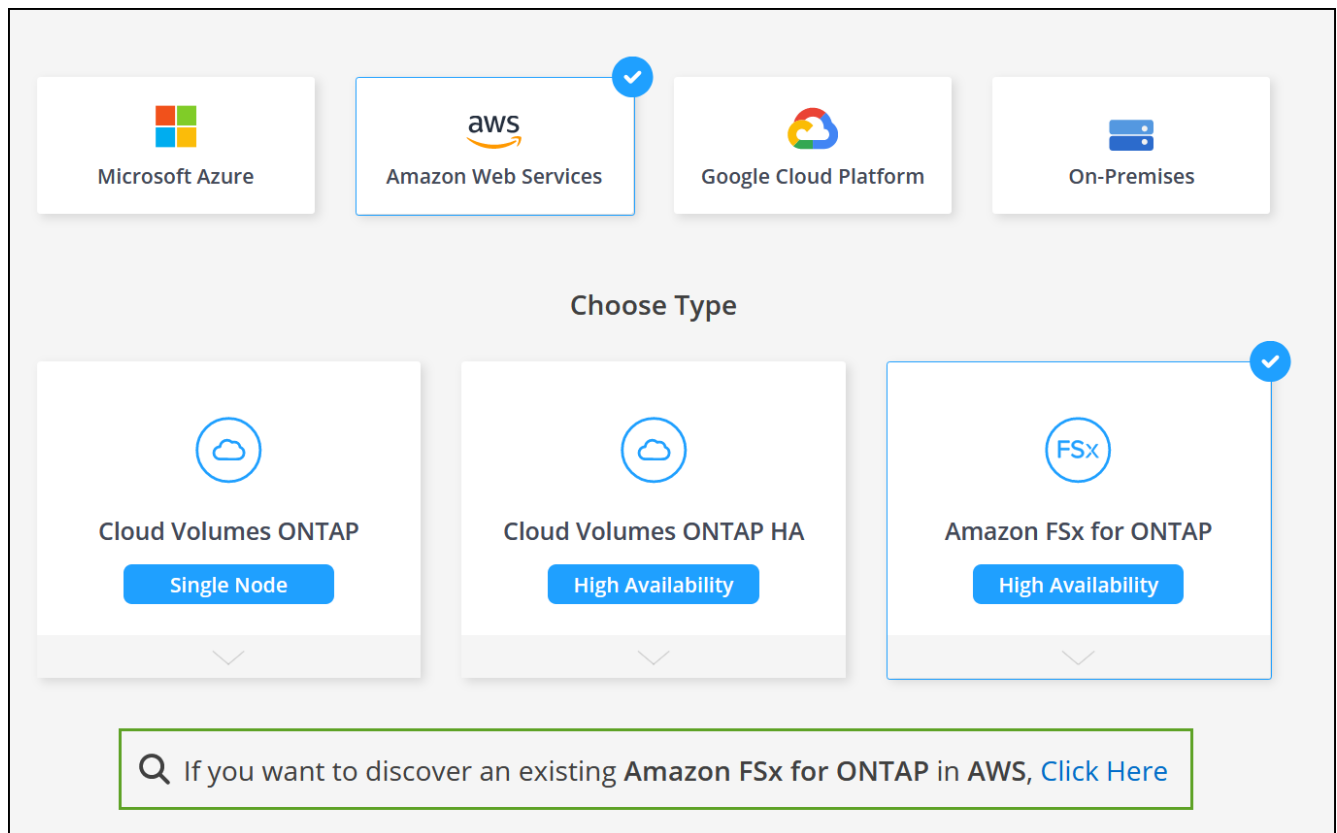
You can now add volumes to your FSx for ONTAP working environment using Cloud Manager.

Discover an existing FSx for ONTAP file system

If you created an FSx for ONTAP file system using the AWS Management Console or if you want to restore a working environment you previously removed, you can discover it using Cloud Manager.

Steps

1. In Cloud Manager, click **Add Working Environment**, select **Amazon Web Services**.
2. Select **Amazon FSx for ONTAP** and click **Click Here**.



3. Select existing credentials or create new credentials. Click **Next**.
4. Select the AWS region and the working environment you want to add.



5. Click **Add**.

Result

Cloud Manager displays your discovered FSx for ONTAP file system.

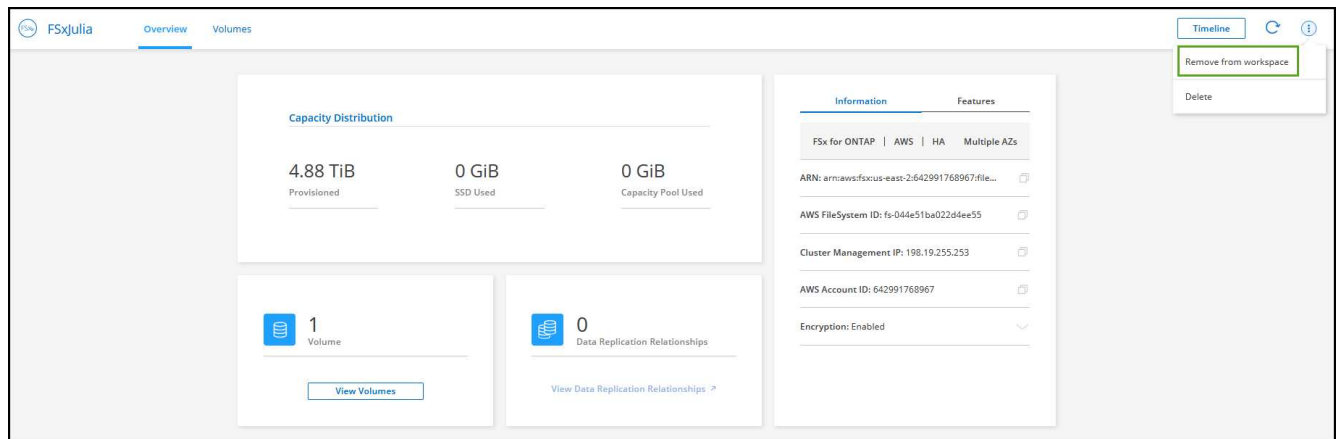
Remove FSx for ONTAP from the workspace

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.

- At the top right of the page, select the actions menu and click **Remove from workspace**.



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

Delete 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 will need an active Connector in AWS to remove or delete volumes.

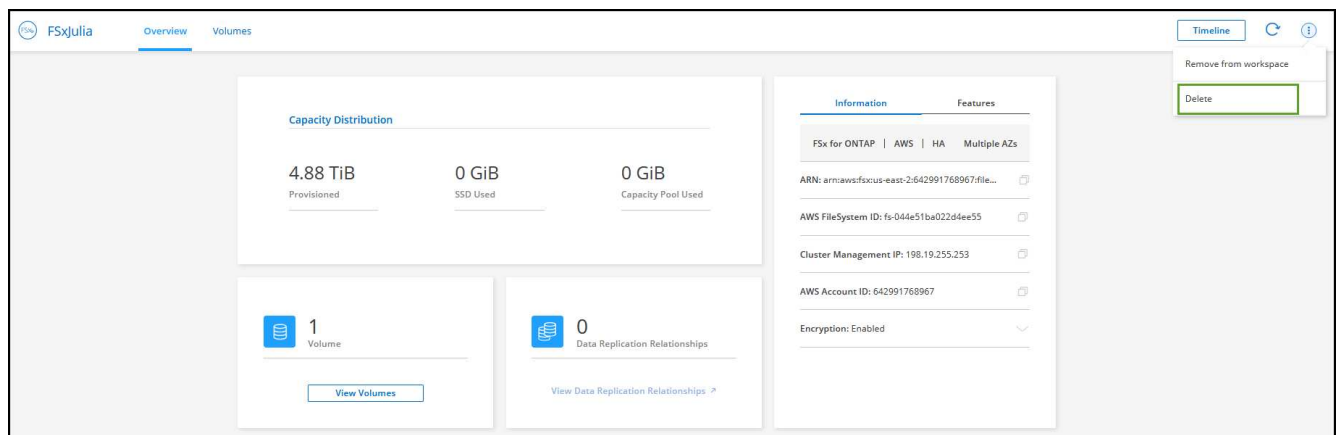
- You cannot delete a working environment that contains failed volumes. Failed volumes must be deleted using the AWS Management Console or CLI prior to deleting FSx for ONTAP files system.



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

Steps

- 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.
- At the top right of the page, select the actions menu and click **Delete**.



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

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, and change tiering policies for FSx for ONTAP.

Create volumes

You can create and manage NFS and CIFS volumes from your FSx for ONTAP working environment in Cloud Manager. NFS and CIFS volumes created using ONTAP CLI will also be visible in your FSx for ONTAP working environment.

You can create iSCSI volumes using ONTAP CLI, ONTAP API, or Cloud Manager API and manage them using Cloud Manager in your FSx for ONTAP working environment.

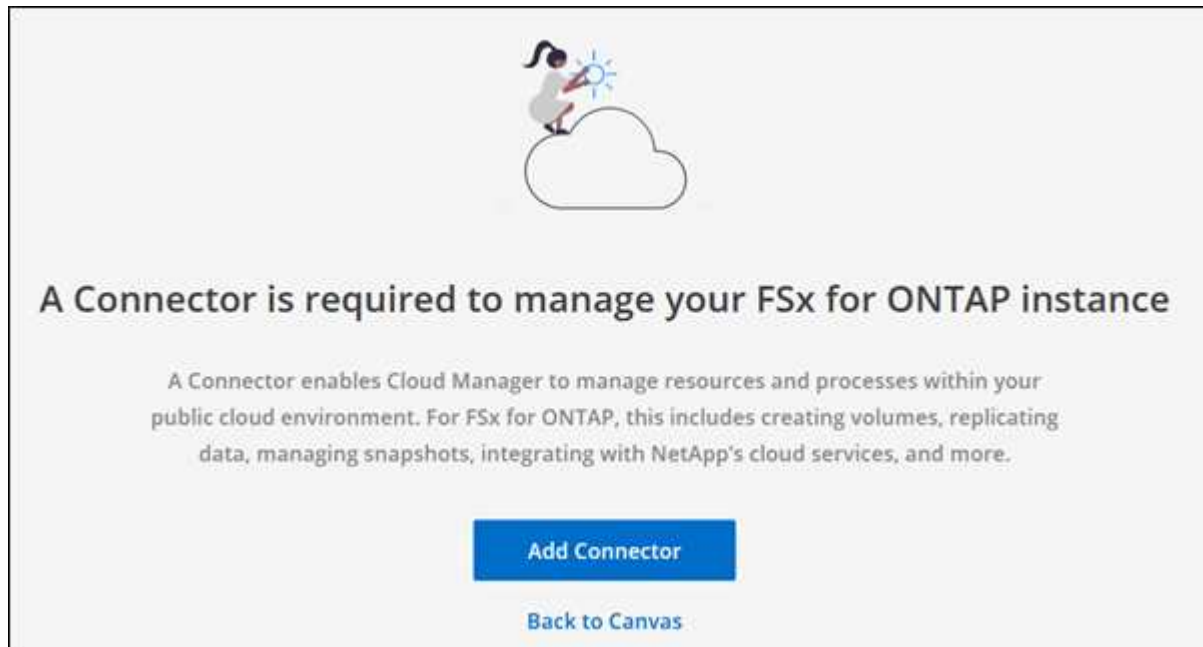
Before you begin

You need:

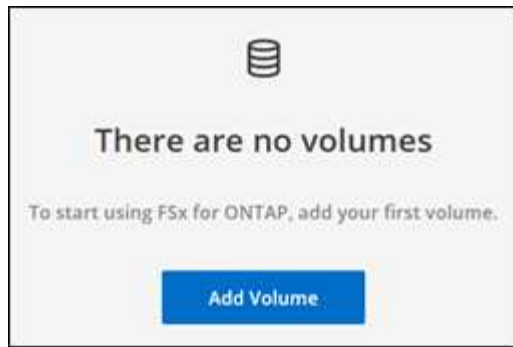
- An active [Connector in AWS](#).
- If you want to use SMB, you must have set up DNS and Active Directory.

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. The Storage VM (SVM) field auto-populates the SVM based on the name of your working environment.
- c. Enter the volume size and select a unit (GiB or TiB). Note that the volume size will grow with usage.
- d. 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).
- e. Click **Next**.

The screenshot shows a web interface for configuring a volume. At the top, there are four tabs: "1 Details and Protection" (active), "2 Protocol", "3 Usage Profile & Tiering Policy", and "4 Review". The main heading is "Volume Details & Protection". Below this, there are four fields: "Volume Name" (a text input with an information icon and a lock icon), "Storage VM (SVM)" (a dropdown menu showing "svm_FSxJulia"), "Volume Size" (a text input with "1-100000" and a range icon), and "Unit" (a dropdown menu with "GiB" selected, and "TiB" and "GiB" as options). Below the "Unit" dropdown, there is a "Snapshot Policy" dropdown menu showing "default", and a link "default policy" with an information icon.

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.

The screenshot shows the 'Volume Protocol' configuration page. At the top, there are four tabs: 'Details & Protection' (checked), '2 Protocol' (active), '3 Usage Profile & Tiering Policy', and '4 Review'. The main heading is 'Volume Protocol'. Below it, a section titled 'Select the volume's protocol:' has two radio buttons: 'NFS Protocol' (selected) and 'CIFS Protocol'. Under 'Access Control', there is a dropdown menu showing 'Custom_export_policy'. To the right, 'Select NFS Version' has two checked checkboxes: 'NFSv3' and 'NFSv4'. Below the dropdown, 'Custom Export Policy' has an information icon and a text input field containing '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.

The screenshot shows the 'Volume Protocol' configuration page with 'CIFS Protocol' selected. The 'Share Name' field contains '<Volume name>_share'. The 'Users/Groups' field contains 'Everyone;' and has an information icon. The 'Permissions' dropdown menu is set to '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.

8. **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.

Mount volumes

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

Steps

1. Open the working environment.
2. Open the volume menu and select **Mount the volume**.



3. Follow the instructions to mount the volume.

Edit 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**.

Clone volumes

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**.

Manage 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.

Change 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**.

Replicate and sync 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](#).

Delete 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.

Copyright Information

Copyright © 2022 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.