Manage volumes

Amazon FSx for NetApp ONTAP

NetApp
February 11, 2026

Table of Contents

Manage volumes

Create an FSx for ONTAP volume in Workload Factory

After setting up your FSx for ONTAP file system, create FSx for ONTAP volumes in Workload Factory as virtual resources for grouping your data.

About this task

FSx for ONTAP volumes group data virtually, determine how data is stored, and determine the type of access to your data. Volumes don't consume file system storage capacity. The data that is stored in a volume primarily consumes SSD storage. Depending on the volume's tiering policy, the data might also consume capacity pool storage. You set a volume's size when you create it, and you can change its size later.

The following protocols might be used for your volumes:

- SMB/CIFS: file storage protocol for Windows operating systems
- NFS: file storage protocol for Unix operating systems
- iSCSI: block storage protocol

S3 endpoints can be attached to an FSx for ONTAP volume. Using an S3 access point, you can access file data residing on SMB/CIFS or NFS volumes via the AWS S3 APIs. This allows you to integrate your existing data with GenAI, ML, and analytics from AWS services that support S3 access points.

Details for volume settings

Immutable files

This feature, also known as SnapLock, is disabled by default. Enabling immutable files prevents data deletion or overwriting for a set period. Enabling this feature is possible only during volume creation. After the feature is enabled, it cannot be disabled. This is a premium feature for FSx for ONTAP that carries an additional charge. For more information, refer to How SnapLock works in Amazon FSx for NetApp ONTAP documentation.

- **Retention modes**: You can select from two retention modes - *Enterprise* or *Compliance*.
  - In *Enterprise* mode, an immutable files, or SnapLock, administrator can delete a file during its retention period.
  - In *Compliance* mode, a WORM file cannot be deleted before its retention period expires. Similarly, the immutable volume cannot be deleted until the retention periods for all files within the volume expire.
- **Retention period**: The retention period has two settings - *retention policy* and *retention periods*. The *retention policy* defines how long to retain files in an immutable WORM state. You can specify your own retention policy or use the default retention policy (unspecified), which is 30 years. The minimum and maximum *retention periods* define the range of time allowed for locking files.

  Even after the retention period expires, you can't modify a WORM file. You can only delete it or set a new retention period to turn on WORM protection again.

- **Autocommit**: You'll have the option to enable the autocommit feature. The autocommit feature commits a file to WORM state on a SnapLock volume if the file did not change for the autocommit period duration. The autocommit feature is disabled by default. You must ensure that the files you want to autocommit reside on a SnapLock volume.

- **Privileged delete**: A SnapLock administrator can turn on privileged delete on a SnapLock Enterprise volume to allow a file to be deleted before the file's retention period expires. This feature is disabled by default.
- **Volume append mode**: You can't modify existing data in a WORM-protected file. However, immutable files allows you to maintain protection for existing data using WORM-appendable files. For example, you can generate log files or preserve audio or video streaming data while writing data to them incrementally. Learn more about volume-append mode in Amazon FSx for NetApp ONTAP documentation.

Before you begin

Review the following prerequisites before you create a volume:

- You must have an FSx for ONTAP file system in the Workload Factory console.
- You must have a storage VM.
- For protocol access, complete the following:
  - To configure access to the volume, you must associate a link. Learn how to associate an existing link or to create and associate a new link. After the link associates, return to this operation.
  - You must configure access for the protocol you select, either SMB/CIFS, NFS, or iSCSI.

Create a volume

You can create a volume using the following tools available in the Codebox: REST API, CloudFormation, and Terraform. Learn how to use Codebox for automation.

When using Terraform from Codebox, the code you copy or download hides `fsxadmin` and `vsadmin` passwords. You'll need to re-enter the passwords when you run the code.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Storage**.
3. From the Storage menu, select **FSx for ONTAP**.
4. From **FSx for ONTAP**, select the actions menu of the file system you want to create a volume in, and select **Create volume**.
5. On the Create volume page under General details, provide the following details:
   a. **Volume name**: Enter a name for the volume.
   b. **Storage VM name**: Optionally, enter a storage VM name.
   c. **Volume style**: Select **FlexVol** or **FlexGroup** volume.

      FlexVol volume style is selected by default.

      FlexGroup volume size depends on the number of constituents, requiring 100 GiB per constituent.

   d. **Volume size**: Enter the volume size and unit.

      Optionally, enable volume autogrow. This option is available when you select **File access** as the volume access type.

   e. **Volume autogrow**: Optionally, enable volume autogrow to automatically expand volume capacity until

the volume reaches the maximum size. This feature accommodates increasing data usage, ensuring uninterrupted operations.

Specify the maximum volume growth size and unit. You cannot set the maximum growth size smaller than the current volume size

f. **Tags**: Optionally, you can add up to 50 tags.

6. Under Access (only for file systems with associated links), provide the following details:

a. **Access type**: Select **File access** or **Block access**. Additional fields to configure volume access differ depending on your selection.

- **File access**: allows multiple authorized users and devices access to the volume using SMB/CIFS, NFS, or dual (SMB/NFS) protocols.

  Complete the following fields to set up file access to the volume.

b. **NFS export policy**: Provide the following details to provide NFS access:

i. **Access control**: Select a **Custom export policy**, **Existing export policy**, or **No access to the volume** from the dropdown menu.

ii. **Export policy name**:

  If you selected a custom export policy, select an existing policy name from the dropdown menu.

  If you selected an existing export policy, enter a new policy name.

iii. **Add Export Policy Rule**: Optionally, for a custom export policy, you can add export policy rules to the policy.

c. **SMB/CIFS share**: Provide the following:

i. **Name**: Enter the SMB/CIFS share name to provide access.

ii. **Permissions**: Select Full control, Read/Write, Read, or No access, and then enter the users or groups separated by a semicolon (;). Users or groups are case sensitive and the user's domain must be included using the format "domain\username".

d. **Security style**: For dual-protocol volumes, select either the UNIX or NTFS security style. UNIX is the default security style for dual-protocol volumes. For detailed guidance on user mapping in this context, refer to the AWS blog article "Enabling multiprotocol workloads with Amazon FSx for NetApp ONTAP".

- **Block access**: allows hosts running critical business applications access to the volume using the iSCSI protocol. Block access is only available when the file system scale-out deployment has six HA pairs or fewer.

  Complete the following fields to set up block access to the volume.

  i. **iSCSI configuration**: Provide the following details to configure iSCSI for block access to the volume.

    A. Select **Create a new initiator group** or **Map an existing initiator group**.

    B. Select the **Host operating system** from the dropdown menu.

    C. Enter an **Initiator group name** for a new initiator group.

    D. Under Host Initiators, add one or more iSCSI qualified name (IQN) host initiators.

e. **S3 access point**: Optionally, attach an S3 access point to access FSx for ONTAP file system data residing on NFS or SMB/CIFS volumes via AWS S3 APIs. Only the file access type is supported.

Providing the following details:

- **S3 access point name**: Enter the name of the S3 access point.
- **User**: Select an existing user with access to the volume or create a new user.
- **User type**: Select **UNIX** or **Windows** as the user type.
- **Network configuration**: Select **Internet** or **Virtual private cloud (VPC)**. The type of network you choose determines whether the access point is accessible from the internet or restricted to a specific VPC.
- **Enable metadata**: Enabling metadata creates an S3 table containing all objects accessible by the S3 access point, which you can use for auditing, governance, automatic, analysis, and optimization. Enabling metadata incurs additional AWS costs. Refer to Amazon S3 pricing documentation for more information.

f. **S3 access point tags**: Optionally, you can add up to 50 tags or remove tags.

7. Under Efficiency and protection, provide the following details:

a. **Storage efficiency**: Enabled by default. Select to disable the feature.

ONTAP achieves storage efficiency using deduplication and compression features. Deduplication eliminates duplicate data blocks. Data compression compresses the data blocks to reduce the amount of physical storage that is required.

b. **Snapshot policy**: Select the snapshot policy to specify the frequency and retention of snapshots.

The following are default policies from AWS. To display existing snapshot policies, you must associate a link.

`default`

This policy automatically creates snapshots on the following schedule, with the oldest snapshot copies deleted to make room for newer copies:

- A maximum of six hourly snapshots taken five minutes past the hour.
- A maximum of two daily snapshots taken Monday through Saturday at 10 minutes after midnight.
- A maximum of two weekly snapshots taken every Sunday at 15 minutes after midnight.

Snapshot times are based on the file system's time zone, which defaults to Coordinated Universal Time (UTC). For information about changing the time zone, refer to Displaying and setting the system time zone in the NetApp Support documentation.

`default-1weekly`

This policy works in the same way as the `default` policy, except that it only retains one snapshot from the weekly schedule.

`none`

This policy doesn't take any snapshots. You can assign this policy to volumes to prevent automatic snapshots from being taken.

c. **Tiering policy**: Select the tiering policy for the data stored in the volume.

Balanced (Auto) is the default tiering policy when creating a volume using the Workload Factory console. For more information about volume tiering policies, refer to Volume storage capacity in AWS FSx for NetApp ONTAP documentation. Note that Workload Factory uses use-case based names in the Workload Factory console for tiering policies and includes FSx for ONTAP tiering policy names in parentheses.

d. **Immutable files**: Enabling the immutable files feature permanently commits files in this volume to an immutable WORM (write-once-read-many) state. Provide the following details:
   i. Select to enable **Immutable files powered by SnapLock**.
   ii. Select the box to agree and proceed.
   iii. Select **Enable**.
   iv. **Retention mode**: Select **Enterprise** or **Compliance** mode.
   v. **Retention period**:
      - Select the retention policy:
        - **Unspecified**: Sets the retention policy to 30 years.
        - **Specify period**: Enter the number of seconds, minutes, hours, days, months, or years to set your own retention policy.
      - Select the minimum and maximum retention periods:
        - **Minimum**: Enter the number of seconds, minutes, hours, days, months, or years to set the minimum retention period.
        - **Maximum**: Enter the number of seconds, minutes, hours, days, months, or years to set the maximum retention period.
   vi. **Autocommit**: Disable or enable autocommit. If you enable autocommit, set the autocommit period.
   vii. **Privileged delete**: Disable or enable. If you enable privileged delete, a SnapLock administrator can delete a file before its retention period expires.
   viii. **Volume append mode**: Disable or enable. Enables you to add new content to WORM files.

e. **ARP/AI**: NetAp Autonomous Ransomware Protection with AI (ARP/AI) is enabled by default when a link is associated with the file system. Learn more about ARP/AI. Accept the statement to proceed.

   If the feature is unavailable, it is because of one of the following reasons:

   - A link is not associated with the file system. Learn how to associate an existing link or to create and associate a new link. After the link associates, return to this operation.
   - Volumes with immutable files, and volumes with iSCSI and NVMe protocols are not supported for ARP/AI.
   - The file system already has an ARP/AI policy.

8. Under Advance configuration, provide the following:
   a. **Junction path**: Enter the location in the storage VM's namespace where the volume gets mounted. The default junction path is `/<volume-name>`.
   b. **Aggregates list**: Only for FlexGroup volumes. Add or remove aggregates. The minimum number of aggregates is one.
   c. **Number of constituents**: Only for FlexGroup volumes. Enter the number of constituents per aggregate. 100 GiB is required per constituent.
9. Select **Create**.

Related information

- Adjust volume capacity in Workload Factory
- Change volume tiering policy in Workload Factory
- Manage S3 access points in Workload Factory

Access your FSx for ONTAP file system data

You can access your FSx for ONTAP file systems from on-premises by mounting volumes for NAS clients and mounting iSCSI LUNs for SAN clients.

Accessing data in Amazon FSx for NetApp ONTAP documentation provides topics about how to access data for your reference.

You can also get the mount point for volumes in NetApp Workload Factory.

Get mount point for volumes in NetApp Workload Factory

Get the mount point for a volume to mount a share on a CIFS share or NFS client.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Storage**.
3. From **FSx for ONTAP**, select the actions menu of the file system with the volume and then select **Manage**.
4. From the file system overview, select the **Volumes** tab.
5. From the Volumes tab, select the actions menu for the volume, then **Basic actions**, and then **View mount command**.
6. In the Mount command dialog, select **Copy** to copy the command for either the NFS mount point or CIFS share. You'll enter the copied command in your terminal.
7. Select **Close**.

Connect to NAS clients

- Mount a volume on Linux clients
- Mount a volume on Windows clients
- Mount a volume on macOS clients

Connect to SAN clients

- Mount an iSCSI LUN on Linux clients
- Mount an iSCSI LUN on Windows clients

Copyright information

Trademark information