# FSx for ONTAP

## User Guide

# FSx for ONTAP: User Guide

# Table of Contents

# What is Amazon FSx for NetApp ONTAP?

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, performant, and feature-rich file storage built on NetApp's popular ONTAP file system. It provides the familiar features, performance, capabilities, and APIs of NetApp file systems with the agility, scalability, and simplicity of a fully managed AWS service.

Amazon FSx for NetApp ONTAP provides feature-rich, fast, and flexible shared file storage that's broadly accessible from Linux, Windows, and macOS compute instances running in AWS or on premises. FSx for ONTAP offers high-performance SSD storage with sub-millisecond latencies, and makes it quick and easy to manage your data by enabling you to snapshot, clone, and replicate your files with the click of a button. It also automatically tiers your data to lower-cost, elastic storage, eliminating the need to provision or manage capacity and allowing you to achieve SSD levels of performance for your workload while only paying for SSD storage for a small fraction of your data. It provides highly available and durable storage with fully managed backups and support for cross-region disaster recovery, and supports popular data security and anti-virus applications that make it even easier to protect and secure your data. For customers who use NetApp ONTAP on-premises, FSx for ONTAP is an ideal solution to migrate, back up, or burst your file-based applications from on-premises to AWS without the need to change your application code or how you manage your data.

As a fully managed service, Amazon FSx for NetApp ONTAP makes it simple to launch and scale reliable, performant, and secure shared file storage in the cloud. With Amazon FSx for NetApp ONTAP, you no longer have to worry about setting up and provisioning file servers and storage volumes, replicating data, installing and patching file server software, detecting and addressing hardware failures, managing failover and failback, and manually performing backups. It also provides rich integration with other AWS services, such as AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS), and AWS CloudTrail.

**Topics**



## Features of FSx for ONTAP

With FSx for ONTAP, you get a fully managed file storage solution with:

- Support for petabyte-scale data sets in a single namespace
- Multiple gigabytes per second (GBps) of throughput per file system
- Multi-protocol access to data using the NFS, SMB, and iSCSI protocols
- High availability and durability with Multi-AZ deployments
- Automatic data tiering that reduces storage costs by automatically transitioning infrequently-accessed data to a lower-cost storage tier based on your access patterns

- Data compression, deduplication, and compaction to reduce your storage consumption
- Support for NetApp's SnapMirror replication feature
- Support for NetApp's on-premises caching solutions: NetApp Global File Cache and FlexCache
- Support for access and management using native AWS or NetApp tools and APIs
  - AWS Management Console, CLI, and SDKs
  - NetApp ONTAP CLI, REST API, and Cloud Manager
- Support for the following data protection and security features:
  - Encryption of file system data and backups at rest using KMS keys
  - Encryption of data in-transit using SMB Kerberos session keys
  - On-demand anti-virus scanning
  - Authentication and authorization using Active Directory
  - File access auditing

# Security and data protection

Amazon FSx provides multiple levels of security and compliance to help ensure that your data is protected. It automatically encrypts data at rest in file systems and backups using keys that you manage in AWS Key Management Service (AWS KMS). You can also encrypt data in transit using Kerberos for NFS and SMB clients. Amazon FSx has been assessed to comply with International Standards Organization (ISO), Payment Card Industry Data Security Standard (PCI DSS), and System and Organization Controls (SOC) certifications, and is Health Insurance Portability and Accountability Act of 1996 (HIPAA) eligible. For more information, see Data protection in Amazon FSx for NetApp ONTAP (p. 77).

Amazon FSx provides access control at the file system level using Amazon Virtual Private Cloud (Amazon VPC) security groups. Amazon FSx provides access control at the API level using AWS Identity and Access Management (IAM) access policies. To provide access control at the file and folder level, Amazon FSx supports Unix permissions, NFS ACLs, and NTFS ACLs. When you join Amazon FSx to an Active Directory (AD), users accessing file systems can authenticate using their Active Directory credentials. Amazon FSx integrates with AWS CloudTrail to monitor and log your Amazon FSx API calls so that you can see actions taken by users on your Amazon FSx resources. For more information, see Logging FSx for ONTAP API Calls with AWS CloudTrail (p. 71).

Additionally, Amazon FSx protects your data with highly durable file system backups. Amazon FSx performs automatic daily backups, and you can take additional backups at any point. For more information, see Protecting your FSx for ONTAP data with backups, snapshots, and scheduled replication (p. 29).

# Pricing for FSx for ONTAP

You are billed for file systems based on the following categories:

- SSD storage capacity (per gigabtye-month, or GB-month)
- SSD IOPS that you provision above 3 IOPS/GB (per IOPS-month)
- Throughput capacity (per MBps-month)
- Capacity pool storage consumption (per GB-month)
- Capacity pool requests (per read and write)
- Backup storage consumption (per GB-month)

For more information about pricing and fees associated with the service, see FSx for ONTAP pricing.

# FSx for ONTAP forums

If you encounter issues while using Amazon FSx, use the FSx for ONTAP discussion forums to get answers.

# Are you a first-time Amazon FSx user?

If you're a first-time user of Amazon FSx, we recommend that you read the following sections in order:

1. If you're new to AWS, see Setting up FSx for ONTAP (p. 10) to set up an AWS account.
2. If you're ready to create your first Amazon FSx file system, follow the instructions in Getting started with Amazon FSx for NetApp ONTAP (p. 12).
3. For information about performance, see Amazon FSx for NetApp ONTAP performance (p. 74).
4. For Amazon FSx security details, see Security in Amazon FSx for NetApp ONTAP (p. 77).
5. For information about the Amazon FSx API, see Amazon FSx API Reference.

# How Amazon FSx for NetApp ONTAP works

This topics describes the major features of FSx for ONTAP and how they work, along with important implementation details.

**Topics**

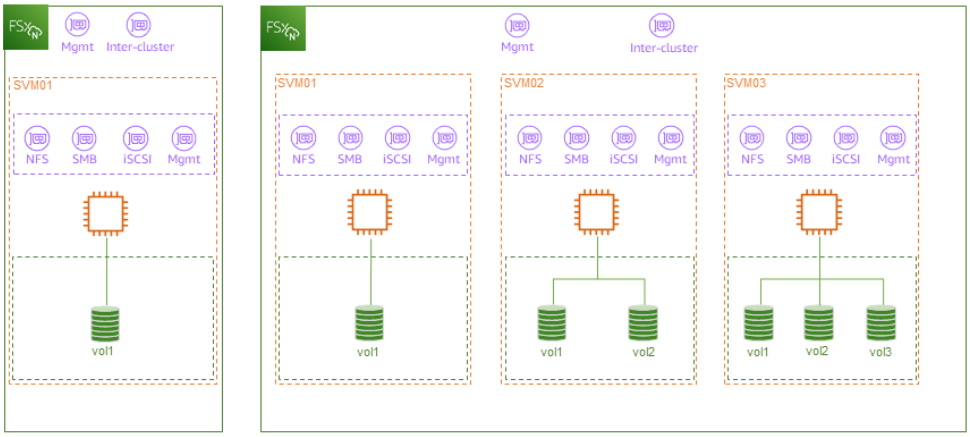


## FSx for ONTAP file systems

An FSx for ONTAP file system is composed of the following primary resources:

- Storage virtual machines (SVMs)
- Volumes

A file system can have one or more SVMs, and an SVM can have one or more volumes. The following image shows the structure of FSx for ONTAP file systems, and the relationship of the three primary resources. The FSx for ONTAP file system on the left is the simplest file system with one SVM and one volume. The file system on the right has multiple SVMs, with some SVMs having multiple volumes. File systems and SVMs each have multiple endpoints for management, with SVMs also having endpoints for data access.




## FSx for ONTAP file systems

A file system is the primary resource in Amazon FSx (analgous to an ONTAP cluster on-premises). You specify the SSD storage capacity and throughput capacity for your file system, and choose an Amazon

Virtual Private Cloud (VPC) in which your file system is created. Each file system has a management endpoint that you can optionally use to manage your data using the ONTAP CLI or ONTAP REST API. Data stored in a file system can be automatically tiered to lower-cost storage if data-tiering is enabled.

You define the following properties when creating an FSx for ONTAP file system:

- Storage capacity – The amount of SSD storage, up to 192 TiB.
- SSD IOPS – By default, each gigabyte of SSD storage includes 3 SSD IOPS. You can optionally provision additional SSD IOPS as needed.
- Throughput capacity – The sustained speed at which the file server can serve data.
- Networking – The VPC, subnets, routes tables, IP address range for the management and data access endpoints your file system creates.
- Encryption – The AWS Key Management Service (KMS) key used to encrypt the file system data at rest.
- Administrative access – You can specify the password for the "fsxadmin" user, which you can use to administer the file system using the NetApp ONTAP CLI and REST API.

For more information, see Managing FSx for ONTAP file systems (p. 37).

## File system endpoints

You can manage FSx for ONTAP file systems using the NetApp ONTAP CLI, REST API, and you can set up SnapMirror relationships between an Amazon FSx file system and another ONTAP deployment (including another Amazon FSx file system). Each Amazon FSx for NetApp ONTAP file system has the following file system endpoints that provide access to NetApp applications:

- **Management** – Use this endpoint to access the ONTAP CLI over SSH, or to use the ONTAP REST API with your file system.
- **Intercluster** – Use this endpoint when setting up replication using NetApp SnapMirror.

For more information, see Managing FSx for ONTAP resources using NetApp applications (p. 55) and Scheduled replication using NetApp SnapMirror (p. 35).

# Storage virtual machines (SVM)

A storage virtual machine (SVM) is an isolated file server with its own administrative credentials and endpoints for administering and accessing data. When you access data on Amazon FSx for NetApp ONTAP, your clients and workstations access the endpoint for the SVM in which the data is stored. Amazon FSx automatically creates a default SVM on your file system for you when you create a file system using the AWS Management Console.

Each SVM is a virtual resource, meaning that the SVMs in your file system share your file system's storage and throughput capacity. Because each SVM is an isolated file server, if you have multiple users or groups who need access to administer data on Amazon FSx, you can create a separate SVM for each user or group so that they can independently administer their data. You can also configure quality of service (QoS) policies within your file system to limit the amount of throughput and IOPS that individual workloads can drive, ensuring that individual workloads don't interfere with the other users and groups on the same file system. You can create additional SVMs on your file system at any time using the AWS Management Console, AWS CLI, or Amazon FSx API and SDKs.

You define the following properties when creating an SVM:

- The file system to which it belongs
- Active Directory configuration – You can optionally join your SVM to a self-managed Microsoft Active Directory for authentication and access control of Windows and Mac clients.

- Root volume security style – Sets the root volume security style (Unix, NTFS, or Mixed) to align with the type of clients you're using to access your data within the SVM.
- The SvmAdminPassword, which is the password for the SVM's `vsadmin` user.

## SVM endpoints

Each SVM has four endpoints that are used to access data or to manage the SVM using the NetApp ONTAP CLI, REST API, listed as follows:

- `Nfs` – for connecting using the NFS protocol
- `Smb` – for connecting using the SMB protocol (if your SVM is joined to an Active Directory)
- `Iscsi` – for connecting using the iSCSI protocol.
- `Management` – for managing SVMs using the NetApp ONTAP CLI, NetApp ONTAP API, or NetApp CloudManager.

For more information, see Managing FSx for ONTAP storage virtual machines (p. 42).

The following table lists the maximum number of SVMs you can create for a file system depending on the amount of throughput capacity provisioned and the protocols used to access volumes.

| Amount of throughput capacity (MB/s) | Maximum number of SVMs per file system |
|---|---|
| 512 | 14 |
| 1024 | 14 |
| 2048 | 24 |

# Volumes

Volumes are isolated data containers in which your files, directories, or iSCSI LUNs are stored. Volumes are thin provisioned, meaning that they only consume storage capacity for the data stored in them. Each volume is created within one of the SVMs in your file system.

You can create volumes using the AWS Management Console, AWS CLI, the Amazon FSx API, or using NetApp Cloud Manager. You can also use your file system's or SVM's administrative endpoint to create, update, and delete volumes using the ONTAP CLI or ONTAP REST API.

When you create a volume, you define the following properties:

- The name of the volume.
- The size of the volume.
- The junction path, which is the location in the SVM's namespace where the volume is mounted.
- You can enable storage efficiency to use compression, deduplication, and compaction to reduce the amount of storage your data consumes.
- Set the volume security style (Unix, NTFS, or Mixed) to match the majority of clients that you expect to be accessing the volume.
- You can enable automatic data tiering and set which tiering policy to use. For more information, see Data tiering (p. 7).

You can create up to 500 volumes per file system. For more information, see Managing FSx for ONTAP volumes (p. 46).

# Data tiering

When you create an Amazon FSx for NetApp ONTAP file system, you provision a level of SSD storage capacity. As you write data to your file system, your less frequently-accessed data is automatically transitioned to the capacity pool tier, a lower-cost storage tier that automatically grows and shrinks with the amount of data tiered to it. As a result, you only need to provision as much SSD storage as needed for the active portion of your data set, with the rest of your data stored in lower-cost capacity pool storage. Amazon FSx automatically and intelligently transitions data between storage tiers based on your access patterns, allowing you to achieve SSD levels of performance for your workload while only paying for SSD storage for a small fraction of your data.

Each volume in your Amazon FSx for NetApp ONTAP file system has a tiering policy associated with it, which determines how the data within that volume is transitioned to and from capacity pool storage. You can choose from one of four tiering policies:

- **Auto** moves cold user data blocks in the active file system and in Snapshot copies to the storage pool tier.

  If read by random reads, the cold data blocks in the capacity tier become hot and move to the primary storage tier. If read by sequential reads, such as those associated with index and antivirus scans, the cold data blocks stay cold and do not move to the primary storage tier.
- **Snapshot-only** moves user data blocks of the volume Snapshot copies that are not associated with the active file system to the storage pool tier.

  If read, cold data blocks on the capacity tier become hot and are moved to the primary storage tier.
- **All** moves moves all user data blocks in the the active file system and in Snapshot copies to the storage pool tier.

  If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier.
- **None** keeps data of a volume in the primary storage tier, preventing it from being moved to the storage pool tier.

For the **Auto** and **Snapshot-only** tiering policies, you can also specify a minimum cooling period, which sets the time that user data in a volume must remain inactive for the data to be considered cold and moved to the capacity pool tier. The minimum cooling period, which applies to both Snapshot and active file system data, ranges from 2 to 183 days. For **Auto** the default cooling period is 31 days, for **Snapshot-only** the default cooling period is 2 days.

When you create a new volume, data tiering is not enabled by default. For information about enabling data tiering on a volume, see Managing FSx for ONTAP volumes (p. 46).

# Using Microsoft Active Directory

You can use your existing Microsoft Active Directory (AD) for user authentication and authorization. To do so, you need to join any SVMs hosting volumes that will be accessed by Windows or macOS SMB clients to your AD. You specify your AD's configuration when you create an SVM. The following are the AD properties you need to set when joining an SVM to your AD:

- NetBiosName – name of the computer object that's created in your Active Directory for your SVM.
- DnsIps – Up to 3 IP addresses for your DNS servers.
- DomainName – The fully qualified domain name of the self-managed AD directory.
- FileSystemAdministratorsGroup – The name of the domain group whose members have administrative privileges on your SVM.

- Credentials – The user name and password for a service account in your self-managed AD domain that Amazon FSx uses to join to your AD domain.

## Keeping your AD configuration updated in Amazon FSx

To help ensure continued, uninterrupted availability of your Amazon FSx file system, update your SVM's self-managed Active Directory (AD) configuration any time that you make changes to your self-managed AD setup.

For example, suppose that your AD uses a time-based password reset policy. In this case, as soon as the password is reset, make sure to update the service account password with Amazon FSx. To do this, use the Amazon FSx console, API, or AWS CLI. Similarly, if the DNS server IP addresses change for your AD domain, as soon as the change occurs update the DNS server IP addresses with Amazon FSx. Again, do this using the Amazon FSx console, API, or CLI.

For more information, see Managing FSx for ONTAP storage virtual machines (p. 42).

# Accessing data stored on Amazon FSx for NetApp ONTAP file systems

You can access the data on your FSx for ONTAP file systems using Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon WorkSpaces, Amazon AppStream 2.0, VMware Cloud on AWS, and on-premises clients.

You can access an ONTAP volume from multiple Linux, Windows, or macOS clients simultaneously over the NFS (v3, v4, v4.1, v4.2) and SMB protocols. You can also use the iSCSI protocol to access iSCSI LUNs. For more information, see Accessing data: supported clients and environments (p. 16).

Amazon FSx for NetApp ONTAP file systems can be accessed from on-premises using AWS VPN or AWS Direct Connect with AWS Transit Gateway (TGW). You can also use TGW or VPC Peering to access clusters from another VPC (including a VPC in another AWS Region). For more information, see Supported access environments (p. 16).

# How to work with Amazon FSx for NetApp ONTAP

There are several ways that you can interact with FSx for ONTAP. You can manage your Amazon FSx for NetApp ONTAP file systems using the following AWS and NetApp management applications and tools:

- AWS management tools:
  - The AWS Management Console
  - The AWS Command Line Interface (AWS CLI)
  - The Amazon FSx APIs and SDKs
- NetApp management tools:
  - NetApp CloudManager
  - The NetApp ONTAP CLI
  - The NetApp ONTAP REST API

# AWS Management Console

The AWS Management Console is a simple web-based user interface. You can manage your Amazon FSx file systems from the console with no programming required. To access the Amazon FSx console, sign in to the AWS Management Console, and then open the Amazon FSx console at https://console.aws.amazon.com/fsx/.

# Amazon FSx command line interface (CLI)

You can use the AWS CLI to access the Amazon FSx API interactively. To install the AWS CLI, see Installing, updating and uninstalling the AWS CLI. To begin using the AWS CLI for Amazon FSx, see AWS Command Line Interface reference for Amazon FSx.

# Amazon FSx application programming interface (API)

If you're a developer, you use the Amazon FSx API actions and data types to programmatically configure and manage Amazon FSx and its resources. You can also use the API in one of the language-specific AWS software development kits (SDKs). For more information, see the Amazon FSx API reference.

For application development, we recommend that you use one of the AWS SDKs. The AWS SDKs handle low-level details such as authentication, retry logic, and error handling, so that you can focus on your application logic. The AWS SDKs are available for a wide variety of languages. For more information, see Tools to Build on AWS.

AWS also provides libraries, sample code, tutorials, and other resources to help you get started more easily. For more information, see the AWS Developer Center.

# NetApp Cloud Manager

NetApp Cloud Manager provides a centralized user interface to manage, monitor, and automate ONTAP deployments in AWS and on premises. For more information, see Managing FSx for ONTAP resources using NetApp applications (p. 55).

# NetApp ONTAP CLI

You can use the NetApp ONTAP CLI to manage your Amazon FSx for NetApp ONTAP file systems. The ONTAP CLI provides a command-based view of the ONTAP management interface. You enter commands at the cluster management endpoint as the `fsxadmin` user, or at the SVM management endpoint as the `vsadmin` user. For more information, see Managing FSx for ONTAP resources using NetApp applications (p. 55).

# NetApp ONTAP REST API

You can use the NetApp ONTAP REST API to manage your Amazon FSx for NetApp ONTAP file systems. You can access the ONTAP REST API using your file system's management endpoint, or using the management endpoint associated with any SVM. For more information, see Managing FSx for ONTAP resources using NetApp applications (p. 55).

# Setting up FSx for ONTAP

Before you use Amazon FSx for the first time, complete the following tasks:

1. Sign up for Amazon Web Services (p. 10)
2. Create an IAM user (p. 10)

**Topics**



## Sign up for Amazon Web Services

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

## Create an IAM user

**To create an administrator user for yourself and add the user to an administrators group (console)**

1. Sign in to the IAM console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   **Note**
   We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.
2. In the navigation pane, choose **Users** and then choose **Add user**.
3. For **User name**, enter **`Administrator`**.
4. Select the check box next to **AWS Management Console access**. Then select **Custom password**, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to **User must create a new password at next sign-in** to allow the new user to reset their password after they sign in.
6. Choose **Next: Permissions**.
7. Under **Set permissions**, choose **Add user to group**.
8. Choose **Create group**.
9. In the **Create group** dialog box, for **Group name** enter **`Administrators`**.

10. Choose **Filter policies**, and then select **AWS managed - job function** to filter the table contents.
11. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.

    **Note**
    You must activate IAM user and role access to Billing before you can use the `AdministratorAccess` permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.
12. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
13. Choose **Next: Tags**.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the *IAM User Guide*.
15. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

# Next step

To get started using FSx for ONTAP see Getting started with Amazon FSx for NetApp ONTAP (p. 12) for instructions to create your Amazon FSx resources.

# Getting started with Amazon FSx for NetApp ONTAP

Learn how to get started using Amazon FSx for NetApp ONTAP. This getting started exercise includes the following steps.

**Topics**



## Step 1: Create an Amazon FSx for NetApp ONTAP file system

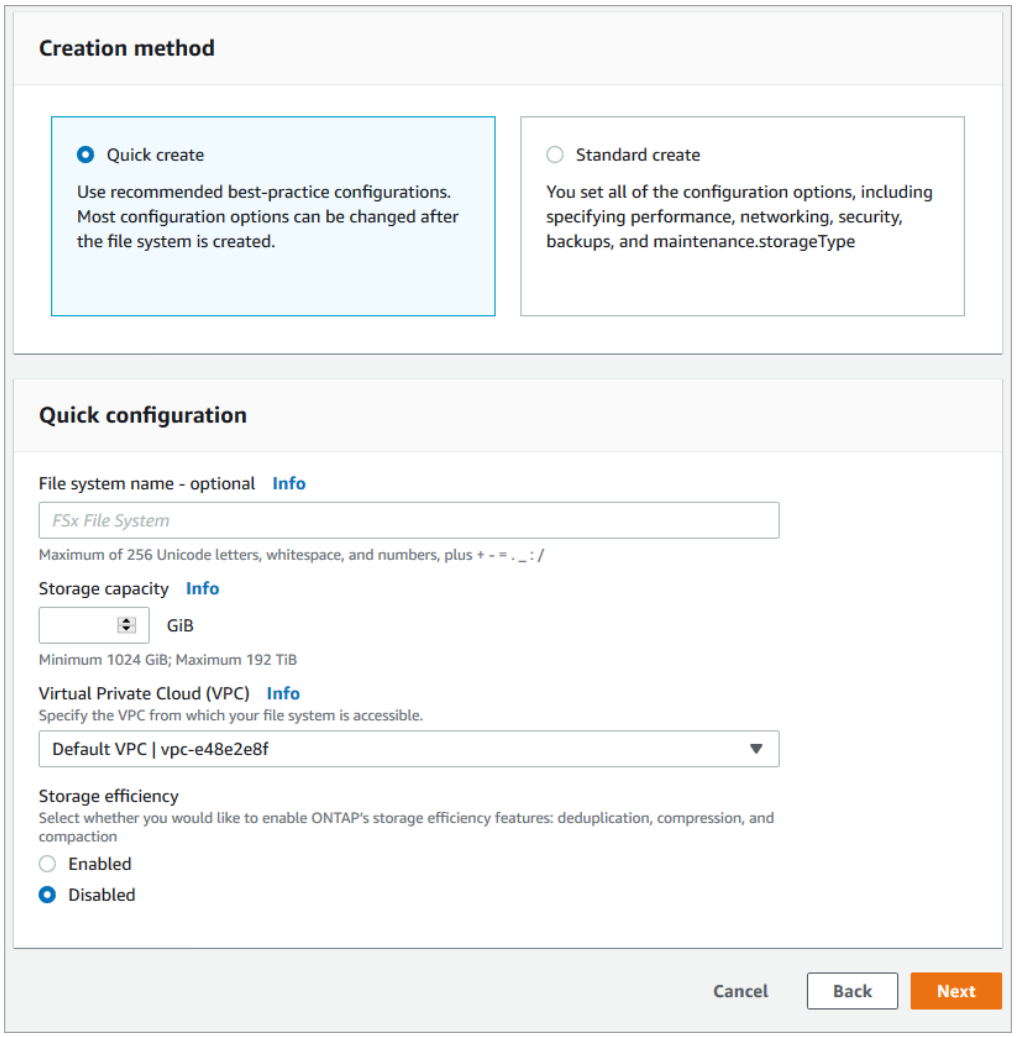
The Amazon FSx console has two options for creating a file system – a **Quick create** option and a **Standard create** option. To rapidly and easily create an Amazon FSx for NetApp ONTAP file system with the service recommended configuration, use the **Quick create** option.

The **Quick create** option creates a file system with a single storage virtual machine (SVM) and one volume. The **Quick create** option configures this file system to allow data access from Linux instances over the Network File System (NFS) protocol. After your file system is created, you can create additional SVMs and volumes as needed, including an SVM joined to an Active Directory to allow access from Windows and macOS clients over the Server Message Block (SMB) protocol.

For information about using the **Standard create** option to create a file system with a customized configuration, see Creating FSx for ONTAP file systems (p. 37).

**To create your file system**

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. On the dashboard, choose **Create file system** to start the file system creation wizard.
3. On the **Select file system type** page, choose **Amazon FSx for NetApp ONTAP**, and then choose **Next**. The **Create ONTAP file system** page appears. For **Creation method**, choose **Quick create**.




4. In the **Quick configuration** section, for **File system name - optional**, enter a name for your file system. It's easier to find and manage your file systems when you name them. You can use a maximum of 256 Unicode letters, white space, and numbers, plus these special characters: **+ -** (hyphen) **= . _** (underscore) **: /**
5. For **SSD storage capacity**, specify the storage capacity of your file system, in gibibytes (GiBs). Enter any whole number in the range of 1,024–196608.
6. For **Virtual Private Cloud (VPC)**, choose the Amazon VPC that you want to associate with your file system.
7. For **Storage efficiency**, choose **Enabled** to turn on the ONTAP storage efficiency features (compression, deduplication, and compaction) or **Disabled** to turn them off.
8. Choose **Next**.
9. Review the file system configuration shown on the **Create ONTAP file system** page. For your reference, note which file system settings you can modify after the file system is created.
10. Choose **Create file system**.

**Quick create** creates a file system with one SVM (named `fsx`) and one volume (named `vol1`). The volume has a junction path of `/vol1` and a capacity pool tiering policy of **Auto** (which will automatically tier any data that hasn't been accessed for 31 days to lower-cost capacity pool storage). The file system data is encrypted at rest using your default service managed AWS KMS key.

# Step 2: Mounting your file system from an Amazon EC2 Linux instance

You can mount your file system from an Amazon Elastic Compute Cloud (Amazon EC2) instance. This procedure uses an instance running Amazon Linux 2.

**To mount your file system from Amazon EC2**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Create or select an Amazon EC2 instance running Amazon Linux 2 that is in the same virtual private cloud (VPC) as your file system. For more information about launching an instance, see Step 1: Launch an instance in the *Amazon EC2 User Guide for Linux Instances*.
3. Connect to your Amazon EC2 Linux instance. For more information, see Connect to your Linux instance in the *Amazon EC2 User Guide for Linux Instances*.
4. Open a terminal on your Amazon EC2 instance using secure shell (SSH), and log in with the appropriate credentials.
5. Make a directory on your Amazon EC2 instance for the volume's mount point with the following command.

```
$ sudo mkdir /fsx
```

6. Mount your Amazon FSx for NetApp ONTAP file system to the directory that you created. Use a `mount` command similar to the following example. In the following example, replace each *`user input placeholder`* with your own information.

```
sudo mount -t nfs nfsvers=4.1,svm-01234567.fs-01234567.fsx.us-east-1.amazonaws.com:/
vol1 /fsx
```

# Step 3: Clean up resources

After you have finished this exercise, you should follow these steps to clean up your resources and protect your AWS account.

**To clean up resources**

1. On the Amazon EC2 console, terminate your instance. For more information, see Terminate Your Instance in the *Amazon EC2 User Guide for Linux Instances*.
2. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
3. On the Amazon FSx console, delete all of your FSx for ONTAP volumes that are not root volumes of your SVM. For more information, see Deleting a volume (p. 50).
4. Delete all of your FSx for ONTAP SVMs. For more information, see Deleting a storage virtual machine (p. 45).
5. On the Amazon FSx console, delete your file system. When you delete a file system, all automatic backups are deleted automatically. However, you still must delete any manually created backups. The following steps outline this process.

    a. From the console dashboard, choose the name of the file system that you created for this exercise.

    b. For **Actions**, choose **Delete file system**.

c. In the **Delete file system** dialog box, enter the ID of the file system that you want to delete in the **File system ID** box.
d. Choose **Delete file system**.
e. The file system is now being deleted, and its status in the dashboard changes to **DELETING**. When the file system has been deleted, it no longer appears in the dashboard. Any automatic backups are deleted along with the file system.
f. Now you can delete any manually created backups for your file system. From the left-side navigation, choose **Backups**.
g. From the dashboard, choose any backups that have the same **File system ID** as the file system that you deleted, and choose **Delete backup**. Be sure to retain the final backup, if you created one.
h. The **Delete backups** dialog box opens. Keep the check box selected for the IDs of the backups that you want to delete, and then choose **Delete backups**.

Your Amazon FSx file system and any related automatic backups are now deleted, along with any manual backups that you chose to delete as well.

# Accessing data: supported clients and environments

You can access your Amazon FSx file systems using a variety of supported clients and methods in both the AWS Cloud and on premises environments.

**Topics**



## Supported clients

FSx for ONTAP file systems support accessing data from a wide variety of compute instances and operating systems. It does this by supporting access using the Network File System (NFS) protocol, (v3, v4.0, and v4.1), Server Message Block (SMB) protocol, and the Internet Small Computer Systems Interface (iSCSI) protocol.

The following AWS compute instances are supported for use with FSx for ONTAP:

- Amazon Elastic Compute Cloud (Amazon EC2) instances running Amazon Linux, Amazon Linux 2, Microsoft Windows, and MacOS; for more information, see Mounting FSx for ONTAP volumes (p. 18)
- Amazon Elastic Container Service (Amazon ECS) Docker containers on Amazon EC2 Windows and Linux instances; for more information, see Mounting FSx for ONTAP from Amazon Elastic Container Service (p. 24)
- Amazon Elastic Kubernetes Service – To learn more, see Amazon FSx for NetApp ONTAP CSI driver in the Amazon EKS User Guide
- Amazon WorkSpaces instances.
- Amazon AppStream 2.0 instances.
- Virtual machines (VMs) running in VMware Cloud on AWS environments

Once mounted, FSx for ONTAP file systems appear as a local directory or drive letter over NFS and SMB, providing fully managed, shared network file storage that can be simultaneously accessed by up to thousands of clients. iSCSI LUNS are accessible as block devices when mounted over iSCSI.

## Supported access environments

Following, you can find information about how to access your FSx for ONTAP file systems.

Amazon VPC enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. For more information, see What is Amazon VPC in the *Amazon Virtual Private Cloud User Guide*.

**Topics**

# Accessing Amazon FSx for NetApp ONTAP file systems from within the same VPC and AWS account

When you create your Amazon FSx for NetApp ONTAP file system, you select the Amazon VPC in which it is located. All SVM's and volumes associated with the Amazon FSx for NetApp ONTAP file system are also located in the same VPC. When the file system and the client mounting the storage virtual machine (SVM) volume are located in the same VPC and AWS account, you can mount a volume using the SVM's DNS name and volume junction or SMB share, depending on the client. For more information, see Mounting FSx for ONTAP volumes (p. 18).

You can achieve better performance and avoid data transfer charges between Availability Zones by accessing an SVM volume using a client that is located in the same Availability Zone as the file system's preferred subnet. To identify a file system's preferred subnet, in the Amazon FSx console, choose **File systems**, then choose the ONTAP file system whose volume you are mounting, and the preferred subnet is displayed in the **Preferred subnet** panel.

## VPC peering

FSx for ONTAP supports the use of Transit Gateway, AWS Direct Connect or AWS VPN to access your file systems from peered networks over NFS and SMB.

A VPC peering connection is a networking connection between two VPCs. This type of connection enables you to route traffic between them using private Internet Protocol version 4 (IPv4) addresses. You can use VPC peering to connect VPCs within the same AWS Region or between different AWS Regions. For more information on VPC peering, see What is VPC peering? in the *Amazon VPC Peering Guide*.

Using AWS Direct Connect, you can access your file system over a dedicated network connection from your on premises environment. Using AWS VPN, you can access your file system from your on premises environment over a secure and private tunnel. For more information about AWS Direct Connect, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*. For more information on setting up AWS VPN connections, see VPN connections in the *Amazon VPC User Guide*.

# Access from peered networks

This section describes how to access Amazon FSx for NetApp ONTAP file systems from peered networks.

## Access NFS, SMB, or the ONTAP CLI and REST API from peered networks

The endpoints used for accesing Amazon FSx for NetApp ONTAP over NFS or SMB, or for administering file systems using the ONTAP CLI or REST API, are floating IP addresses that are created in the VPC route tables you associate with your file system. These IP addresses are within an `EndpointIpAddressRange` that you can specify when creating a file system. By default, Amazon FSx chooses an IP address range for you from within the 198.19.0.0/16 IP address range.

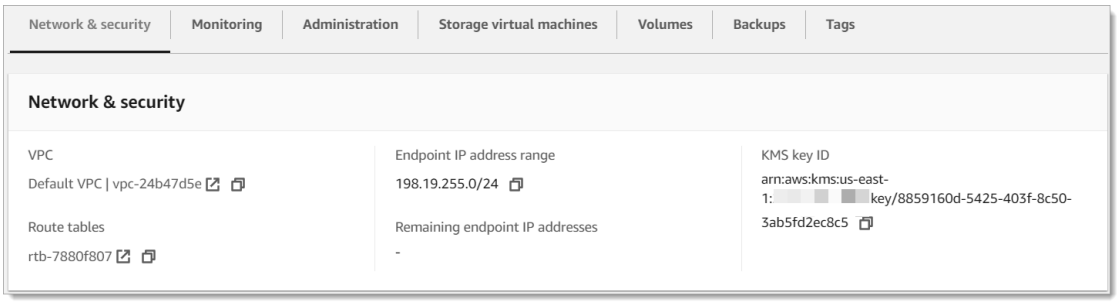
To access these floating IP address endpoints from a peered network, you need to configure your peered network to route traffic destined to your file system's `EndpointIpAddressRange` to the VPC in which your file system is created. Alternatively, if you are using NetApp Global File Cache or NetApp FlexCache for remote office caching, both of these technologies communicate with your FSx for ONTAP file system using your file system's inter-cluster endpoint, which is not a floating IP address. As a result, you don't

need to configure Transit Gateway if all of your clients are accessing Amazon FSx using one of these caching technologies.

For example, to configure routing using AWS Transit Gateway, use the following procedure.

**To configure routing using AWS Transit Gateway**

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. Choose the FSx for ONTAP file system for which you are configuring access from a peered network.
3. In **Network & security>** copy the **Endpoint IP address range**.




4. Add a route to Transit Gateway that routes traffic destined for this IP address range to your file system's VPC. For more information, see Working with transit gateways in the *Amazon VPC Transit Gateways*.
5. Confirm that you can access your FSx for ONTAP file system from the peered network.

**Note**
DNS records for the management, NFS, and SMB endpoints are only resolvable from within the same VPC as the file system. In order to mount a volume or connect to a management port from another network, you need to use the endpoint's IP address. Theese IP addresses do not change over time.

## Access over iSCSI from peered networks

AWS Transit Gateway isn't required when accessing data over iSCSI. You can use VPC peering, Transit Gateway, AWS Direct Connect, AWS VPN to access the iSCSI port using it's IP address. You do not need to configure any additional routing.

# Mounting FSx for ONTAP volumes

You access the data in FSx for ONTAP by mounting a volume on your client. The commands in this section use the DNS name or the IP address of the SVM in which the volume is created to mount or attach a volume. You can find the SVM's DNS name and IP address in the Amazon FSx console by choosing **ONTAP > Storage virtual machines**, or on the **Storage virtual machine** tab in the **File system details** page for the file system. Or, you can find them in the response of the DescribeStorageVirtualMachines API operation.

**Topics**

# Mounting ONTAP volumes to Linux clients

We recommend that SVM volumes to which you are attaching Linux clients have a security style setting of `UNIX` or `mixed`. For more information, see Managing FSx for ONTAP volumes (p. 46).

**To mount an ONTAP volume on a Linux client**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Create or select an Amazon EC2 instance running Amazon Linux 2 that is in the same VPC as the file system.

   For more information on launching an EC2 Linux instance, see Step 1: Launch an instance in the *Amazon EC2 User Guide for Linux Instances*.
3. Connect to your Amazon EC2 Linux instance. For more information, see Connect to your Linux instance in the *Amazon EC2 User Guide for Linux Instances*.
4. Open a terminal on your EC2 instance using secure shell (SSH), and log in with the appropriate credentials.
5. Create a directory on the EC2 instance for mounting the SVM volume as follows:

   ```
   sudo mkdir /fsx
   ```
6. Mount the volume using the following command.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   The following example uses sample values.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   You can also use the SVM's IP address SVM instead of its DNS name.

   ```
   sudo mount -t nfs 198.51.100.1:/vol1 /fsx
   ```

# Using /etc/fstab to mount automatically on instance reboot

To automatically remount your FSx for ONTAP volume when an Amazon EC2 Linux instance reboots, use the `/etc/fstab` file. The `/etc/fstab` file contains information about file systems. The command `mount -a`, which runs during instance start-up, mounts the file systems listed in `/etc/fstab`.

**Note**
FSx for ONTAP file systems do not support automatic mounting using `/etc/fstab` on Amazon EC2 Mac instances.

**Note**
Before you can update the `/etc/fstab` file of your EC2 instance, make sure that you already created your FSx for ONTAP file system. For more information, see Creating FSx for ONTAP file systems (p. 37).

**To update the /etc/fstab file on your EC2 instance**

1. Connect to your EC2 instance:

   - To connect to your instance from a computer running macOS or Linux, specify the .pem file for your SSH command. To do this, use the `-i` option and the path to your private key.

- To connect to your instance from a computer running Windows, you can use either MindTerm or PuTTY. To use PuTTY, install it and convert the .pem file to a .ppk file.

For more information, see the following topics in the *Amazon EC2 User Guide for Linux Instances*:

- Connecting to your Linux instance using SSH
- Connecting to your Linux instance from Windows using PuTTY

2. Create a local directory that will be used to mount the SVM volume.

```
sudo mkdir /fsx
```

3. Open the `/etc/fstab` file in an editor of your choice.
4. Add the following line to the `/etc/fstab` file. Insert a tab character between each parameter. It should appear as one line with no line breaks.

```
svm-dns-name:volume-junction-path /fsx nfs nfsver=version defaults 0 0
```

You can also use the IP address of volume's SVM. The last three parameters indicate NFS options (which we set to default), dumping of file system and filesystem check (these are typically not used so we set them to 0).

5. Save the changes to the file.
6. Now mount the file share using the following command. The next time the system starts, the folder will be mounted automatically.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

Your EC2 instance is now configured to mount the ONTAP volume whenever it restarts.

# Attaching ONTAP volumes to Microsoft Windows clients

This section describes how to access data in your FSx for ONTAP file system with clients running the Microsoft Windows operating system. Review the following requirements, regardless of the type of client you are using.

This procedure assumes that the client and the file system are located in the same VPC and AWS account. If the client is located on-premise, or in a different VPC, AWS account or AWS Region, you've set up AWS Transit Gateway or a dedicated network connection using AWS Direct Connect or a private, secure tunnel using AWS Virtual Private Network. For more information, see Access from peered networks (p. 17).

We recommend that you attach volumes to your Windows clients using the SMB protocol.

## Prerequisites

To access an ONTAP storage volume using a Microsoft Windows client, you have to satisfy the following prerequisites:

- The SVM of the volume you are attaching must be joined to your organization's Active Directory. For more information, see Managing FSx for ONTAP storage virtual machines (p. 42).
- The volume you are attaching has a security style setting of `NTFS` or `mixed`. For more information, see Managing FSx for ONTAP volumes (p. 46).

**To attach an ONTAP volume on a Windows client using SMB**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Create or select an Amazon EC2 instance running Microsoft Windows that is in the same VPC as the file system, and joined to the same Microsoft Active Directory as the volume's SVM.

   For more information on launching an instance, see Step 1: Launch an instance in the *Amazon EC2 User Guide for Windows Instances*.

   For more information about joining an SVM to an Active Directory, see Managing FSx for ONTAP storage virtual machines (p. 42).
3. Connect to your Amazon EC2 Windows instance. For more information, see Connecting to your Windows instance in the *Amazon EC2 User Guide for Windows Instances*.
4. Open a command prompt.
5. Run the following command. Replace the following:

   - Replace `Z:` with any available drive letter.
   - Replace `DNS_NAME` with the DNS name or the IP address of the SMB endpoint for the volume's SVM.
   - `C$` is the default SMB share at the root of the SVM's namespace. If you've created any SMB shares in your SVM, you can provide the SMB share name to mount instead of `C$`. For more information about creating SMB shares, see Creating SMB shares (p. 51).

   ```
   net use Z: \\DNS_NAME\C$
   ```

   The following example uses sample values.

   ```
   net use Z: \\corp.example.com:\new_share
   ```

   You can also use the IP address of the SVM instead of its DNS name.

   ```
   net use Z: \\198.51.100.5:\new_share
   ```

# Attaching ONTAP volumes to an EC2 Mac instance using SMB

This section describes how to access data in your FSx for ONTAP file system with clients running the macOS operating system. Review the following requirements, regardless of the type of client you are using.

This procedure assumes that the client and the file system are located in the same VPC and AWS account. If the client is located on-premise, or in a different VPC, AWS account or AWS Region, you've set up AWS Transit Gateway or a dedicated network connection using AWS Direct Connect or a private, secure tunnel using AWS Virtual Private Network. For more information, see Access from peered networks (p. 17).

We recommend that you attach volumes to your Mac clients using the SMB protocol.

**To mount an ONTAP volume on a Mac client using SMB**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Create or select an Amazon EC2 Mac instance running the macOS that is in the same VPC as the file system.

For more information on launching an instance, see Step 1: Launch an instance in the *Amazon EC2 User Guide for Linux Instances*.

3. Connect to your Amazon EC2 Mac instance. For more information, see Connect to your Linux instance in the *Amazon EC2 User Guide for Linux Instances*.
4. Open a terminal on your EC2 instance using secure shell (SSH), and log in with the appropriate credentials.
5. Create a directory on the EC2 instance for mounting the volume as follows:

```
sudo mkdir /fsx
```

6. Mount the volume using the following command.

```
sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
```

The following example uses sample values.

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
east-1.amazonaws.com:/C$ /fsx
```

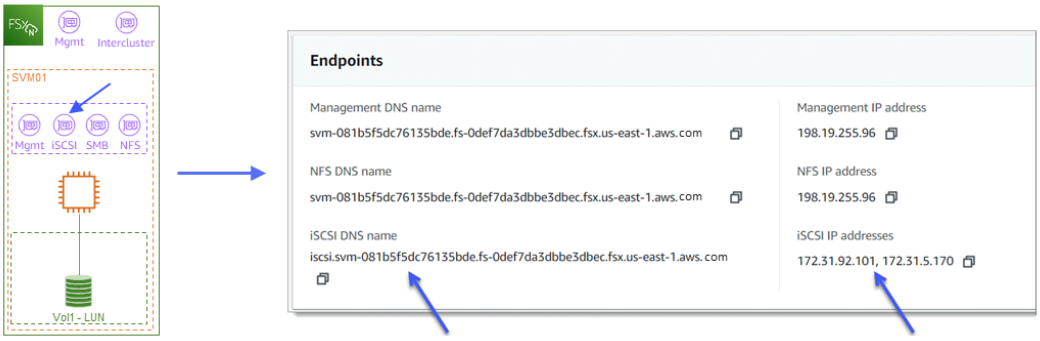
You can also use the SVM's IP address instead of its DNS name.

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

`C$` is the default SMB share that you can mount to see the root of the SVM's namespace. If you've created any Server Message Block (SMB) shares in your SVM, provide the SMB share names instead of `C$`. For more information about creating SMB shares, see Creating SMB shares (p. 51).

# Attaching ONTAP volumes using iSCSI

You can use FSx for ONTAP for your iSCSI block storage needs. iSCSI clients connect to LUNs using the SVM's iSCSI endpoint. Before attempting to use the procedures described in the following sections, you need to use the NetApp ONTAP CLI to set up an iSCSI LUN. For more information about setting up and managing LUNs using the NetApp ONTAP CLI, see Setting up and managing LUNs for FC and iSCSI in the *NetApp ONTAP 9 Documentation Center*.



# Attach an Amazon FSx for NetApp ONTAP iSCSI LUN on a Linux client

This procedure describes how to attach an FSx for ONTAP LUN on a Linux client. To use this procedure, you must have first set up an iSCSI LUN on your FSx for ONTAP file system as described in Setting up and managing LUNs for FC and iSCSI in the *NetApp ONTAP 9 Documentation Center*.

**Note**
Make sure the security group for your EC2 Linux instance allows the iSCSI protocol.

### To attach an iSCSI LUN on a Linux client

1. Log on to your Linux client.
2. To access the NetApp ONTAP CLI, establish an SSH session on the management port of the FSx for ONTAP file system where the LUN is located, for more information, see Managing file systems with the NetApp ONTAP CLI (p. 55). You can also connect to the management port of the SVM where the LUN is located, for more information, see Managing SVMs using the NetApp ONTAP 9.9.1 CLI (p. 56).
3. Discover the LUNs that exist in the file system or SVM, depending on which endpoint you have established the SSH connection.

```
FSxId0123456789abcdef8::> lun show
Vserver     Path                State    Mapped   Type    Size
---------   ---------------     -------  ------   -----   ------
svm01       /vol/vol1/MyLunName  online   unmapped linux     4GB
```

4. Create a new initiator group (igroup). Use igroups to control which hosts have access to specific LUNs. When you bind an igroup to a portset, a host in the igroup can access the LUNs only by connecting to the target ports in the portset. For more information, see lun igroup create in the NetApp ONTAP 9.9.1 CLI command reference. Use the following command:

```
FSxId0123456789abcdef8::> igroup create -igroup MyIG -ostype linux -protocol iscsi -
vserver svm01 -initiator iqn.initiator.for.your.client
```

5. Map the LUN to the igroup you just created using the following command.

```
FSxId0123456789abcdef8::> lun map -vserver svm01 -volume vol1 -lun MyLunName -
igroup MyIG
```

6. Verify the mapping:

```
FSxId0123456789abcdef8::> lun mapping show
```

7. Retrieve the iscsi data interface IP address on the SVM.

```
FSxId0123456789abcdef8::> network interface show -role data
Vserver    Logical                 Status      Network             Current
   Current   Is
             Interface               Admin/Oper  Address/Mask        Node
    Port      Home
---------   ---------------         ----------- -----------------   ------------------
    --------- ------
svm01
             iscsi_1                 up/up       172.31.20.161/20
 FsxId0123456789abcdef1 01e0e     true
             iscsi_2                 up/up       172.31.41.87/20
 FsxId0123456789abcdef1 02e0e     true
```

```
            nfs-smb-management_1    up/up       198.19.255.95/20
 FsxId0123456789abcdef1 01e0e     true
3 entries were displayed.
FSxId0123456789abcdef8::>
```

8. On your Linux client, discover the target:

```
[ec2-user@ip-172.31.22.200 ~]$ sudo iscsiadm -m discovery -t sendtargets -p
 172.31.20.161
172.31.20.161:3260,1030 iqn.1992-08.com.hetapp:sn.e0eac84906ba11ecabd7112118508572:vs.3
172.31.41.87:3260,1029 iqn.1992-08.com.hetapp:sn.e0eac84906ba11ecabd7112118508572:vs.3
```

9. Log in to the target:

```
[ec2-user@ip-172.31.22.200 ~]$ sudo iscsiadm -m node -
T iqn.initiator.for.your.client:vs.3 --login
Logging in to [iface: default, target: iqn.initiator.for.your.client, portal:
 172.31.20.161:3260] (multiple)
Logging in to [iface: default, target: iqn.initiator.for.your.client, portal:
 172.31.41.87:3260] (multiple)
Login to [iface: default, target: iqn.initiator.for.your.client, portal:
 172.31.20.161:3260] successful
Login to [iface: default, target: iqn.initiator.for.your.client, portal:
 172.31.41.87:3260] successful
```

10. Discover the block devices:

```
[ec2-user@ip-172.31.22.200 ~]$ lsblk
NAME            MAJ:MIN  RM  SIZE  RO  TYPE  MOUNTPOINT
sda                8:0     0    4G   0  disk
sdb                8:16    0    4G   0  disk
nvme0n1          259:0     0    8G   0  disk
\_nvme0n1p1      259:1     0    8G   0  port /
 \_nvme0n1p128   259:2     0    1M   0  port
```

11. Create a host partition using the following commands.

```
[ec2-user@ip-172.31.22.200 ~]$ sudo fdisk /dev/sdb options n,p,#number, w device-
partition
[ec2-user@ip-172.31.22.200 ~]$ lsblk
```

12. Create your file system and mount it:

```
[ec2-user@ip-172.31.22.200 ~]$ sudo mkfs.ext4 /dev/sdb1
[ec2-user@ip-172.31.22.200 ~]$ mkdir iscsi
[ec2-user@ip-172.31.22.200 ~]$ sudo mount -t ext4 /dev/sdb1 isci
```

# Mounting FSx for ONTAP from Amazon Elastic Container Service

You can access your Amazon FSx for NetApp ONTAP file systems from an Amazon Elastic Container Service (Amazon ECS) Docker container on an Amazon EC2 Linux or Windows instance.

## Mounting on an Amazon ECS Linux container

1. Create an ECS cluster using the EC2 Linux + Networking cluster template for your Linux containers. For more information, see Creating a cluster in the *Amazon Elastic Container Service Developer Guide*.

2. Create a directory on the EC2 instance for mounting the SVM volume as follows:

```
sudo mkdir /fsxontap
```

3. Mount your FSx for ONTAP volume on the Linux EC2 instance by either using a user-data script during instance launch, or by running the following commands:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Mount the volume using the following command:

```
sudo mount -t nfs nfsvers=NFS_version svm-dns-name:/volume-junction-path /fsxontap
```

The following example uses sample values.

```
sudo mount -t nfs nfsvers=4.1 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsxontap
```

You can also use the SVM's IP address SVM instead of it's DNS name.

```
sudo mount -t nfs nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. When creating your Amazon ECS task definitions, add the following `volumes` and `mountPoints` container properties in the JSON container definition. Replace the `sourcePath` with the mount point and directory in your FSx for ONTAP file system.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

## Mounting on an Amazon ECS Windows container

1. Create an ECS cluster using the EC2 Windows + Networking cluster template for your Windows containers. For more information, see Creating a cluster in the *Amazon Elastic Container Service Developer Guide*.
2. Add a domain-joined Windows EC2 instance to the ECS Windows cluster and map an SMB share.

   Launch an ECS optimized Windows EC2 instance that is joined to your Active Directory domain and initialize the ECS agent by running the following command. You can also pass the information in a script to the user-data text field.

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
</powershell>
```

3. Create an SMB global mapping on the EC2 instance so that you can map your SMB share to a drive. Replace the values below netbios or DNS name for your FSx file system and share name. The NFS volume vol1 that was mounted on the Linux EC2 instance is configured as a CIFS share fsxontap on the FSx file system.

```
vserver cifs share show -vserver svm08 -share-name fsxontap

                                     Vserver: svm08
                                       Share: fsxontap
                    CIFS Server NetBIOS Name: FSXONTAPDEMO
                                        Path: /vol1
                              Share Properties: oplocks
                                                browsable
                                                changenotify
                                                show-previous-versions
                           Symlink Properties: symlinks
                     File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                                Share Comment: -
                                    Share ACL: Everyone / Full Control
            File Attribute Cache Lifetime: -
                                  Volume Name: vol1
                                Offline Files: manual
            Vscan File-Operations Profile: standard
          Maximum Tree Connections on Share: 4294967295
                 UNIX Group for File Create: -
```

4. Create the SMB global mapping on the EC2 instance using the following command:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. When creating your Amazon ECS task definitions, add the following `volumes` and `mountPoints` container properties in the JSON container definition. Replace the `sourcePath` with the mount point and directory in your FSx for ONTAP file system.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

# Availability and durability

Amazon FSx for NetApp ONTAP file systems are highly available and durable across AWS Availability Zones, and are designed to provide continuous availability to data even in the event that an Availability Zone is unavailable. Each file system is powered by two file servers in separate Availability Zones, each with its own storage. Amazon FSx automatically replicates your data across Availability Zones to protect it from component failure, continuously monitors for hardware failures, and automatically replaces infrastructure components in the event of a failure. File systems automatically fail over and back as needed (typically within 60 seconds), and clients automatically fail over and back with the file system.

Amazon FSx for NetApp ONTAP also offers a native backups feature, designed to support archival, data retention, and compliance needs. A backup is a secondary, offline copy of a volume in your file system. Amazon FSx backups are crash-consistent and are also incremental, which means that only the changes after your most recent backup are saved, thus saving on backup storage costs by not duplicating data. By default, Amazon FSx takes an automatic backup of your volumes each day during a backup window that you specify. You can create additional backups at any time using the AWS Management Console, AWS Command Line Interface, or Amazon FSx API.

## Failover process for FSx for ONTAP

File systems automatically fail over from the preferred file server to the standby file server if any of the following conditions occur:

- The preferred file server undergoes planned maintenance.
- The preferred file server becomes unavailable.
- An Availability Zone outage occurs.

When failing over from one file server to another, the new active file server automatically begins serving all file system read and write requests. When the resources in the preferred subnet are available, Amazon FSx automatically fails back to the preferred file server in the preferred subnet. A failover typically completes in less than 60 seconds from the detection of the failure on the active file server to the promotion of the standby file server to active status. Failback to the original Multi-AZ configuration also completes in less than 60 seconds, and only occurs once the file server in the preferred subnet is fully recovered.

When failing over from one file server to another, the new active file server automatically begins serving all file system read and write requests. After the resources in the preferred subnet are available, Amazon FSx automatically fails back to the preferred file server in the preferred subnet. Because the endpoint IP address that clients use to access data over NFS or SMB remains the same, failovers are transparent to Linux, Windows, and macOS applications, which resume file system operations without manual intervention.

## Working with file systems

### Subnets

When you create a VPC, it spans all the Availability Zones (AZs) in the Region. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. After

creating a VPC, you can add one or more subnets in each Availability Zone. The default VPC has a subnet in each Availability Zone. Each subnet must reside entirely within one Availability Zone and cannot span zones.

When you create a Multi-AZ file system, you specify two subnets, one for the preferred file server, and one for the standby file server. The two subnets you choose must be in different Availability Zones within the same AWS Region.

For in-AWS applications, we recommend that you launch your clients in the same Availability Zone as your preferred file server to reduce cross-AZ data transfer costs and minimize latency.

# File system elastic network interfaces

When you create an Amazon FSx file system, Amazon FSx provisions an elastic network interface (ENI) in each of the subnets that you associate with your file system. The network interface allows your client to communicate with the FSx for ONTAP file system. The network interfaces are considered to be within the service scope of Amazon FSx, despite being part of your account's VPC.

> **Warning**
> You must not modify or delete the elastic network interfaces associated with your file system. Modifying or deleting the network interface can cause a permanent loss of connection between your VPC and your file system.

Following is a summary of the subnet, elastic network interface, and IP address resources for FSx for ONTAP file systems:

- Number of subnets: 2
- Number of elastic network interfaces: 2
- Number of IP addresses per ENI: 1 + the number of SVMs in the file system

> **Important**
> Amazon FSx doesn't support accessing file systems from, or exposing file system to the public Internet. If an Elastic IP address, which is a public IP address reachable from the Internet, gets attached to a file system's elastic network interface, Amazon FSx automatically detaches it.

# Protecting your FSx for ONTAP data with backups, snapshots, and scheduled replication

Beyond automatically replicating your file system's data across multiple Availability Zones to ensure high durability, Amazon FSx provides you with the following options to further protect the data stored on your file systems:

- Built-in Amazon FSx backups support your backup retention and compliance needs within Amazon FSx.
- Snapshots enable your users to easily undo file changes and compare file versions by restoring files to previous versions.
- You can schedule automatic replication of your Amazon FSx file system to a second file system to provide data protection and recovery.

**Topics**



## Working with backups

With FSx for ONTAP, you can take automatic daily backups and user-initiated backups of the volumes on your file system. Amazon FSx backups are per volume; that is, each backup contains only the data in a particular volume. Amazon FSx backups are highly durable and incremental.

Amazon FSx backups are incremental, whether they are generated using the automatic daily backup or the user-initiated backup feature. This means that only the data on the volume that has changed after your most recent backup is saved. This minimizes the time required to create the backup and saves on storage costs by not duplicating data. When you delete a backup, only the data unique to that backup is removed. Each Amazon FSx backup contains all of the information that is needed to create a new volume from the backup, effectively restoring a point-in-time snapshot of the file system volume.

Creating regular backups for your volumes is a best practice that helps support your backup retention and compliance needs. Working with Amazon FSx backups is easy, whether it's creating backups, restoring from a backup, or deleting a backup.

**Topics**

# Working with automatic daily backups

By default, Amazon FSx takes an automatic daily backup of your file system's volumes. These automatic daily backups occur during the daily backup window that was established when you created the file system. At some point during the daily backup window, storage I/O might be suspended briefly while the backup process initializes (typically for less than a few seconds). When you choose your daily backup window, we recommend that you choose a convenient time of the day. This time ideally is outside of the normal operating hours for the applications that use your volumes.

Automatic daily backups are kept for a certain period of time, known as a retention period. The default retention period for automatic daily backups is 7 days. You can set the retention period to be between 1–90 days.

> **Note**
> While automatic daily backups have a maximum retention period of 90 days, user-initiated backups are kept forever, unless you delete them. For more information about user-initiated backups, see Working with user-initiated backups (p. 30)..

Automatic daily backups are deleted when the volume is deleted. If you set the retention period to 0, automatic backups will be disabled.

Both the daily backup window and retention period are system-level settings that apply to all the volumes on your file system. You can use the Amazon FSx console, AWS CLI, or one of the AWS SDKs to change the backup window and backup retention period for your file systems. Use the `UpdateFileSystem` API operation or the `update-file-system` CLI command.

# Working with user-initiated backups

With Amazon FSx, you can manually take backups of your file system's volumes at any time. You can do so using the Amazon FSx console, API, or the AWS Command Line Interface (AWS CLI). Your user-initiated backups never expire, and they are available for as long as you want to keep them. User-initiated backups are retained even after you delete the volume or the file system the backups were taken on. You can delete user-initiated backups only by using the Amazon FSx console, API, or CLI. They are never automatically deleted by Amazon FSx. For more information, see Deleting backups (p. 31).

## Creating user-initiated backups

The following procedure guides you through how to create a user-initiated backup in the Amazon FSx console for a volume of an existing file system.

**To create a user-initiated backup of a volume**

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. Navigate to **File systems** and choose the ONTAP file system that you want to back up a volume for.
3. Choose the **Volumes** tab.
4. Choose the volume you want to back up.
5. From **Actions**, choose **Create backup**.
6. In the **Create backup** dialog box that opens, provide a name for your backup. Backup names can be a maximum of 256 Unicode characters, including letters, white space, numbers, and the special characters . + - = _ : /
7. Choose **Create backup**.

You have now created a backup of one of your file system's volumes. You can find a table of all your backups in the Amazon FSx console by choosing **Backups** in the left side navigation. You can search for the name you gave your backup, and the table filters to only show matching results.

When you create a user-initiated backup as this procedure described, it has the type `USER_INITIATED`, and it has the `CREATING` status until it is fully available.

# Restoring backups

You can use an available backup to create a new volume, effectively restoring a point-in-time snapshot of a volume. You can restore a backup using the console, AWS CLI, or one of the AWS SDKs. Restoring a backup to a file system takes the same amount of time as creating a new volume. The data restored from the backup must be downloaded to your file system before the volume can be brought online.

The following procedure guides you through how to restore a backup using the console to create a new volume.

**To restore a volume from a backup**

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. From the console dashboard, choose **Backups** from the left side navigation.
3. Choose the backup that you want to restore from the **Backups** table, and then choose **Restore backup**.

   Doing so opens the volume creation wizard. This wizard is identical to the standard volume creation wizard, except that the file system ID is already filled in.
4. Provide configuration information for the volume. For more information, see To create a volume (console) (p. 47).
5. Review the settings, and then choose **Confirm**.

You have restored from a backup, and a volume is now being created. When its status changes to `CREATED`, you can use the volume as normal.

# Deleting backups

Deleting a backup is a permanent, unrecoverable action. Any data in a deleted backup is also deleted. Do not delete a backup unless you're sure you won't need that backup again in the future.

**To delete a backup**

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. From the console dashboard, choose **Backups** from the left side navigation.
3. Choose the backup that you want to delete from the **Backups** table, and then choose **Delete backup**.
4. In the **Delete backups** dialog box that opens, confirm that the ID of the backup identifies the backup that you want to delete.
5. Confirm that the check box is checked for the backup that you want to delete.
6. Choose **Delete backups**.

Your backup and all included data are now permanently and unrecoverably deleted.

# Setting up a custom backup schedule

Amazon FSx for NetApp ONTAP automatically takes a backup of your volumes once a day during a daily backup window that you can specify. Amazon FSx enforces a retention period that you specify for these automatic backups. It also supports user-initiated backups, so you can take backups of your volumes at any time.

Following, you can find the resources and configuration to deploy custom backup scheduling. Custom backup scheduling performs user-initiated backups of your Amazon FSx volumes on a custom schedule that you define. Examples might be once every six hours, once every week, and so on. This script also configures deleting backups older than your specified retention period.

The solution automatically deploys all the components needed, and takes in the following parameters:

- A volume ID
- A CRON schedule pattern for performing backups
- The backup retention period (in days)
- The backup name tags

For more information on CRON schedule patterns, see Schedule Expressions for Rules in the *Amazon CloudWatch Events User Guide*.

## Architecture overview

This solution does the following:

1. The AWS CloudFormation template deploys an CloudWatch Event, a Lambda function, an Amazon SNS queue, and an IAM role. The IAM role gives the Lambda function permission to invoke the Amazon FSx API operations.
2. The CloudWatch event runs on a schedule you define as a CRON pattern, during the initial deployment. This event invokes the solution's backup manager Lambda function that invokes the Amazon FSx `CreateBackup` API operation to initiate a backup.
3. The backup manager retrieves a list of existing user-initiated backups for the specified volume using `DescribeBackups`. It then deletes backups older than the retention period, which you specify during the initial deployment.
4. The backup manager sends a notification message to the Amazon SNS queue on a successful backup if you choose the option to be notified during the initial deployment. A notification is always sent in the event of a failure.

## AWS CloudFormation template

This solution uses AWS CloudFormation to automate the deployment of the Amazon FSx custom backup scheduling solution. To use this solution, download the fsx-ontap-scheduled-backup.template AWS CloudFormation template.

## Automated deployment

The following procedure configures and deploys this custom backup scheduling solution. It takes about five minutes to deploy. Before you start, you must have the ID of a volume on an Amazon FSx file system running in an Amazon Virtual Private Cloud (Amazon VPC) in your AWS account. For more information on creating these resources, see Creating a volume (p. 47).

> **Note**
> Implementing this solution incurs billing for the associated AWS services. For more information, see the pricing details pages for those services.

**To launch the custom backup solution stack**

1. Download the fsx-ontap-scheduled-backup.template AWS CloudFormation template. For more information on creating an AWS CloudFormation stack, see Creating a stack on the AWS CloudFormation console in the *AWS CloudFormation User Guide*.

**Note**
By default, this template launches in the US East (N. Virginia) AWS Region. Amazon FSx is currently only available in specific AWS Regions. You must launch this solution in an AWS Region where Amazon FSx is available. For more information, see Amazon FSx endpoints and quotas in the *AWS General Reference.*

2. For **Parameters**, review the parameters for the template and modify them for the needs of your file system volumes. This solution uses the following default values.

| Parameter | Default | Description |
|---|---|---|
| FSx for NetApp ONTAP Filesystem Volume ID | No default value | The volume ID for the volume that you want to back up. |
| CRON schedule pattern for backups | 0 0/6 * * ? * | The schedule to run the CloudWatch event, triggering a new backup and deleting old backups outside of the retention period. |
| Backup retention (days) | 7 | The number of days to keep user-initiated backups. The Lambda function deletes user-initiated backups older than this number of days. |
| Name for backups | User-scheduled backup | The name for these backups, which appears in the **Backup Name** column of the Amazon FSx Management Console. |
| Backup Notification | Yes | Choose whether to be notified when backups are successfully initiated. A notification is always sent if there's an error. |
| Email address | No default value | The email address to subscribe to the SNS notifications. |

3. Choose **Next**.
4. For **Options**, choose **Next**.
5. For **Review**, review and confirm the settings. You must select the check box acknowledging that the template create IAM resources.
6. Choose **Create** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should see a status of **CREATE_COMPLETE** in about five minutes.

## Additional options

You can use the Lambda function created by this solution to perform custom scheduled backups of more than one FSx for ONTAP volume. The volume ID is passed to the Amazon FSx function in the input JSON for the CloudWatch event. The default JSON passed to the Lambda function is as follows, where the values for `VolumeId` and `SuccessNotification` are passed from the parameters specified when launching the AWS CloudFormation stack.

```
{
```

```
 "start-backup": "true",
 "purge-backups": "true",
 "volume-id": "${VolumeId}",
 "notify_on_success": "${SuccessNotification}"
}
```

To schedule backups for an additional FSx for ONTAP volume, create another CloudWatch event rule. You do so using the Schedule event source, with the Lambda function created by this solution as the target. Choose **Constant (JSON text)** under **Configure Input**. For the JSON input, simply substitute the volume ID of the FSx for ONTAP volume to back up in place of `${VolumeId}`. Also, substitute either `Yes` or `No` in place of `${SuccessNotification}` in the JSON above.

Any additional CloudWatch Event rules you create manually aren't part of the AWS CloudFormation stack for the Amazon FSx custom scheduled backup solution. Thus, they aren't removed if you delete the stack.

# Working with snapshots

A *snapshot* is a read-only image of an Amazon FSx for NetApp ONTAP volume at a point in time. Snapshots offer protection against accidental deletion or modification of files in your volumes. With snapshots, your users can easily view and restore individual files or folders from an earlier snapshot. Doing this enables users to easily undo changes and compare file versions.

Because snapshots are stored alongside your file system's data, they consume the file system's storage capacity. However, snapshots consume storage capacity only for the changed portions of files since the last snapshot. Snapshots stored in your file system are not included in backups of your file system volumes.

Snapshots are enabled by default on your volumes, using the default snapshot policy. Snapshots are stored in the `.snapshot` directory at the root of a volume.

**Topics**



## Snapshot policies

By default, every volume is associated with the file system's `default` snapshot policy. The snapshot policy defines how the system creates snapshots for a volume. The policy specifies when to create snapshots, how many copies to retain, and how to name them.

The `default` 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.

You can store up to 1023 snapshots per file system at any point in time. When you reach this limit, the next snapshot copy replaces the oldest snapshot copy.

## Restoring individual files and folders

Using the snapshots on your Amazon FSx file system, your users can quickly restore previous versions of individual files or folders. Doing this enables them to recover deleted or changed files stored on the

shared file system. They do this in a self-service manner directly on their desktop without administrator assistance. This self-service approach increases productivity and reduces administrative workload.

Linux and macOS clients can view snapshots in the `.snapshot` directory at the root of a volume. Windows clients can view snapshots in the `Previous Versions` tab of Windows Explorer (when right-clicking on a file or folder).

### To restore a file from a snapshot (Linux and macOS clients)

1. If the original file still exists and you do not want it overwritten by the file in a snapshot, then use your Linux or macOS client to rename the original file or move it to a different directory.
2. In the `.snapshot` directory, locate the snapshot that contains the version of the file that you want to restore.
3. Copy the file from the `.snapshot` directory to the directory in which the file originally existed.

### To restore a file from a snapshot (Windows clients)

Users on Windows clients can restore files to previous versions using the familiar Windows File Explorer interface.

1. To restore a file, users choose the file to restore, then choose **Restore previous versions** from the context (right-click) menu.
2. Users can then view and restore a previous version from the **Previous Versions** list.

Data in snapshots is read-only. If you want to make modifications to files and folders listed in the the **Previous Versions** tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

# Scheduled replication using NetApp SnapMirror

You can use NetApp SnapMirror to schedule periodic replication of your FSx for ONTAP file system to or from a second file system. This capability is available for both in-Region and cross-Region deployments.

NetApp SnapMirror replicates data at high speeds, so you get high data availability and fast data replication across ONTAP systems, whether you're replicating between two Amazon FSx file systems in AWS, or from on-premises to AWS. Replication can be scheduled as frequently as every 1 minute, although intervals should be carefully chosen based on RPOs (Recovery Point Objectives), RTOs (Recovery Time Objectives), and performance considerations.

When you replicate data to NetApp storage systems and continually update the secondary data, your data is kept current and remains available whenever you need it. No external replication servers are required. For more information about using NetApp SnapMirror to replicate your data, see Learn about the Replication service in the *NetApp Cloud Manager documentation*.

You can use NetApp Cloud Manager or the NetApp ONTAP CLI to schedule replication for your file system.

## Using NetApp Cloud Manager to schedule replication

You can use Cloud Manager to set up replication with SnapMirror on your FSx for ONTAP file system. For more information, see Replicating data between systems in the *NetApp Cloud Manager documentation*.

# Using the NetApp ONTAP CLI to schedule replication

You can use the NetApp ONTAP CLI to configure scheduled volume replication. For information, see Managing SnapMirror volume replication.

# Administering file systems

Administering FSx for ONTAP file systems includes the following tasks:

- Creating, listing, updating, and deleting file systems, storage virtual machines (SVMs), and volumes
- Managing tags, file system backups, access, and network accessibility for the mount targets of existing file systems

You can perform these file system management tasks using the AWS Management Console, or programmatically using the AWS Command Line Interface (AWS CLI) or API, as discussed in the following sections.

**Topics**



# Managing FSx for ONTAP file systems

A *file system* is the primary FSx for ONTAP resource, analogous to a NetApp ONTAP cluster. You create a file system in a particular virtual private cloud (VPC), and specify the file system's primary storage capacity and throughput capacity at creation. If you enable data-tiering, data stored in a file system can be transferred to lower-cost storage.

## Creating FSx for ONTAP file systems

By default, when you create a new file system from the AWS Management Console, Amazon FSx automatically creates a file system with a single storage virtual machine (SVM) and one volume, allowing for quick access to data from Linux instances over the Network File System (NFS) protocol. When creating the file system, you can optionally join the SVM to an Active Directory to enable access from Windows and macOS clients over the Server Message Block (SMB) protocol. After your file system is created, you can create additional SVMs and volumes as needed.

You can create an FSx for ONTAP file system using the Amazon FSx console, AWS CLI, or the Amazon FSx API.

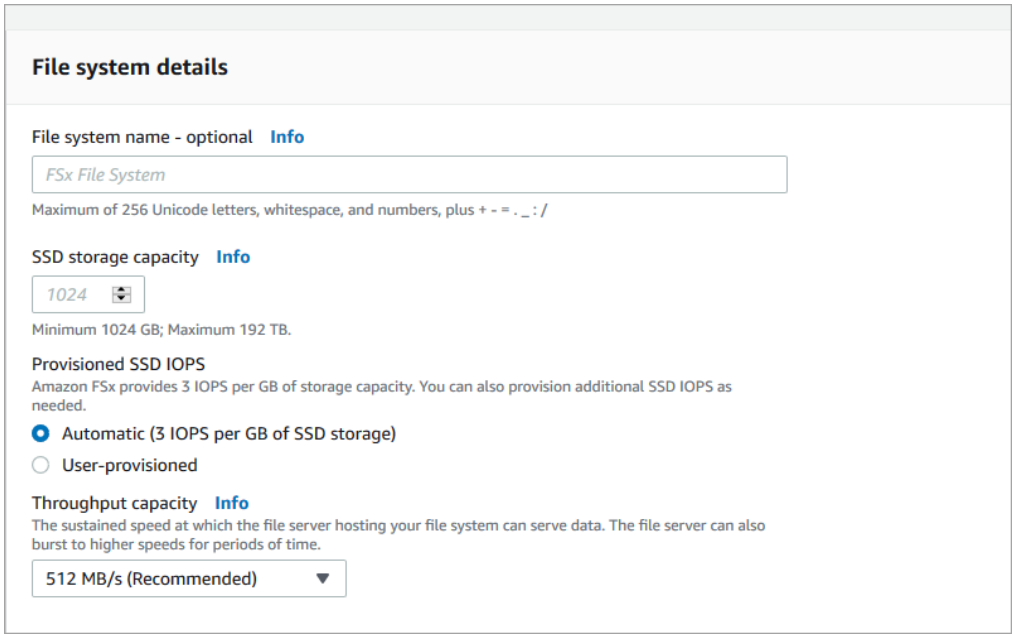
### To create a file system (console)

This procedure uses the **Standard create** creation option to create an FSx for ONTAP file system with a configuration that you customize for your needs. For information about using the **Quick create** creation option to rapidly create a file system with a default set of configuration parameters, see Step 1: Create an Amazon FSx for NetApp ONTAP file system (p. 12).

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.

2. On the dashboard, choose **Create file system** to start the file system creation wizard.
3. On the **Select file system type** page, choose **Amazon FSx for NetApp ONTAP**, and then choose **Next**. The **Create file system** page appears.
4. For **Creation method**, choose **Standard create**.

   Begin your configuration with the **File system details** section.




5. For **File system name - optional**, enter a name for your file system. It's easier to find and manage your file systems when you name them. You can use a maximum of 256 Unicode letters, white space, and numbers, plus these special characters: + - = . _ : /
6. For **SSD storage capacity**, enter the storage capacity of your file system, in GB. Enter any whole number in the range of 1024–196608.
7. For **Provisioned SSD IOPS**, you have two options to provision the number of IOPS for your file system:

   - Choose **Automatic** (the default) if you want Amazon FSx to automatically provision 3 IOPS per GB of SSD storage.
   - Choose **User-provisioned** if you want to specify the number of IOPS. You can provision a maximum of 80,000 SSD IOPS per file system.
8. For **Throughput capacity**, choose a value that is your desired throughput capacity in MB per second (MBps). **Throughput capacity** is the sustained speed at which the file server that hosts your file system can serve data. The **Recommended** value is based on the amount of storage capacity that you chose. For more information, see Amazon FSx for NetApp ONTAP performance (p. 74).
9. In the **Networking** section, for **Virtual Private Cloud (VPC)**, choose the VPC that you want to associate with your file system.
10. Each file system has a primary file server and a standby file server, each in a separate AWS Availability Zone and subnet. For the primary file server, choose a **Preferred subnet** value. For the standby file server, choose a **Standby subnet** value.
11. For **VPC route tables**, specify the VPC route tables in which your file system's endpoints will be created. You should select all VPC route tables associated with the subnets in which your clients are located. By default, Amazon FSx selects your VPC's default route table.
12. **Endpoint IP address range** specifies the IP address range in which the endpoints to access your file system will be created. You have two options to create the IP address range:

- If you want Amazon FSx to choose an unused IP address range for you from the 198.19.0.0/16 range, choose **No preference**.
- If you want to provide the address range, choose **Select an IP address range**.

  **Note**
  Do not choose the following ranges, as they are incompatible with FSx for ONTAP:
  - 0.0.0.0/8
  - 127.0.0.0/8
  - 198.19.0.0/20
  - 224.0.0.0/4
  - 240.0.0.0/4
  - 255.255.255.255/32

13. In the **Security & encryption** section, for **Encryption key**, choose the AWS Key Management Service (AWS KMS) encryption key that protects your file system's data at rest.
14. For **File system administrative password**, enter a secure password for the `fsxadmin` user. Confirm the password.

    You can use the `fsxadmin` user to administer your file system using the ONTAP CLI and REST API. For more information about the `fsxadmin` user, see Managing file systems with the NetApp ONTAP CLI (p. 55).
15. In the **Default storage virtual machine configuration** section, provide the following information:

    - In the **Storage virtual machine name** field, provide a name for the storage virtual machine. You can use a maximum of 47 alphanumeric characters, plus the underscore (_) special character.
    - For **SVM administrative password**, you can optionally choose **Specify a password** and provide a password for the SVM's `vsadmin` user. You can use the `vsadmin` user to administer the SVM using the ONTAP CLI or REST API. For more information about the `vsadmin` user, see Managing SVMs using the NetApp ONTAP 9.9.1 CLI (p. 56).

      If you choose **Don't specify a password** (the default), you can still use the file system's `fsxadmin` user to manage your file system using the ONTAP CLI or REST API, but you can't use your SVM's `vsadmin` user to do the same.
    - In the **Active Directory** section, you can join an Active Directory to the SVM. Joining an Active Directory provides user authentication and access control for Windows and macOS clients accessing the file system.

      If you don't want to join your SVM to an Active Directory, choose **Do not join an Active Directory**.

      If you want to join your SVM to a self-managed Active Directory domain, choose **Join an Active Directory**, and provide the following details for your Active Directory:
      - The NetBIOS name of the Active Directory computer object to create for your SVM. The NetBIOS name cannot exceed 15 characters.
      - The fully qualified domain name of your Active Directory. The domain name cannot exceed 255 characters.
      - **DNS server IP addresses** – The IPv4 addresses of the Domain Name System (DNS) servers for your domain.
      - **Service account username** – The user name of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
      - **Service account password** – The password for the service account.
      - **Confirm password** – The password for the service account.
      - (Optional) **Organizational Unit (OU)** – The distinguished path name of the organizational unit to which you want to join your file system.

- (Optional) **Delegated file system administrators group** – The name of the group in your Active Directory that can administer your file system. The default group is `Domain Admins`.

16. In **Backup and maintenance - *optional***, you can set the following options:
    - For **Daily automatic backup**, choose **Enabled** for automatic daily backups. This option is enabled by default.
    - For **Daily automatic backup window**, set the time of the day in Coordinated Universal Time (UTC) that you want the daily automatic backup window to start. The window is 30 minutes starting from this specified time. This window can't overlap with the weekly maintenance backup window.
    - For **Automatic backup retention period**, set a period from 1–90 days that you want to retain automatic backups.
    - For **Weekly maintenance window**, you can set the time of the week that you want the maintenance window to start. Day 1 is Monday, 2 is Tuesday, and so on. The window is 30 minutes starting from this specified time. This window can't overlap with the daily automatic backup window.
17. For **Tags - *optional***, you can enter a key and value to add tags to your file system. A tag is a case-sensitive key-value pair that helps you manage, filter, and search for your file system.

    Choose **Next**.
18. Review the file system configuration shown on the **Create file system** page. For your reference, note which file system settings you can modify after the file system is created.
19. Choose **Create file system**.

## To create a file system (CLI)

- To create an FSx for ONTAP file system, use the create-file-system CLI command (or the equivalent CreateFileSystem API operation), as shown in the following example.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \
    --subnet-ids subnet-id1,subnet-id2 \
    --ontap-configuration
 DeploymentType=MULTI_AZ_HA_1,ThroughputCapacity=512,PreferredSubnetId=subnet-id1
```

**Note**
If you use the `EndpointIpAddressRange` parameter, don't specify any of the following ranges, as they are incompatible with FSx for ONTAP:

- 0.0.0.0/8
- 127.0.0.0/8
- 198.19.0.0/20
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

After successfully creating the file system, Amazon FSx returns the file system's description in JSON format.

**Note**
Unlike the console file creation procedure, the `create-file-system` CLI command and the `CreateFileSystem` API operation don't create an SVM and a volume. To create an SVM, see Creating a storage virtual machine (p. 42); to create a volume, see Creating a volume (p. 47).

# Updating a file system

You can update the configuration of an FSx for ONTAP file system using the Amazon FSx console, the AWS CLI, and the Amazon FSx API.

## To update a file system (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **File systems**, and then choose the ONTAP file system that you want to update.
3. Choose a tab for the setting you want to update. For example:
   - To change the weekly maintenance window or the ONTAP administrative password for the `fsxadmin` user, choose the **Administration** tab.
   - To update the daily automatic backup window and the automatic backup retention period, choose the **Backups** tab.
4. Choose **Update** next to a setting and provide the new information in the dialog box.

## To update a file system (CLI)

- To update the configuration of an FSx for ONTAP file system, use the update-file-system CLI command (or the equivalent UpdateFileSystem API operation), as shown in the following example.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,FSxAdminPassword=new-fsx-admin-password
```

# Deleting a file system

You can delete an FSx for ONTAP file system using the Amazon FSx console, the AWS CLI, and the Amazon FSx API and SDKs.

**To delete a file system:**

- **Using the console** – Follow the procedure described in Step 3: Clean up resources (p. 14).
- **Using the CLI or API** – First delete all the volumes and SVMs on your file system. Then use the delete-file-system CLI command or the DeleteFileSystem API operation.

# Viewing your file system

You can view the details of your FSx for ONTAP file system using the Amazon FSx console, the AWS CLI, and the Amazon FSx API and SDKs.

**To view a file system:**

- **Using the console** – Choose a file system to view the **File systems** detail page. The **Summary** panel shows the file system's ID, lifecycle status, deployment type, SSD storage capacity, throughput capacity, provisioned IOPS, Availability Zones, and creation time.

  The tabs provide detailed information and configuration functions for the file system's features, such as backups, SVMs, and volumes.
- **Using the CLI or API** – Use the describe-file-systems CLI command or the DescribeFileSystems API operation.

# Managing FSx for ONTAP storage virtual machines

You can create one or multiple *storage virtual machines* (SVMs) on each FSx for ONTAP file system. Each SVM is a virtual, isolated file server with its own administrative credentials and IP address for accessing data.

Every storage virtual machine has a *root volume* (`/`) that resides at the top level of the namespace hierarchy and contains junction paths (also known as mount points) for the volumes that you create in your SVM. We recommend that you not store user data in the root volume, but you can create additional volumes within your storage virtual machine at any time.

You can optionally join your storage virtual machines to your organization's Active Directory during the SVM's creation. Joining an SVM to your Active Directory enables your users to use their existing AD-based identities to authenticate and access FSx for ONTAP over the Network File System (NFS) or Server Message Block (SMB) protocol.

## Creating a storage virtual machine

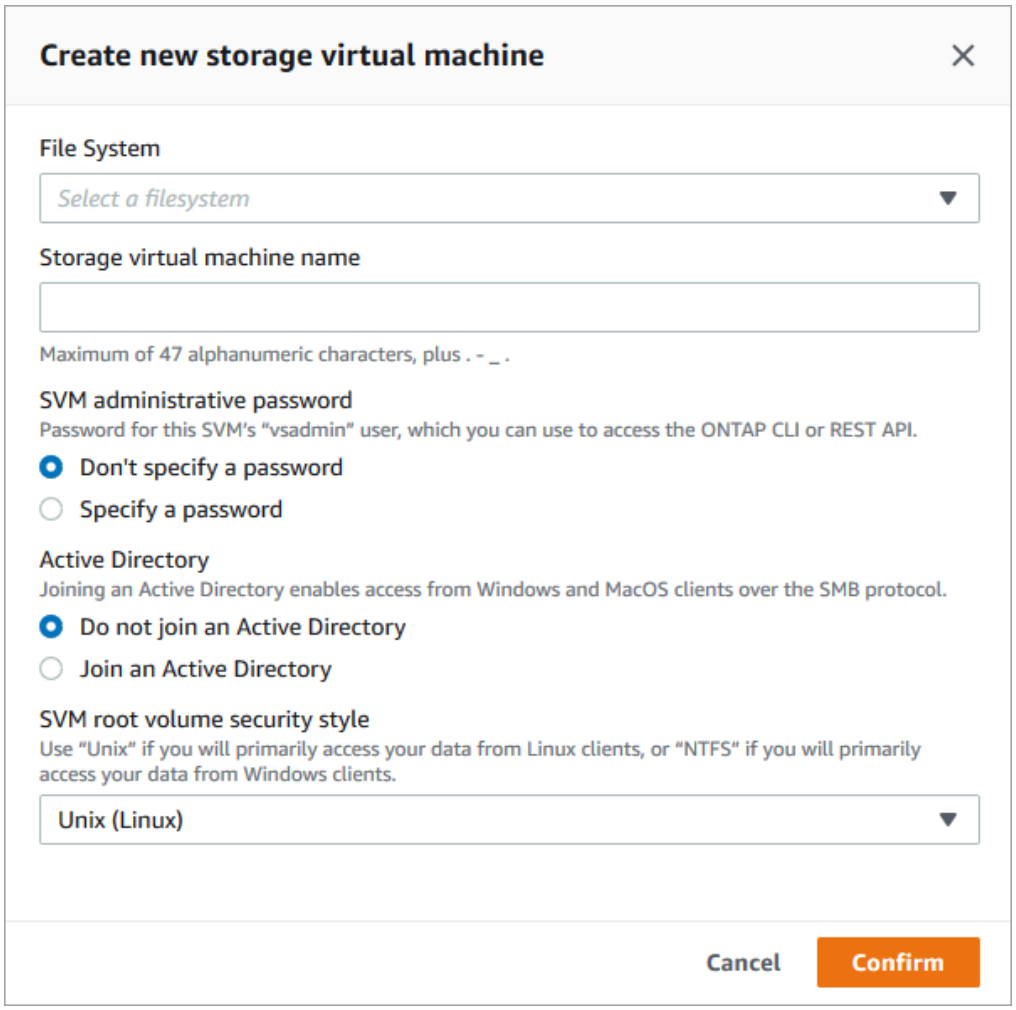
You can create an FSx for ONTAP SVM using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, as well as the NetApp ONTAP command-line interface (CLI) and REST API.

The maximum number of SVMs you can create for a file system depends on the amount of throughput capacity provisioned. For more information, see Storage virtual machines (SVM) (p. 5).

### To create a storage virtual machine (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **Storage virtual machines**.
3. Choose **Create new storage virtual machine**.

   The **Create new storage virtual machine** dialog box appears.




4. For **File system**, choose the file system to create the storage virtual machine on.
5. In the **Storage virtual machine name** field, provide a name for the storage virtual machine. You can use a maximum of 47 alphanumeric characters, plus the underscore (_) special character.
6. For **SVM administrative password**, you can optionally choose **Specify a password** and provide a password for this SVM's `vsadmin` user. You can use the `vsadmin` user to administer the SVM using the ONTAP CLI or REST API. For more information about the `vsadmin` user, see Managing SVMs using the NetApp ONTAP 9.9.1 CLI (p. 56).

   If you choose **Don't specify a password** (the default), you can still use the file system's `fsxadmin` user to manage your file system using the ONTAP CLI or REST API, but you can't use your SVM's `vsadmin` user to do the same.
7. For **Active Directory**, you have the following options:

   - If you don't want to join your file system to an Active Directory, choose **Do not join an Active Directory**.
   - If you want to join your file system to a self-managed Active Directory domain, choose **Join an Active Directory**, and provide the following details for your Active Directory:
     - The NetBIOS name of the Active Directory computer object to create for your SVM. The NetBIOS name cannot exceed 15 characters.
     - The fully qualified domain name of your Active Directory. The domain name cannot exceed 255 characters.

- **DNS server IP addresses** – The IPv4 addresses of the Domain Name System (DNS) servers for your domain.
- **Service account username** – The user name of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
- **Service account password** – The password for the service account.
- **Confirm password** – The password for the service account.
- (Optional) **Organizational Unit (OU)** – The distinguished path name of the organizational unit to which you want to join your file system.
- (Optional) **Delegated file system administrators group** – The name of the group in your Active Directory that can administer your file system. The default group is `Domain Admins`.

8. For **SVM root volume security style**, choose the security style for the SVM depending on the type of clients that will access your data. Choose **Unix (Linux)** if you will primarily access your data using Linux clients; choose **NTFS** if you will primarily access your data using Windows clients.
9. Choose **Confirm** to create the storage virtual machine.

You can monitor the update progress on the **File systems** detail page, in the **Status** column of the **Storage virtual machines** pane. The storage virtual machine is ready for use when its status is **Created**.

### To create a storage virtual machine (CLI)

- To create an FSx for ONTAP storage virtual machine (SVM), use the create-storage-virtual-machine CLI command (or the equivalent CreateStorageVirtualMachine API operation), as shown in the following example.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name vol1 \
    --svm-admin-password password \
    --ontap-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdministra
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

After successfully creating the storage virtual machine, Amazon FSx returns its description in JSON format.

# Updating a storage virtual machine

You can update the configuration of an FSx for ONTAP storage virtual machine using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, in addition to the NetApp ONTAP command line interface (CLI) and REST API.

### To update a storage virtual machine (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **File systems**, and then choose the ONTAP file system that you want to update a storage virtual machine for.
3. Choose the **Storage virtual machines** tab.
4. Choose the storage virtual machine that you want to update.
5. For **Actions**, choose **Update storage virtual machine**.

6. For **SVM administrative password**, you can choose **Specify a password** and provide a new password for this SVM's `vsadmin` user. You can use the `vsadmin` user to administer your SVM using the ONTAP CLI or REST API.

   If you choose **Don't specify a password** (the default), you can still use the file system's `fsxadmin` user to manage your file system using the ONTAP CLI or REST API, but you can't use your SVM's `vsadmin` user to do the same.
7. For **Active Directory**, you can update the following properties of your Active Directory configuration:
   - **DNS server IP addresses** – The IPv4 addresses of the Domain Name System (DNS) servers for your domain.
   - **Service account username** – The user name of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
   - **Service account password** – The password for the service account.
8. Choose **Confirm** to update the storage virtual machine.

### To update a storage virtual machine (CLI)

- To update the configuration of an FSx for ONTAP volume, use the update-storage-virtual-machine CLI command (or the equivalent UpdateStorageVirtualMachine API operation), as shown in the following example.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-5ab87160b8e4ad90d \
    --svm-admin-password new-svm-password \
    --ontap-configuration SelfManagedActiveDirectoryConfiguration='{UserName="new-user-
name", \
      Password="new-password", DnsIps=["10.0.1.28"]}'
```

# Deleting a storage virtual machine

You can delete an FSx for ONTAP storage virtual machine (SVM) using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, in addition to the NetApp ONTAP command line interface (CLI) and REST API.

**Note**
Before you delete a storage virtual machine, make sure that no applications are accessing the data in the SVM that you want to delete and that you have deleted all non-root volumes.

### To delete a storage virtual machine (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **File systems**, and then choose the ONTAP file system that you want to delete an SVM from.
3. Choose the **Storage virtual machines** tab.
4. Choose the storage virtual machine that you want to delete.
5. For **Actions**, choose **Delete storage virtual machine**.
6. In the delete confirmation dialog box, choose **Delete storage virtual machines**.

### To delete a storage virtual machine (CLI)

- To delete an FSx for ONTAP storage virtual machine, use the delete-storage-virtual-machine CLI command (or the equivalent DeleteStorageVirtualMachine API operation), as shown in the following example.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id
 svm-5ab87160b8e4ad90d
```

## Viewing a storage virtual machine

You can see the FSx for ONTAP storage virtual machines that are currently on your file system using the Amazon FSx console, the AWS CLI, and the Amazon FSx API and SDKs.

**To view a storage virtual machine on your file system:**

- **Using the console** – Choose a file system to view its **File systems** detail page. To list all the storage virtual machines on the file system, choose the **Storage virtual machines** tab, and then choose the storage virtual machine that you want to view.
- **Using the CLI or API** – Use the delete-storage-virtual-machine CLI command or the DescribeStorageVirtualMachines API operation.

# Managing FSx for ONTAP volumes

Each storage virtual machine (SVM) on an FSx for ONTAP file system can contain one or more *volumes*, which are isolated data containers for files, directories, or iSCSI logical units of storage (LUNs). Volumes are *thin provisioned*, meaning that they consume storage capacity only for the data stored in them.

You can access a volume from Linux, Windows, or macOS clients over the Network File System (NFS) protocol, the Server Message Block (SMB) protocol, or over the Internet Small Computer Systems Interface (iSCSI) protocol by creating an iSCSI LUN (shared block storage). FSx for ONTAP also supports multi-protocol access (concurrent NFS and SMB access) to the same volume.

When you create or update a volume, two important configuration settings are the capacity pool tiering policy and the security style, as explained in the following sections.

## Volume data-tiering policy

Capacity pool storage is an elastic storage tier that can scale to petabytes in size and is cost-optimized for colder data. When you enable tiering on a volume, FSx for ONTAP automatically transitions data between primary storage and capacity pool storage based on your data access patterns. Tiering allows you to reduce your storage costs and store virtually unlimited data in a cluster. Capacity pool storage automatically grows and shrinks as you tier data to it, providing elastic storage for the portion of your dataset that grows over time.

You configure data-tiering policies on a per-volume basis. Amazon FSx supports the following tiering policies:

- **Auto** moves cold user data blocks in both the active file system and the snapshot copies to the storage pool tier.

  If data is read from the capacity pool tier in a random fashion, the cold data blocks in the capacity tier become hot and move to the primary storage tier. If read by sequential reads, such as those associated

with index and antivirus scans, the cold data blocks stay cold and do not move to the primary storage tier.

- **Snapshot Only** moves user data blocks of the volume snapshot copies that are not associated with the active file system to the storage pool tier.

  If read, cold data blocks on the capacity tier become hot and are moved to the primary storage tier.
- **All** moves cold user data blocks in both the snapshot copies and the active file system to the storage pool tier.

  If read, cold data blocks on the storage pool tier stay cold and are not written back to the primary storage tier.
- **None** (default) keeps a volume's data in the primary storage tier, preventing it from being moved to the storage pool tier.

You can also specify a minimum cooling period for tiering, which sets the time that user data in a volume must remain inactive before the data is considered cold and moved to the storage pool tier. The minimum cooling period, which applies to `Snapshot Only` and `Auto` tiering policies, ranges from 2–183 days. (The default is 2 days for `Snapshot Only` and 31 days for `Auto` policies.)

# Volume security style

A volume's *security style* setting determines what type of permissions are used for data on volumes when authorizing users. The two factors that you use to determine the security style for a volume are the type of administrator that manages the file system and the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. Following are considerations that can help you decide which security style to choose for a volume:

- **Unix (Linux)** – Choose this security style if the file system is managed by a Unix administrator, the majority of users are NFS clients, and an application accessing the data uses a Unix user as the service account.
- **NTFS** – Choose this security style if the file system is managed by a Windows administrator, the majority of users are SMB clients, and an application accessing the data uses a Windows user as the service account.
- **Mixed** – Choose this security style if the file system is managed by both Unix and Windows administrators and users consist of both NFS and SMB clients.

Keep in mind that security styles can differ between volumes.

# Creating a volume

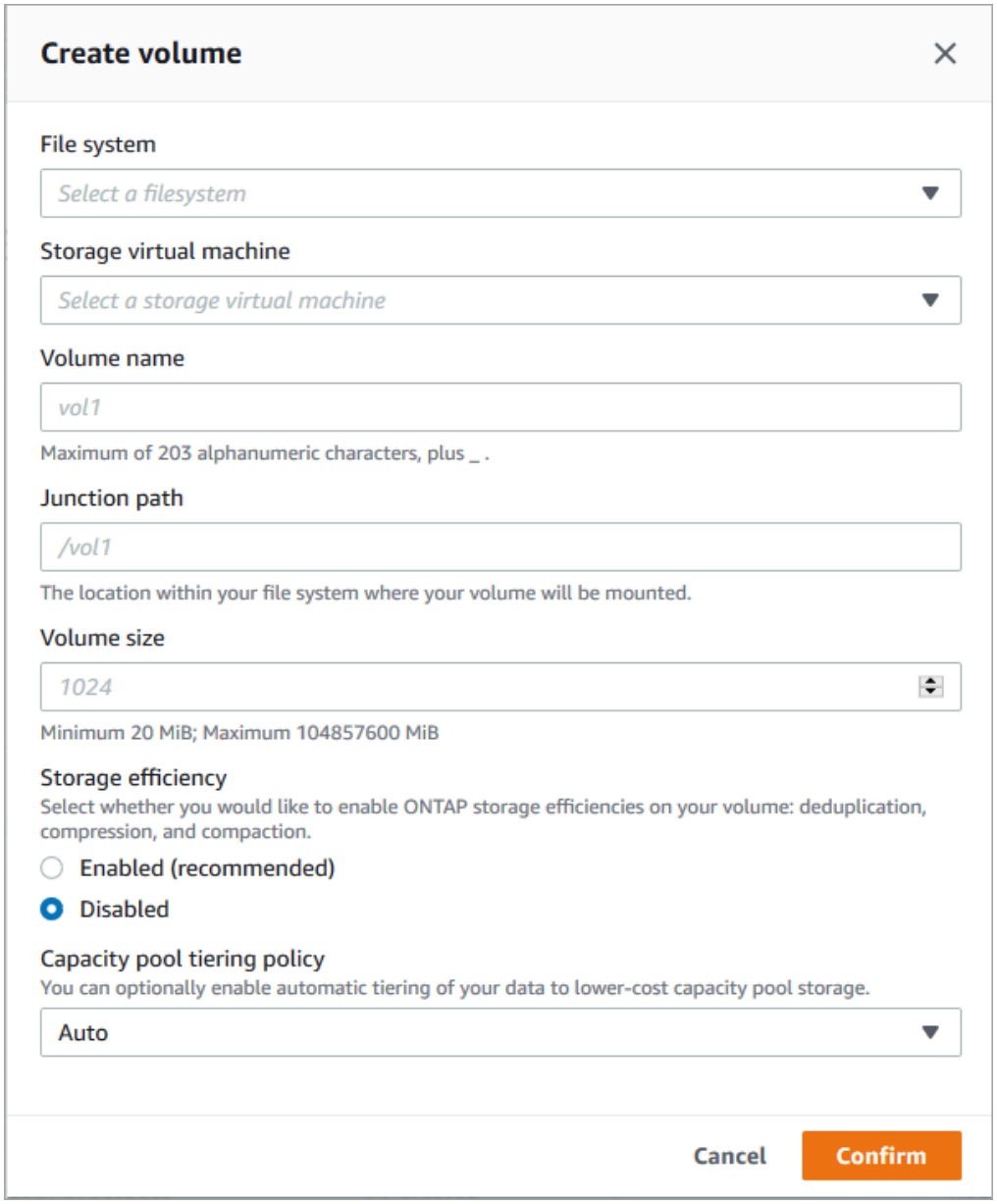
You can create an FSx for ONTAP volume using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, in addition to the NetApp ONTAP command line interface (CLI) and REST API.

## To create a volume (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **File systems**, and then choose the ONTAP file system that you want to create a volume for.
3. Choose the **Volumes** tab.

4. Choose the **Create volume** tab.

   The **Create volume** dialog box appears.




5. For **File system**, choose the file system to create the volume on.
6. For **Storage virtual machine**, choose the storage virtual machine (SVM) that this volume is created on.
7. In the **Volume name** field, provide a name for the volume. You can use a maximum of 203 alphanumeric characters, plus the underscore (_) special character.
8. For **Junction path**, enter a location within the file system where the volume will be mounted. The name must have a leading forward slash, for example `/vol3`.
9. For **Volume size**, enter any whole number in the range of 20–104857600 to specify the size in mebibytes (MiB).
10. For **Storage efficiency**, choose **Enabled** to enable the ONTAP storage-efficiency features (deduplication, compression, and compaction).

11. For **Capacity pool tiering policy**, choose the storage pool tiering policy for the volume, which can be **Auto** (the default), **Snapshot Only**, **All**, or **None**. For more information about capacity pool tiering policies, see Volume data-tiering policy (p. 46).
12. Choose **Confirm** to create the volume.

You can monitor the update progress on the **File systems** detail page, in the **Status** column of the **Volumes** pane. The volume is ready for use when its status is **Created**.

### To create a volume (CLI)

- To create an FSx for ONTAP volume, use the create-volume CLI command (or the equivalent CreateVolume API operation), as shown in the following example.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration JunctionPath=/
vol1,SizeInMegabytes=1024,StorageVirtualMachineId=svm-5ab87160b8e4ad90d
```

After successfully creating the volume, Amazon FSx returns its description in JSON format.

## Updating a volume configuration

You can update the configuration of an FSx for ONTAP volume using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, in addition to the NetApp ONTAP command line interface (CLI) and REST API.

### To update a volume configuration (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. Navigate to **File systems** and choose the ONTAP file system that you want to update a volume for.
3. Choose the **Volumes** tab.
4. Choose the volume that you want to update.
5. For **Actions**, choose **Update volume**.

   The **Update volume** dialog box displays with the volume's current settings.
6. For **Junction path**, enter an existing location within the file system where the volume will be mounted. The name must have a leading forward slash, such as `/vol5`.
7. For **Volume size**, enter any whole number in the range of 20–104867600 to specify the new size in mebibytes (MiB). You can increase or decrease the size of the volume.
8. For **Storage efficiency**, choose **Enabled** to enable the ONTAP storage efficiency features (deduplication, compression, and compaction), or choose **Disabled** to disable them.
9. For **Capacity pool tiering policy**, choose a new storage pool tiering policy for the volume, which can be **Auto** (the default), **Snapshot-only**, **All**, or **None**. For more information about capacity pool tiering policies, see Volume data-tiering policy (p. 46).
10. Choose **Update** to update the volume.

### To update a volume configuration (CLI)

- To update the configuration of an FSx for ONTAP volume, use the update-volume CLI command (or the equivalent UpdateVolume API operation), as shown in the following example.

```
aws fsx update-volume \
    --volume-id fsxvol-90d5ab87160b8e4ad \
    --name new_vol \
    --ontap-configuration JunctionPath=/
new_vol,SizeInMegabytes=2048,StorageEfficiencyEnabled=true
```

# Deleting a volume

You can delete an FSx for ONTAP volume using the Amazon FSx console, the AWS CLI, and the Amazon FSx API, in addition to the NetApp ONTAP command line interface (CLI) and REST API.

**Important**
When you delete a volume from the Amazon FSx console, you are given the option to take a final backup of the volume. New volumes can be created from backups. We recommend that you choose to take a final backup as a best practice. If you find you don't need it after a certain period of time, you can delete this and other manually created volume backups. By default, the `delete-volume` CLI command takes a final backup.

Before you delete a volume, make sure that no applications are accessing the data in the volume that you want to delete.

## To delete a volume (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. In the left navigation pane, choose **File systems**, and then choose the ONTAP file system that you want to delete a volume from.
3. Choose the **Volumes** tab.
4. Choose the volume that you want to delete.
5. For **Actions**, choose **Delete volume**.
6. In the confirmation dialog box, for **Create final backup**, you have two options:
   - Choose **Yes** to take a final backup of the volume. The name of the final backup is displayed.
   - Choose **No** if you don't want a final backup of the volume. You are asked to acknowledge that once the volume is deleted, automatic backups will no longer be available.
7. Confirm the volume deletion by entering **delete** in the **Confirm delete** field.
8. Choose **Delete volume(s)**.

## To delete a volume (CLI)

- To delete an FSx for ONTAP volume, use the delete-volume CLI command (or the equivalent DeleteVolume API operation), as shown in the following example.

```
aws fsx delete-volume --volume-id fsxvol-90d5ab87160b8e4ad
```

# Viewing a volume

You can see the FSx for ONTAP volumes that are currently on your file system using the Amazon FSx console, the AWS CLI, and the Amazon FSx API and SDKs.

**To view the volumes on your file system:**

- **Using the console** – Choose a file system to view the **File systems** detail page. Choose the **Volumes** tab to list all the volumes on the file system, and then choose the volume you want to view.
- **Using the CLI or API** – Use the describe-volumes CLI command or the DescribeVolumes API operation.

# Creating SMB shares

To manage file shares on your Amazon FSx file system, you can use the Shared Folders GUI. The Shared Folders GUI provides a central location for managing all shared folders in your storage virtual machine (SVM). The following procedures detail how to manage your file shares.

**To connect shared folders to your Amazon FSx file system**

1. Launch your Amazon EC2 instance and connect it to the Microsoft Active Directory that your Amazon FSx file system is joined to. To do this, choose one of the following procedures from the *AWS Directory Service Administration Guide*:
   - Seamlessly join a Windows EC2 instance
   - Manually join a Windows instance
2. Connect to your instance as a user that is a member of the file system administrators group. For more information, see Connecting to Your Windows Instance in the *Amazon EC2 User Guide for Windows Instances*.
3. Open the **Start** menu and run **fsmgmt.msc** using **Run As Administrator**. Doing this opens the Shared Folders GUI tool.
4. For **Action**, choose **Connect to another computer**.
5. For **Another computer**, enter the DNS name for your storage virtual machine (SVM), for example **`netbios_name.corp.example.com`**.

   To find your SVM's DNS name on the Amazon FSx console, choose **Storage virtual machines**, choose your SVM, and then scroll down to **Endpoints** until you find **SMB DNS name**. You can also get the DNS name in the response of the DescribeStorageVirtualMachines API operation.
6. Choose **OK**. An entry for your Amazon FSx file system then appears in the list for the Shared Folders tool.

Now that Shared Folders is connected to your Amazon FSx file system, you can manage the Windows file shares on the file system with the following actions:

- **Create a new file share** – In the Shared Folders tool, choose **Shares** in the left pane to see the active shares for your Amazon FSx file system. Choose **New Share** and complete the Create a Shared Folder wizard.

  You have to create the local folder prior to creating the new file share. You can do so as follows:
  - Using the Shared Folders tool: choose **Browse** when specifying a local folder path, choose **Make new folder** to create the local folder.
  - Using command line:

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C$\MyNewFolder
```

- **Modify a file share** – In the Shared Folders tool, open the context (right-click) menu for the file share that you want to modify in the right pane, and choose **Properties**. Modify the properties and choose **OK**.

- **Remove a file share** – In the Shared Folders tool, open the context (right-click) menu for the file share that you want to remove in the right pane, and then choose **Stop Sharing**.

  **Note**
  Removing file shares from the GUI is possible only if you connected to **fsmgmt.msc** using the DNS name of the Amazon FSx file system. If you connected using the IP address or DNS alias name of the file system, the **Stop Sharing** option won't work and the file share isn't removed.

# Tag your Amazon FSx resources

To help you manage your file systems and other Amazon FSx resources, you can assign your own metadata to each resource in the form of tags. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags that you've assigned to it. This topic describes tags and shows you how to create them.

**Topics**



## Tag basics

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. For example, you could define a set of tags for your account's Amazon FSx file systems that helps you track each instance's owner and stack level.

We recommend that you devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your resources. You can search and filter the resources based on the tags you add. For more information about how to implement an effective resource tagging strategy, see the AWS whitepaper Tagging Best Practices.

Tags don't have any semantic meaning to Amazon FSx and are interpreted strictly as a string of characters. Also, tags are not automatically assigned to your resources. You can edit tag keys and values, and you can remove tags from a resource at any time. You can set the value of a tag to an empty string, but you can't set the value of a tag to null. If you add a tag that has the same key as an existing tag on that resource, the new value overwrites the old value. If you delete a resource, any tags for the resource are also deleted.

If you're using the Amazon FSx API, the AWS CLI, or an AWS SDK, you can use the `TagResource` API action to apply tags to existing resources. Additionally, some resource-creating actions enable you to specify tags for a resource when the resource is created. If tags cannot be applied during resource creation, we roll back the resource creation process. This ensures that resources are either created with tags or not created at all, and that no resources are left untagged at any time. By tagging resources at the time of creation, you can eliminate the need to run custom tagging scripts after resource creation. For more information about enabling users to tag resources on creation, see Grant permission to tag resources during creation (p. 92).

# Tagging your resources

You can tag Amazon FSx resources that exist in your account. If you're using the Amazon FSx console, you can apply tags to resources by using the Tags tab on the relevant resource screen. When you create resources, you can apply the Name key with a value, and you can apply tags of your choice when creating a new file system. The console may organize resources according to the Name tag, but this tag doesn't have any semantic meaning to the Amazon FSx service.

You can apply tag-based resource-level permissions in your IAM policies to the Amazon FSx API actions that support tagging on creation to implement granular control over the users and groups that can tag resources on creation. Your resources are properly secured from creation—tags are applied immediately to your resources, therefore any tag-based resource-level permissions controlling the use of resources are immediately effective. Your resources can be tracked and reported on more accurately. You can enforce the use of tagging on new resources, and control which tag keys and values are set on your resources.

You can also apply resource-level permissions to the `TagResource` and `UntagResource` Amazon FSx API actions in your IAM policies to control which tag keys and values are set on your existing resources.

For more information about tagging your resources for billing, see Using cost allocation tags in the *AWS Billing and Cost Management User Guide*.

# Tag restrictions

The following basic restrictions apply to tags:

- Maximum number of tags per resource – 50
- For each resource, each tag key must be unique, and each tag key can have only one value.
- Maximum key length – 128 Unicode characters in UTF-8
- Maximum value length – 256 Unicode characters in UTF-8
- The allowed characters are: letters, numbers, and spaces representable in UTF-8, and the following characters: + - = . _ : / @.
- Tag keys and values are case-sensitive.
- The `aws:` prefix is reserved for AWS use. If a tag has a tag key with this prefix, then you can't edit or delete the tag's key or value. Tags with the `aws:` prefix do not count against your tags per resource limit.

You can't delete a resource based solely on its tags; you must specify the resource identifier. For example, to delete a file system that you tagged with a tag key called `DeleteMe`, you must use the `DeleteFileSystem` action with the file system resource identifier, such as fs-1234567890abcdef0.

When you tag public or shared resources, the tags you assign are available only to your AWS account; no other AWS account will have access to those tags. For tag-based access control to shared resources, each AWS account must assign its own set of tags to control access to the resource.

# Permissions and tag

For more information about the permissions required to tag Amazon FSx resources at creation, see Grant permission to tag resources during creation (p. 92).

For more information about using tags to restrict access to Amazon FSx resources in IAM policies, see Using tags to control access to your Amazon FSx resources (p. 93).

# FSx for ONTAP file system status

You can view the status of an Amazon FSx file system by using the Amazon FSx console, the AWS CLI command describe-file-systems, or the API operation DescribeFileSystems.

| File system status | Description |
|---|---|
| AVAILABLE | The file system has been successfully created and is available for use. |
| CREATING | Amazon FSx is creating a new file system. |
| DELETING | Amazon FSx is deleting an existing file system. |
| MISCONFIGURED | The file system is in a misconfigured but recoverable state. |
| FAILED | 1. The file system has failed and Amazon FSx can't recover it.<br>2. When creating new file system, Amazon FSx was unable to create a new file system. |

# Working with Amazon FSx maintenance windows

FSx for ONTAP performs routine software patching for the NetApp ONTAP software it manages. The maintenance window is your opportunity to control what day and time of the week this software patching occurs.

Patching occurs infrequently, typically once every several weeks. Patching should require only a fraction of your 30-minute maintenance window. During these few minutes of time, your Multi-AZ file systems automatically fail over and fail back.

You choose the maintenance window during file system creation. If you have no time preference, then a 30-minute default window is assigned.

> **Note**
> To ensure data integrity during maintenance activity, FSx for ONTAP completes any pending write operations to the underlying storage volumes hosting your file system before maintenance begins.

You can use the Amazon FSx Management Console, AWS CLI, AWS API, or one of the AWS SDKs to change the maintenance window for your file systems.

### To change the weekly maintenance window (console)

1. Open the Amazon FSx console at https://console.aws.amazon.com/fsx/.
2. Choose **File systems** in the left hand navigation column.
3. Choose the file system that you want to change the weekly maintenance window for. The file system details page displays.
4. Choose **Administration** to display the file system administration **Settings** panel.
5. Choose **Update** to display the **Change maintenance window** window.
6. Enter the new day and time that you want the weekly maintenance window to start.

7. Choose **Save** to save your changes. The new maintenance start time is displayed in the file system administration **Settings** panel.

To change the weekly maintenance window using the CLI or API using the UpdateFileSystem operation, see To update a file system (CLI) (p. 41).

# Managing FSx for ONTAP resources using NetApp applications

In addition to the AWS Management Console, AWS CLI, and AWS API and SDKs, you can also use these NetApp management tools and applications to manage your FSx for ONTAP resources:

**Topics**



## Using NetApp Cloud Manager

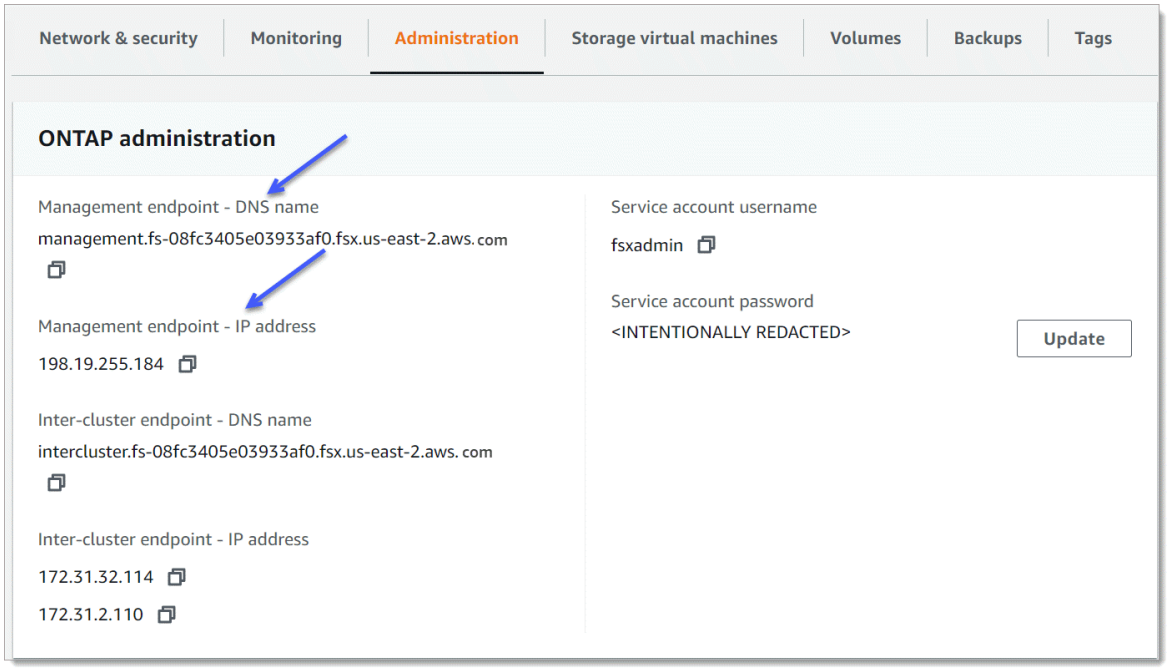
NetApp Cloud Manager provides a centralized user interface to manage, monitor, and automate ONTAP deployments in AWS and on premises. For more information, see the Cloud Manager documentation.

## Using the NetApp ONTAP CLI

You can manage your Amazon FSx for NetApp ONTAP resources using the NetApp ONTAP 9.9.1 CLI. You can manage resources at the file system (analagous to NetApp ONTAP cluster) level, and at the SVM level.

### Managing file systems with the NetApp ONTAP CLI

You can run NetApp ONTAP CLI commands on your FSx for ONTAP file system, analagous to running them on a NetApp ONTAP cluster. You access the NetApp ONTAP CLI on your file system by establishing a secure shell (SSH) connection to the file system's management endpoint. You use the `fsxadmin` password you created when you created the file system to log in. You can find the file system's management endpoint **DNS name** and **IP address** in the Amazon FSx console, in the **Administration** tab of the FSx for ONTAP file system details page, shown in the following graphic.




To connect to the file system's management endpoint with SSH, use the user `fsxadmin` and the password that you set when you created the file system. You can SSH into the file system from a client that is in the same VPC as the file system, using the management endpoint IP address or DNS name.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

The SSH command with sample values:

```
ssh fsxadmin@198.51.100.0
```

The SSH command using the management endpoint DNS name:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

The SSH command using a sample DNS name:

```
ssh fsxadmin@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

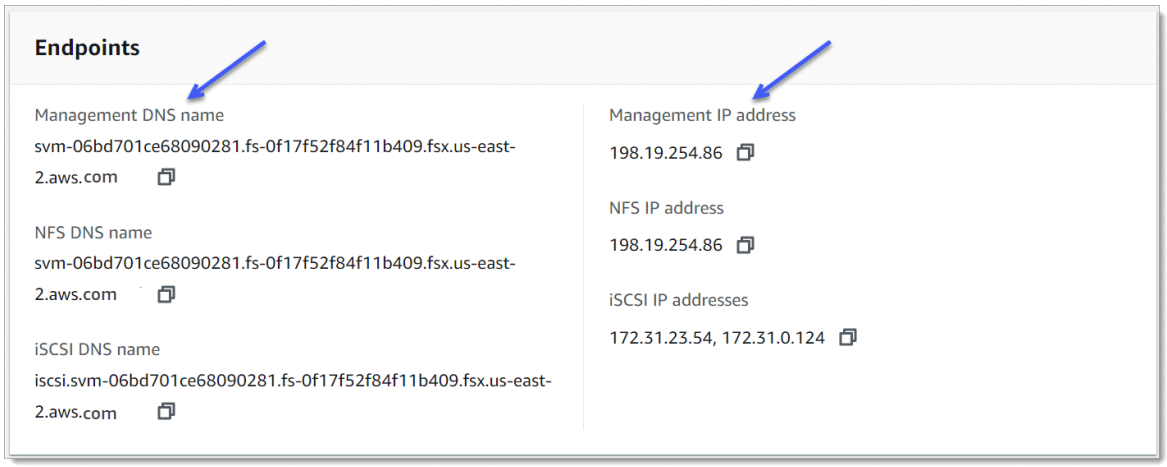
```
Password: fsxadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

The `fsxadmin` user has a view at the file system level, which includes all SVMs and volumes in the file system, equivalent to that of a NetApp ONTAP cluster administrator. However, you cannot perform most NetApp ONTAP CLI `cluster` commands.

## Managing SVMs using the NetApp ONTAP 9.9.1 CLI

You can run NetApp ONTAP CLI commands on your FSx for ONTAP SVM by establishing a secure shell (SSH) connection to the SVM's management endpoint. You can use the `fsxadmin` username and

password you created on the SVM's file system, or the `vsadmin` username and password, if you specified one when you created the SVM. You can find the SVM's management endpoint **DNS name** and **IP address** in the Amazon FSx console, in the **Endpoints** panel of the Storage virtual machines details page, shown in the following graphic.




To connect to the SVM's management endpoint with SSH, use username `vsadmin` and the vsadmin password that you set when you created the SVM. If you did not set a vsadmin password, use username `fsxadmin` and the fsxadmin password. You can SSH into the SVM from a client that is in the same VPC as the file system, using the management endpoint IP address or DNS name.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

The command with sample values:

```
ssh vsadmin@198.51.100.10
```

The SSH command using the management endpoint DNS name:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

The SSH command using a sample DNS name:

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

Amazon FSx for NetApp ONTAP supports the NetApp ONTAP 9.9.1 CLI commands.

For a complete reference of NetApp ONTAP CLI 9.9.1 commands, see the ONTAP 9.9.1 Commands: Manual Page Reference.

# Using the NetApp ONTAP REST API

When accessing your Amazon FSx for NetApp ONTAP using the NetApp ONTAP REST API with the `fsxadmin` login, you will need to do one of the following:

- Disable TLS validation.
- Trust the AWS certificate authorities (CAs) – The certificate bundle for the CAs in each region can be found at the follow URLs:
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle-<region>.pem for Public AWS Regions
  - https://fsx-aws-us-gov-certificates.s3.amazonaws.com/bundle-<region>.pem for AWSGovCloud Regions
  - https://fsx-aws-cn-certificates.s3.amazonaws.com/bundle-<region>.pem for AWS China Regions

For a complete reference of NetApp ONTAP 9.9.1 REST API commands, see the ONTAP 9.9.1 REST API Online Reference.

# Working with Microsoft Active Directory in FSx for ONTAP

Amazon FSx works with Microsoft Active Directory (AD) to integrate with your existing Windows and macOS environments. Active Directory is the Microsoft directory service used to store information about objects on the network and make this information easy for administrators and users to find and use. These objects typically include shared resources such as file servers and network user and computer accounts.

When you create a storage virtual machine (SVM) with Amazon FSx, you can optionally join it to your Active Directory domain to provide user authentication and file- and folder-level access control. Your Windows and macOS SMB clients can then use their existing user identities in Active Directory to authenticate themselves and access the SVM's volumes. Users can also use their existing identities to control access to individual files and folders. In addition, you can migrate your existing files and folders and these items' security access control list (ACL) configuration to Amazon FSx without any modifications.

When you join Amazon FSx for NetApp ONTAP to an Active Directory, you join each SVM to the AD independently. This means that you can have a file system where some SVMs are joined to an AD, while other SVMs are not. For example, you could have an SVM with AD primarily for Windows and macOS SMB clients, and another SVM without AD for Linux clients.

After join your SVM to an Active Directory, you can update the following properties:

- Service user credentials
- DNS server IP addresses

**Topics**



## Using Amazon FSx SVMs with an Active Directory

Your organization might manage identities and devices in an Active Directory (on-premises or in the cloud). If so, you can join your Amazon FSx file system's SVMs directly to your existing AD domain. When you create a new FSx for ONTAP SVM in the console, choose **Join an Active Directory** under the **Active Directory** section. Provide the following details for your self-managed AD:

- The NetBIOS name of the Active Directory computer object to create for your SVM. The NetBIOS name cannot exceed 15 characters.
- The fully qualified domain name of your Active Directory. The domain name cannot exceed 255 characters.

  **Note**
  Domain name must not be in the Single Label Domain (SLD) format. Amazon FSx currently does not support SLD domains.
- Up to 3 IP addresses of the DNS servers for your domain.

  The DNS server IP addresses and AD domain controller IP addresses can be in any IP address range, except:
  - IP addresses that conflict with Amazon Web Services-owned IP addresses in that AWS Region. For a list of AWS-owned IP addresses by region, see the AWS IP address ranges.

  - IP addresses in the following CIDR block range: 198.19.0.0/16
- User name and password for a service account on your AD domain, for Amazon FSx to use to join the SVM to your AD domain.
- (Optional) The Organizational Unit (OU) in your domain in which you want your SVM to be joined.

  **Note**
  If you are joining your SVM to an AWS Directory Service AD, you must provide the name of an OU that's within the default OU that Directory Service creates for your AWS -related directory objects. This is because Directory Service does not provide access to your AD's default `Computers` OU. For example, if your AD domain is `example.com`, you can specify the following OU: `OU=Computers,OU=example,DC=example,DC=com`
- (Optional) The domain group to which you want to delegate authority to perform administrative actions on your file system. For example, this domain group might manage Windows SMB file shares, take ownership of files and folders, and so on. If you don't specify this group, Amazon FSx delegates this authority to the Domain Admins group in your AD domain by default.

  For more information, see Creating a storage virtual machine (p. 42).

  **Important**
  Amazon FSx only registers DNS records for an SVM if you are using Microsoft DNS as the default DNS service. If you are using a third-party DNS, you will need to manually set up DNS entries for your Amazon FSx SVMs after you create them.

When you join your FSx for ONTAP SVM directly to your self-managed AD, your SVM resides in the same AD forest (the top-most logical container in an AD configuration that contains domains, users, and computers) and in the same AD domain as your users and existing resources (including existing file servers).

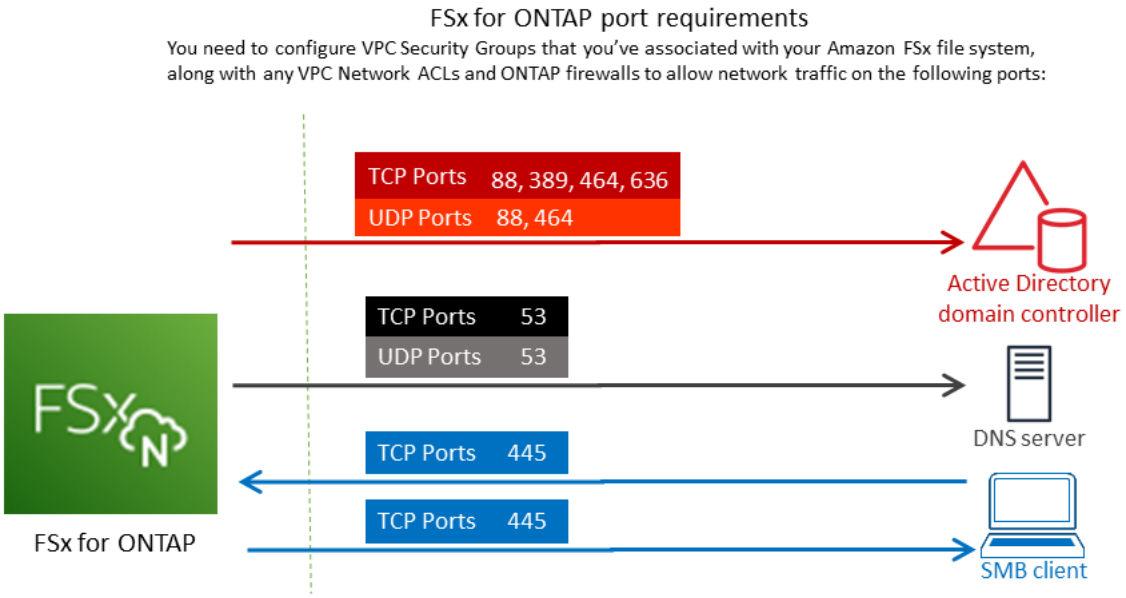
**Topics**



# Prerequisites for using a self-managed Microsoft AD

Before you create an FSx for ONTAP SVM joined to your self-managed Microsoft AD domain, make sure that you have created and set up the following requirements:

- An on-premises or other self-managed Microsoft AD that the SVM is to join, with the following configuration:
  - The domain functional level of your AD domain controller is at Windows Server 2000 or higher.
  - The DNS server IP addresses and AD domain controller IP addresses.
  - Domain name that is not in the Single Label Domain (SLD) format. Amazon FSx does not support SLD domains.
  - If you have Active Directory sites defined, you must make sure that the subnets in the VPC associated with your Amazon FSx file system are defined in the same Active Directory site, and that no conflicts exist between the subnets in your VPC and the subnets in your other sites.
- The following network configurations:
  - Connectivity configured between the Amazon VPC where you want to create the file system and your self-managed Active Directory. You can set up connectivity using AWS Direct Connect, AWS VPN, or AWS Transit Gateway.
  - Ensure that the security group and the VPC Network ACLs for the subnet(s) where you're creating your FSx file system allow traffic on the ports and in the directions shown in the following diagram.




The following table identifies the role of each port.

| Protocol | Ports | Role |
|---|---|---|
| TCP/UDP | 53 | Domain Name System (DNS) |
| TCP/UDP | 88 | Kerberos authentication |
| TCP/UDP | 389 | Lightweight Directory Access Protocol (LDAP) |
| TCP | 445 | Directory Services SMB file sharing |
| TCP/UDP | 464 | Change/Set password |
| TCP | 636 | Lightweight Directory Access Protocol over TLS/SSL (LDAPS) |

- Ensure that these traffic rules are also mirrored on the firewalls that apply to each of the AD domain controllers, DNS servers, FSx clients and FSx administrators.

  **Important**
  While Amazon VPC security groups require ports to be opened only in the direction that network traffic is initiated, most Windows firewalls and VPC network ACLs require ports to be open in both directions.

- A service account in your self-managed Microsoft AD with delegated permissions to join computers to the domain. A *service account* is a user account in your self-managed Microsoft AD that has been delegated certain tasks.

  The service account also needs to, at a minimum, be delegated the following permissions in the OU that you're joining the file system to:

  - Ability to reset passwords
  - Ability to restrict accounts from reading and writing data
  - Validated ability to write to the DNS host name
  - Validated ability to write to the service principal name

- Be delegated control to create and delete computer objects
- Validated ability to read and write Account Restrictions

These represent the minimum set of permissions that are required to join computer objects to your Active Directory. For more information, see the Microsoft Windows Server documentation topic Error: Access is denied when non-administrator users who have been delegated control try to join computers to a domain controller.

To learn more about creating a service account with the correct permissions, see Delegating privileges to your Amazon FSx service account (p. 62).

**Note**
Amazon FSx requires a valid service account throughout the lifetime of your Amazon FSx file system. Amazon FSx must be able to fully manage the file system and perform tasks that require unjoining and rejoining your AD domain using, such as replacing a failed file SVM or patching NetApp ONTAPP software. Keep your Active Directory configuration, including the service account credentials, updated with Amazon FSx. To learn how, see Keeping your Active Directory configuration updated with Amazon FSx (p. 63).

If this is your first time using AWS and FSx for ONTAP, make sure to set up before starting. For more information, see Setting up FSx for ONTAP (p. 10).

**Important**
Do not move computer objects that Amazon FSx creates in the OU after your SVMs are created. Doing so will cause your SVMs to become misconfigured.

# Best practices for joining FSx for ONTAP SVMs to an Active Directory domain

Here are some suggestions and guidelines you should consider when joining Amazon FSx for NetApp ONTAP SVMs to your self-managed Microsoft Active Directory. Note that these are recommended as best practices, but not required.

## Delegating privileges to your Amazon FSx service account

Make sure to configure the service account that you provide to Amazon FSx with the minimum privileges required. In addition, segregate the Organizational Unit (OU) from other domain controller concerns.

To join Amazon FSx SVMs to your domain, make sure that the service account has delegated privileges. Members of the **Domain Admins** group have sufficient privileges to perform this task. However, as a best practice, use a service account that only has the minimum privileges necessary to do this. The following procedure demonstrates how to delegate just the privileges necessary to join FSx for ONTAP SVMs to your domain.

Perform this procedure on a machine that is joined to your directory and has the Active Directory User and Computers MMC snap-in installed.

**To create a service account for your Active Directory domain**

1. Make sure that you are logged in as a domain administrator for your Active Directory domain.
2. Open the **Active Directory User and Computers** MMC snap-in.
3. In the task pane, expand the domain node.
4. Locate and open the context (right-click) menu for the OU that you want to modify, and then choose **Delegate Control**.

5. On the **Delegation of Control Wizard** page, choose **Next**.
6. Choose **Add** to add a specific user or a specific group for **Selected users and groups**, and then choose **Next**.
7. On the **Tasks to Delegate** page, choose **Create a custom task to delegate**, and then choose **Next**.
8. Choose **Only the following objects in the folder**, and then choose **Computer objects**.
9. Choose **Create selected objects in this folder** and **Delete selected objects in this folder**. Then choose **Next**.
10. For **Permissions**, choose the following:
    - **Reset Password**
    - **Read and write Account Restriction**s
    - **Validated write to DNS host name**
    - **Validated write to service principal name**
11. Choose **Next**, and then choose **Finish**.
12. Close the Active Directory User and Computers MMC snap-in.

**Important**
Do not move computer objects that Amazon FSx creates in the OU after your SVMs are created. Doing so will cause your SVMs to become misconfigured.

## Keeping your Active Directory configuration updated with Amazon FSx

To help ensure continued, uninterrupted availability of your Amazon FSx SVMs, update an SVM's self-managed Active Directory (AD) configuration any time that you make changes to your self-managed AD setup.

For example, suppose that your AD uses a time-based password reset policy. In this case, as soon as the password is reset, make sure to update the service account password with Amazon FSx. To do this, use the Amazon FSx console, Amazon FSx API, or AWS CLI. Similarly, if the DNS server IP addresses change for your Active Directory domain, as soon as the change occurs update the DNS server IP addresses with Amazon FSx. Again, do this using the Amazon FSx console, API, or CLI.

If there's an issue with the updated self-managed AD configuration, the SVM state switches to **Misconfigured**. This state shows an error message and recommended action beside the SVM description in the console, API, and CLI. If an issue happens, take the recommended corrective action to provide the correct configuration properties. If the issue is resolved, verify that your SVM's state changes to **Created**.

## Using security groups to limit traffic within your VPC

To limit network traffic in your virtual private cloud (VPC), you can implement the principle of least privilege in your VPC. In other words, you can limit privileges to the minimum ones necessary. To do this, use security group rules. To learn more, see Amazon VPC security groups (p. 105).

## Creating outbound security group rules for your file system's network interface

For greater security, consider configuring a security group with outbound traffic rules. These rules should allow outbound traffic only to your self-managed Microsoft AD domains controllers or within the subnet or security group. Apply this security group to the VPC associated with your Amazon FSx file system's elastic network interface. To learn more, see File System Access Control with Amazon VPC (p. 105).

# Joining an FSx for ONTAP SVM to an Active Directory domain

The following sections provide information about joining an SVM to an Active Directory domain and updating the SVM's Active Directory configuration.

## Joining an SVM to an AD

When you create an FSx for ONTAP storage virtual machine, you can optionally join it to your organization's Active Directory during the SVM's creation. You create an SVM joined to an Active Directory domain in one of the following scenarios:

- You use the **Standard create** creation option to create an FSx for ONTAP file system on the Amazon FSx console. For more information, see To create a file system (console) (p. 37).
- You create a new SVM on an existing FSx for ONTAP file system using the Amazon FSx console, AWS CLI, or the Amazon FSx API. For more information, see Creating a storage virtual machine (p. 42).

## Updating an SVM AD configuration

You can use the Amazon FSx console, AWS CLI, or the Amazon FSx API to update the service credentials or the DNS server IP addresses of an SVM's Active Directory configuration. For more information, see Updating a storage virtual machine (p. 44).

> **Note**
> You cannot change the Active Directory configuration of an existing SVM using the Amazon FSx console, AWS CLI, or the Amazon FSx API. For example, if an SVM was created without being joined to an Active Directory, you cannot join it to an Active Directory afterwards.
> You can change the Active Directory configuration of an existing SVM by using the ONTAP CLI or API directly, using the `vserver cifs` commands. For more information, see Manage the CIFS configuration of a Vserver.

# Migrating to Amazon FSx for NetApp ONTAP

The following section provides information on how to migrate to Amazon FSx for NetApp ONTAP using SnapMirror.

## Migrating to FSx for ONTAP using SnapMirror

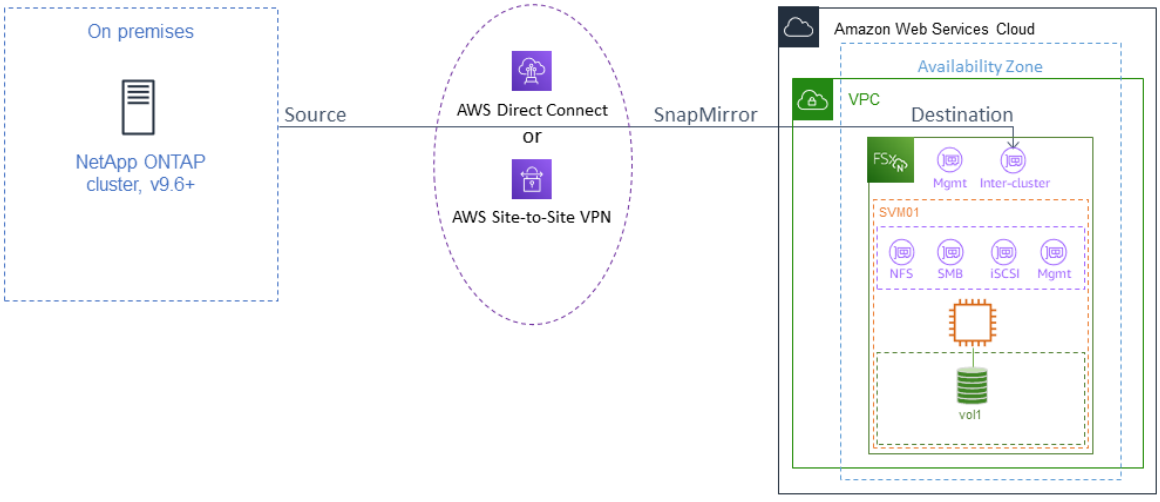
You can migrate your NetApp ONTAP file systems to Amazon FSx for NetApp ONTAP using NetApp SnapMirror.

NetApp SnapMirror employs block-level replication between two ONTAP file systems, replicating data from a specified source volume to a destination volume. We recommend using SnapMirror to migrate on-premise NetApp ONTAP file systems to FSx for ONTAP because its block-level replication is quick and efficient even for file systems with complex directory structures, over 50 million files, and very small file sizes (on the order of kilobytes).

When you use SnapMirror to migrate to FSx for ONTAP, deduplicated and compressed data remains in those states, which reduces transfer times and reduces the amount of bandwidth required for migration. Snapshots that exist on the source ONTAP volumes are preserved when migrated to the destination volumes. Migrating your on-premises NetApp ONTAP file systems to FSx for ONTAP involves the following high level tasks:

1. Create the destination volume in Amazon FSx.
2. Gather source and destination logical interfaces (LIFs)
3. Establish cluster peering between the source and destination file system.
4. Create an SVM peering relationship.
5. Create the SnapMirror relationship.
6. Maintain an updated destination cluster.
7. Cutover to your FSx for ONTAP file system.

The following diagram illustrates the migration scenario described in this section.



**Topics**



# Before you begin

Before you begin using the procedures described in the following sections, be sure that the following prerequisites are met:

- The source and destination file systems are connected in the same VPC, or are in networks that are peered using Amazon VPC Peering, Transit Gateway, AWS Direct Connect or AWS VPN. For more information, see VPC peering (p. 17) and What is VPC peering? in the *Amazon VPC Peering Guide*.
- The source file system must be a NetApp ONTAP file system running ONTAP version 9.6 or newer. These procedures use an on-premise NetApp ONTAP file system for the source.
- Your on-premises NetApp ONTAP file system includes a SnapMirror license.
- You have created a destination FSx for ONTAP file system with an SVM, but you have not created a destination volume. For more information, see Creating FSx for ONTAP file systems (p. 37).

The commands in these procedures use the following cluster, SVM, and volume aliases:

- *`FSx-Dest`* – the destination (FSx) cluster's ID (in the format FSxIdabcdef1234567890a).
- *`OnPrem-Source`* – the source cluster's ID.
- *`DestSVM`* – the destination SVM name.
- *`SourceSVM`* – the source SVM name.
- Both the source and destination volume names are `vol1`.

> **Note**
> An FSx for ONTAP file system is referred to as a cluster in all of the ONTAP CLI commands.

The procedures in this section use the following NetApp ONTAP CLI commands.

- volume create command
- cluster commands
- vserver peer commands
- snapmirror commands

You will use the NetApp ONTAP CLI to create and manage a SnapMirror configuration on your FSx for ONTAP file system. For more information, see Using the NetApp ONTAP CLI (p. 55).

# Create the destination volume

In this procedure, you will use the NetApp ONTAP CLI to create a destination volume on your FSx for ONTAP file system. You will need the `fsxadmin` password and the IP address or DNS name of the file system's management port.

1. Establish an SSH session with the destination file system using user `fsxadmin` and the password that you set when you created the file system.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Create a volume on the destination cluster with a capacity that is at least equal to the capacity of the source volume. Use `-type DP` to designate it as a destination for a SnapMirror relationship.

```
FSx-Dest::> vol create -volume vol1 -junction-path /vol1 -vserver fsx -aggregate aggr1
 -size 1g -type DP
```

# Record the source and destination inter-cluster LIFs

SnapMirror uses inter-cluster logical interfaces (LIFs), each with a unique IP address, to facilitate data transfer between source and destination clusters.

1. For the destination FSx for ONTAP file systems, you can retrieve the **Inter-cluster endpoint - IP addresses** from the Amazon FSx console by navigating to the **Administration** tab on your file system's details page.
2. For the source NetApp ONTAP cluster, retrieve the inter-cluster LIF IP addresses using the ONTAP CLI. Run the following command:

```
OnPrem-Source::> network interface show -role inter-cluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

   Save the `inter_1` and `inter_2` IP addresses. They are referenced in the `FSx-Dest` as `dest_inter_1` and `dest_inter_2` and for `OnPrem-Source` as `source_inter_1` and `source_inter_2`.

# Establish cluster peering between source and destination

Establish a cluster peer relationship on the destination cluster by providing the `source_inter_1` and `source_inter_2` IP addresses. You will also need to create a passphrase which you will need to enter in when you establish cluster peering on the source cluster.

1. Set up peering on the destination cluster using the following command:

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the other
 cluster.
```

2. Next, establish the cluster peer relationship on the source cluster. You'll need to enter the passphrase you created above to authenticate.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Verify the peering was successful using the following command on the source cluster. In the output, `Availability` should be set to `Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

# Create an SVM peering relationship

With cluster peering established, the next step is peering the SVMs. Create an SVM peering relationship on the destination cluster (FSx-Dest) using the `vserver peer` command. Additional aliases used in the following commands are as follows:

- `DestLocalName` – this is name used to identify the destination SVM when configuring SVM peering on the source SVM.
- `SourceLocalName` – this is the name used to identify the source SVM when configuring SVM peering on the destination SVM.

1. Use the following command to create an SVM peering relationship between the source and destination SVMs.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Accept the peering relationship on the source cluster:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -local-
name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Verify the SVM peering status using the following command; `Peer State` should be set to `peered` in the response.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

# Create the SnapMirror relationship

Now that you have peered the source and destination SVMs, the next steps are to create and initialize the SnapMirror relationship on the destination cluster.

**Note**
Once you create and initialize a SnapMirror relationship, the destination volumes are read-only until the relationship is broken.

- Use the `snapmirror create` command to create the SnapMirror relationship on the destination cluster. The `snapmirror create` command must be used from the destination SVM.

  You can optionally use `-throttle` to set the maximum bandwidth (in kB/sec) for the SnapMirror relationship.

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

# Transfer data to your FSx for ONTAP file system

Now that the you've created the SnapMirror relationship, you can transfer data to the destination file system.

1. You can transfer data to the destination file system by running the following command on the destination file system.

   **Note**
   Once you run this command, SnapMirror begins transferring snapshots of data from the source volume to the destination volume.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. If you are migrating data that is being actively used, you'll need to update your destination cluster so that it remains synced with your source cluster. To perform a one-time update to the destination cluster, run the following command.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. You can also schedule hourly or daily updates prior to completing the migration and moving your clients to FSx for ONTAP. You can establish a SnapMirror update schedule using the `snapmirror modify` command.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

# Cutting over to Amazon FSx

To prepare for the cut over to your FSx for ONTAP file system, do the following:

- Disconnect all clients that write to the source cluster.
- Perform a final SnapMirror transfer to ensure there is no data loss when cutting over.

- Break the SnapMirror relationship.
- Connect all clients to your FSx for ONTAP file system.

1. To ensure that all data from the source cluster is transferred to FSx for ONTAP file system, perform a final Snapmirror transfer.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Ensure that the data migration is complete by verifying that `Mirror State` is set to `Snapmirrored`, and `Relationship Status` is set to `Idle`. You also should ensure that the `Last Transfer End Timestamp` date is as expected, as it shows when the last transfer to the destination volume occurred.
3. Run the following command to show the SnapMirror status.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source      Destination   Mirror        Relationship Last Transfer End
Path        Path          State         Status       Timestamp
----------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Disable any future SnapMirror transfers by using the `snapmirror quiesce` command.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verify that the `Relationship Status` has changed to `Quiesced` using `snapmirror show`.

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------- --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. During migration, the destination volume is read-only. To enable read/write, you need to break the SnapMirror relationship and cut over to your FSx for ONTAP file system. Break the SnapMirror relationship using the following command.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

Now the volume is available with the data from the source volume fully migrated to the destination volume and is available for clients to read and write to it. To make this data accessible to clients and applications, see Accessing data: supported clients and environments (p. 16).

# Logging FSx for ONTAP API Calls with AWS CloudTrail

Amazon FSx is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon FSx. CloudTrail captures all Amazon FSx API calls for Amazon FSx for NetApp ONTAP as events. Captured calls include calls from the Amazon FSx console and from code calls to Amazon FSx API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon FSx. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon FSx. You can also determine the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

## Amazon FSx Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When API activity occurs in Amazon FSx, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history.

For an ongoing record of events in your AWS account, including events for Amazon FSx, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics in the *AWS CloudTrail User Guide:*

- Creating a trail for your AWS account
- AWS service integrations with CloudTrail Logs
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

All Amazon FSx API calls are logged by CloudTrail. For example, calls to the `CreateFileSystem` and `TagResource` operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element in the *AWS CloudTrail User Guide.*

# Understanding Amazon FSx Log File Entries

A *trail* is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An *event* represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `TagResource` operation when a tag for a file system is created from the console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

The following example shows a CloudTrail log entry that demonstrates the `UntagResource` action when a tag for a file system is deleted from the console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
```

```
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

# Amazon FSx for NetApp ONTAP performance

Following is an overview of Amazon FSx for NetApp ONTAP file system performance, with a discussion of the available performance and throughput options and useful performance tips.

**Topics**



## Overview

File system performance is measured by its latency, throughput, and I/O operations per second (IOPS).

### Latency

Amazon FSx for NetApp ONTAP provides sub-millisecond file operation latencies with solid state drive (SSD) storage, and tens of milliseconds of latency for capacity pool storage. Above that, Amazon FSx has two layers of read caching on each file server—NVMe drives and in-memory—to provide even lower latencies when you access your most frequently-read data.

### Throughput and IOPS

Each Amazon FSx file system provides up to multiple GB/s of throughput and hundreds of thousands of IOPS. The specific amount of throughput and IOPS that your workload can drive on your file system depends on the throughput capacity and storage capacity configuration of your file system, along with the nature of your workload, including the size of the active working set.

### SMB Multichannel and NFS nconnect support

With Amazon FSx, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. SMB Multichannel uses multiple network connections between the client and server simultaneously to aggregate network bandwidth for maximal utilization. For information on using the NetApp ONTAP CLI to configure SMB Multichannel, see Configuring SMB Multichannel for performance and redundancy.

NFS clients can use the `nconnect` mount option to have multiple TCP connections (up to 16) associated with a single NFS mount. Such an NFS client multiplexes file operations onto multiple TCP connections in a round-robin fashion and thus obtains higher throughput from the available network bandwidth. See your NFS client documentation to confirm whether `nconnect` is supported in your client version. For more information about NetApp ONTAP support for `nconnect`, see ONTAP support for NFSv4.1.

## Performance details

To understand the Amazon FSx for NetApp ONTAP performance model in detail, you can examine the architectural components of an Amazon FSx file system. Your client compute instances, whether they

exist in AWS or on-premises, access your file system through one or multiple elastic network interfaces (ENI). These network interfaces reside in the Amazon VPC that you associate with your file system. Behind each file system ENI is an NetApp ONTAP file server that is serving data over the network to the clients accessing the file system. Amazon FSx provides a fast in-memory cache and NVMe cache on each file server to enhance performance for the most frequently accessed data. Attached to each file server are the disks hosting your file system data.

Corresponding with these architectural components–network interface, in-memory cache, NVMe cache, and storage volumes–are the primary performance characteristics of an Amazon FSx for NetApp ONTAP file system that determine the overall throughput and IOPS performance.

- Network I/O performance: throughput/IOPS of requests between the clients and the file server (in aggregate)
- In-memory and NVMe cache size on the file server: size of active working set that can be accommodated for caching
- Disk I/O performance: throughput/IOPS of requests between the file server and the storage disks

There are two factors that determine these performance characteristics for your file system: the amount of SSD IOPS and throughput capacity that you configure for it. The first two performance characteristics – network I/O performance and in-memory and NVMe cache size – are solely determined by throughput capacity, while the third one – disk I/O performance – is determined by a combination of throughput capacity and SSD IOPS.

File-based workloads are typically spiky, characterized by short, intense periods of high I/O with plenty of idle time between bursts. To support spiky workloads, in addition to the baseline speeds that a file system can sustain 24/7, Amazon FSx provides the capability to burst to higher speeds for periods of time for both network I/O and disk I/O operations. Amazon FSx uses a network I/O credit mechanism to allocate throughput and IOPS based on average utilization — file systems accrue credits when their throughput and IOPS usage is below their baseline limits, and can use these credits when they perform I/O operations.

# Impact of storage capacity on performance

The maximum disk throughput and IOPS levels your file system can achieve is the lower of:

- the disk performance level provided by your file server, based on the throughput capacity you select for your file system
- the disk performance level provided by the number of SSD IOPS you provision for your file system

By default, your file system's SSD storage provides the following levels of disk throughput and IOPS:

- Disk throughput (MB/s per TiB of storage): 750
- Disk IOPS (IOPs per TiB of storage): 3,000

You can optionally provision a higher level of SSD IOPS when creating your file system.

# Impact of throughput capacity on performance

Every Amazon FSx file system has a throughput capacity that you configure when the file system is created. The throughput capacity determines the level of network I/O performance, that is, the speed at which the file server hosting your file system can serve file data over the network to clients accessing it. Higher levels of throughput capacity come with more memory and NVMe storage for caching data on the file server, and higher levels of disk I/O performance supported by the file server.

The following table shows the full set of specifications for throughput capacity, along with baseline and burst levels, and amount of memory for caching on the file server.

| FSx throughput capacity (MBps) | Network throughput capacity (MBps) | | Network IOPS | In-memory caching (GB) | NVMe caching (GB) | Disk throughput (MBps) | | SSD drive IOPS * | |
|---|---|---|---|---|---|---|---|---|---|
| | Baseline | Burst | | | | Baseline | Burst | Baseline | Burst |
| 512 | 625 | 1,250 | Hundreds of thousands baseline | 32 | 600 | 512 | 600 | 18,750 | Tens of thousands baseline |
| 1,024 | 1,500 | – | | 64 | 1200 | 1,024 | – | 40,000 | |
| 2,048 | 3,125 | – | | 128 | 2400 | 2,048 | – | 80,000 | |

**Note**
* Your SSD IOPS are only used when you access data that is not cached in your file server's in-memory cache or NVMe cache.

# Example: storage capacity and throughput capacity

The following example illustrates how storage capacity and throughput capacity impact file system performance.

A file system that is configured with 2 TiB of SSD storage capacity and 512 MBps of throughput capacity has the following throughput levels:

- Network throughput – 625 MBps baseline and 1,250 MBps burst (see throughput capacity table)
- Disk throughput – 512 MBps baseline and 600 MBps burst.

Your workload accessing the file system will therefore be able to drive up to 512 MBps baseline and 600 MBps burst throughput for file operations performed on actively accessed data cached in the file server in-memory cache and NVMe cache.

# Security in Amazon FSx for NetApp ONTAP

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon FSx for NetApp ONTAP, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon FSx. The following topics show you how to configure Amazon FSx to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon FSx resources.

**Topics**



# Data protection in Amazon FSx for NetApp ONTAP

The AWS shared responsibility model applies to data protection in Amazon FSx for NetApp ONTAP. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.

- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Amazon FSx or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

# Data encryption in FSx for ONTAP

Amazon FSx for NetApp ONTAP supports encryption of data at rest and encryption of data in transit. Encryption of data at rest is automatically enabled when creating an Amazon FSx file system. Encryption of data in transit is supported on file shares that are mapped on a compute instance that supports SMB protocol 3.0 or newer. When enabled, Amazon FSx supports encryption of data in transit using SMB encryption as you access your file system without the need for you to modify your applications.

## When to use encryption

If your organization is subject to corporate or regulatory policies that require encryption of data and metadata at rest, your data is automatically encrpyted at rest, and we recommend enabling encryption of data in transit by mounting your file system using encryption of data in transit.

For more information on encryption with Amazon FSx for NetApp ONTAP, see these related topics:

- Getting started: Create your Amazon FSx for NetApp ONTAP file system (p. 12)
- Creating Amazon FSx file systems (p. 37)

### Encryption at rest

All Amazon FSx file systems are encrypted at rest with keys managed using AWS Key Management Service (AWS KMS). Data is automatically encrypted before being written to the file system, and automatically decrypted as it is read. These processes are handled transparently by Amazon FSx, so you don't have to modify your applications.

Amazon FSx uses an industry-standard AES-256 encryption algorithm to encrypt Amazon FSx data and metadata at rest. For more information, see Cryptography Basics in the *AWS Key Management Service Developer Guide*.

> **Note**
> The AWS key management infrastructure uses Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms. The infrastructure is consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations.

#### How Amazon FSx uses AWS KMS

Amazon FSx integrates with AWS KMS for key management. Amazon FSx uses KMS keys to encrypt your file system. You choose the KMS key used to encrypt and decrypt file systems (both data and metadata).

You can enable, disable, or revoke grants on this KMS key. This KMS key can be one of the two following types:

- **AWS-managed KMS key** – This is the default KMS key, and it's free to use.
- **Customer-managed KMS key** – This is the most flexible KMS key to use, because you can configure its key policies and grants for multiple users or services. For more information on creating KMS keys, see Creating Keys in the *AWS Key Management Service Developer Guide*.

If you use a customer-managed KMS key as your KMS key for file data encryption and decryption, you can enable key rotation. When you enable key rotation, AWS KMS automatically rotates your key once per year. Additionally, with a customer-managed KMS key, you can choose when to disable, re-enable, delete, or revoke access to your KMS key at any time. For more information, see Rotating AWS KMS keys in the *AWS Key Management Service Developer Guide.*

File system encryption and decryption at rest are handled transparently. However, AWS account IDs specific to Amazon FSx appear in your AWS CloudTrail logs related to AWS KMS actions.

### Amazon FSx key policies for AWS KMS

Key policies are the primary way to control access to KMS keys. For more information on key policies, see Using key policies in AWS KMS in the *AWS Key Management Service Developer Guide.* The following list describes all the AWS KMS-related permissions supported by Amazon FSx for encrypted at rest file systems:

- **kms:Encrypt** – (Optional) Encrypts plaintext into ciphertext. This permission is included in the default key policy.
- **kms:Decrypt** – (Required) Decrypts ciphertext. Ciphertext is plaintext that has been previously encrypted. This permission is included in the default key policy.
- **kms:ReEncrypt** – (Optional) Encrypts data on the server side with a new AWS KMS key, without exposing the plaintext of the data on the client side. The data is first decrypted and then re-encrypted. This permission is included in the default key policy.
- **kms:GenerateDataKeyWithoutPlaintext** – (Required) Returns a data encryption key encrypted under a KMS key. This permission is included in the default key policy under **kms:GenerateDataKey***.
- **kms:CreateGrant** – (Required) Adds a grant to a key to specify who can use the key and under what conditions. Grants are alternate permission mechanisms to key policies. For more information on grants, see Using Grants in the *AWS Key Management Service Developer Guide.* This permission is included in the default key policy.
- **kms:DescribeKey** – (Required) Provides detailed information about the specified KMS key. This permission is included in the default key policy.
- **kms:ListAliases** – (Optional) Lists all of the key aliases in the account. When you use the console to create an encrypted file system, this permission populates the list of KMS keys. We recommend using this permission to provide the best user experience. This permission is included in the default key policy.

## Encryption in transit

Encryption of data in transit is supported on file shares that are mapped on a compute instance that supports SMB protocol 3.0 or newer. This includes all Microsoft Windows versions starting from Windows Server 2012 and Windows 8. When enabled, FSx for ONTAP automatically encrypts data in transit using SMB encryption as you access your file system without the need for you to modify your applications.

SMB encryption uses AES-128-GCM or AES-128-CCM (with the GCM variant being chosen if the client supports SMB 3.1.1) as its encryption algorithm, and also provides data integrity with signing using SMB Kerberos session keys. The use of AES-128-GCM leads to better performance, for example, up to a 2x performance improvement when copying large files over encrypted SMB connections.

# Identity and Access Management for Amazon FSx for NetApp ONTAP

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon FSx resources. IAM is an AWS service that you can use with no additional charge.

**Topics**



## Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon FSx.

**Service user** – If you use the Amazon FSx service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon FSx features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon FSx, see Troubleshooting Amazon FSx for NetApp ONTAP identity and access (p. 90).

**Service administrator** – If you're in charge of Amazon FSx resources at your company, you probably have full access to Amazon FSx. It's your job to determine which Amazon FSx features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon FSx, see How Amazon FSx for NetApp ONTAP works with IAM (p. 84).

**IAM administrator** – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon FSx. To view example Amazon FSx identity-based policies that you can use in IAM, see Identity-based policy examples for Amazon FSx for NetApp ONTAP (p. 88).

## Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google

or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

## AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

## IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

## IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as

*federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.

- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, resources, and condition keys for Amazon FSx for NetApp ONTAP in the *Service Authorization Reference*.
  - **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
  - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

# Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

## Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

## Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

## Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

## Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the *AWS Organizations User Guide*.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

## Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

# How Amazon FSx for NetApp ONTAP works with IAM

Before you use IAM to manage access to Amazon FSx, learn what IAM features are available to use with Amazon FSx.

**IAM features you can use with Amazon FSx for NetApp ONTAP**

| IAM feature | Amazon FSx support |
|---|---|
| Identity-based policies (p. 84) | Yes |
| Resource-based policies (p. 85) | No |
| Policy actions (p. 85) | Yes |
| Policy resources (p. 86) | Yes |
| Policy condition keys (p. 86) | Yes |
| ACLs (p. 87) | No |
| ABAC (tags in policies) (p. 87) | Partial |
| Temporary credentials (p. 87) | Yes |
| Principal permissions (p. 88) | Yes |
| Service roles (p. 88) | Yes |
| Service-linked roles (p. 88) | Yes |

To get a high-level view of how Amazon FSx and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

# Identity-based policies for Amazon FSx

| | |
|---|---|
| Supports identity-based policies | Yes |

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform,

on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

### Identity-based policy examples for Amazon FSx

To view examples of Amazon FSx identity-based policies, see Identity-based policy examples for Amazon FSx for NetApp ONTAP (p. 88).

## Resource-based policies within Amazon FSx

| | |
|---|---|
| Supports resource-based policies | No |

## Policy actions for Amazon FSx

| | |
|---|---|
| Supports policy actions | Yes |

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon FSx actions, see Actions defined by Amazon FSx for NetApp ONTAP in the *Service Authorization Reference*.

Policy actions in Amazon FSx use the following prefix before the action:

```
fsx
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

To view examples of Amazon FSx identity-based policies, see Identity-based policy examples for Amazon FSx for NetApp ONTAP (p. 88).

## Policy resources for Amazon FSx

| | |
|---|---|
| Supports policy resources | Yes |

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of Amazon FSx resource types and their ARNs, see Resources defined by Amazon FSx for NetApp ONTAP in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions defined by Amazon FSx for NetApp ONTAP.

To view examples of Amazon FSx identity-based policies, see Identity-based policy examples for Amazon FSx for NetApp ONTAP (p. 88).

## Policy condition keys for Amazon FSx

| | |
|---|---|
| Supports policy condition keys | Yes |

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Amazon FSx condition keys, see Condition keys for Amazon FSx for NetApp ONTAP in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions defined by Amazon FSx for NetApp ONTAP.

To view examples of Amazon FSx identity-based policies, see Identity-based policy examples for Amazon FSx for NetApp ONTAP (p. 88).

## Access control lists (ACLs) in Amazon FSx

| | |
|---|---|
| Supports ACLs | No |

## Attribute-based access control (ABAC) with Amazon FSx

| | |
|---|---|
| Supports ABAC (tags in policies) | Partial |

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

For more information about ABAC, see What is ABAC? in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

For more information about tagging Amazon FSx resources, see Tag your Amazon FSx resources (p. 52).

To view an example identity-based policy for limiting access to a resource based on the tags on that resource, see Using tags to control access to your Amazon FSx resources (p. 93).

## Using Temporary credentials with Amazon FSx

| | |
|---|---|
| Supports temporary credentials | Yes |

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switching to a role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

## Cross-service principal permissions for Amazon FSx

| | |
|---|---|
| Supports principal permissions | Yes |

When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, resources, and condition keys for Amazon FSx for NetApp ONTAP in the *Service Authorization Reference*.

## Service roles for Amazon FSx

| | |
|---|---|
| Supports service roles | Yes |

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
> Changing the permissions for a service role might break Amazon FSx functionality. Edit service roles only when Amazon FSx provides guidance to do so.

## Service-linked roles for Amazon FSx

| | |
|---|---|
| Supports service-linked roles | Yes |

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Amazon FSx service-linked roles, see Using service-linked roles for Amazon FSx (p. 95).

# Identity-based policy examples for Amazon FSx for NetApp ONTAP

By default, IAM users and roles don't have permission to create or modify Amazon FSx resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform actions on the resources that they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating policies on the JSON tab in the *IAM User Guide*.

**Topics**

- Allow users to view their own permissions (p. 89)

## Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Amazon FSx resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started using AWS managed policies** – To start using Amazon FSx quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

## Using the Amazon FSx console

To access the Amazon FSx for NetApp ONTAP console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon FSx resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

To ensure that users and roles can still use the Amazon FSx console, also attach the `AmazonFSxConsoleReadOnlyAccess` AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

You can see the `AmazonFSxConsoleReadOnlyAccess` and other Amazon FSx managed service policies in AWS managed policies for Amazon FSx (p. 98).

## Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

# Troubleshooting Amazon FSx for NetApp ONTAP identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon FSx and IAM.

**Topics**



## I am not authorized to perform an action in Amazon FSx

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but does not have the fictional `fsx:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

In this case, Mateo asks his administrator to update his policies to allow him to access the *`my-example-widget`* resource using the `fsx:`*`GetWidget`* action.

## I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Amazon FSx.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon FSx. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

## I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

## I'm an administrator and want to allow others to access Amazon FSx

To allow others to access Amazon FSx, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon FSx.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

## I want to allow people outside of my AWS account to access my Amazon FSx resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon FSx supports these features, see How Amazon FSx for NetApp ONTAP works with IAM (p. 84).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.

# Using tags with Amazon FSx

You can use tags to control access to Amazon FSx resources and to implement attribute-based access control (ABAC). Users need to have permission to apply tags to Amazon FSx resources during creation.

## Grant permission to tag resources during creation

Some resource-creating Amazon FSx API actions enable you to specify tags when you create the resource. You can use resource tags to implement attribute-based access control (ABAC). For more information, see What is ABAC for AWS in the *IAM User Guide*.

To enable users to tag resources on creation, they must have permissions to use the action that creates the resource, such as `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine` or `fsx:CreateVolume`. If tags are specified in the resource-creating action, Amazon performs additional authorization on the `fsx:TagResource` action to verify if users have permissions to create tags. Therefore, users must also have explicit permissions to use the `fsx:TagResource` action.

The following example demonstrates a policy that allows users to create file systems and storage virtual machines (SVMs) and apply tags to them during creation in a specific AWS account.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

Similarly, the following policy allows users to create backups on a specific file system and apply any tags to the backup during backup creation.

```
{
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

The `fsx:TagResource` action is only evaluated if tags are applied during the resource-creating action. Therefore, a user that has permissions to create a resource (assuming there are no tagging conditions) does not require permissions to use the `fsx:TagResource` action if no tags are specified in the request. However, if the user attempts to create a resource with tags, the request fails if the user does not have permissions to use the `fsx:TagResource` action.

For more information about tagging Amazon FSx resources, see *Tagging resources*. For more information about using tags to control access to FSx resources, see Using tags to control access to your Amazon FSx resources (p. 93).

# Using tags to control access to your Amazon FSx resources

To control access to Amazon FSx resources and actions, you can use AWS Identity and Access Management (IAM) policies based on tags. You can provide the control in two ways:

1. Control access to Amazon FSx resources based on the tags on those resources.
2. Control what tags can be passed in an IAM request condition.

For information about how to use tags to control access to AWS resources, see Controlling access using tags in the *IAM User Guide*. For more information about tagging Amazon FSx resources at creation, see Grant permission to tag resources during creation (p. 92). For more information about tagging resources, see Tag your Amazon FSx resources (p. 52).

## Controlling access based on tags on a resource

To control what actions a user or role can perform on an Amazon FSx resource, you can use tags on the resource. For example, you might want to allow or deny specific API operations on a file system resource based on the key-value pair of the tag on the resource.

**Example Example policy – Create a file system on when providing a specific tag**

This policy allows the user to create a file system only when they tag it with a specific tag key value pair, in this example, `key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
```

```
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

### Example Example policy – Create backups only of FSx for ONTAP volumes with a specific tag

This policy allows users to create backups only of FSx for ONTAP volumes that are tagged with the key value pair `key=Department, value=Finance`, and the backup will be created with the tag `Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:/file-system/*/volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

### Example Example policy – Create a volume with a specific tag from backups with a specific tag

This policy allows users to create volumes that are tagged with `Department=Finance` only from backups that are tagged with `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*/volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

**Example Example policy – Delete file systems with specific tags**

This policy allows a user to delete only file systems that are tagged with `Department=Finance`. If they create a final backup, then it must be tagged with `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

# Using service-linked roles for Amazon FSx

Amazon FSx uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon FSx. Service-linked roles are predefined by Amazon FSx and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon FSx easier because you don't have to manually add the necessary permissions. Amazon FSx defines the permissions of its service-linked roles, and unless defined

otherwise, only Amazon FSx can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon FSx resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

## Service-linked role permissions for Amazon FSx

Amazon FSx uses the service-linked role named **AWSServiceRoleForAmazonFSx** – Which performs certain actions in your account, like creating Elastic Network Interfaces for your file systems in your VPC.

The role permissions policy allows Amazon FSx to complete the following actions on the all applicable AWS resources:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData",
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

## Creating a service-linked role for Amazon FSx

You don't need to manually create a service-linked role. When you create a file system in the AWS Management Console, the IAM CLI, or the IAM API, Amazon FSx creates the service-linked role for you.

> **Important**
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. To learn more, see A New Role Appeared in My IAM Account.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a file system, Amazon FSx creates the service-linked role for you again.

## Editing a service-linked role for Amazon FSx

Amazon FSx does not allow you to edit the AWSServiceRoleForAmazonFSx service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

## Deleting a service-linked role for Amazon FSx

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must delete all of your file systems and backups before you can manually delete the service-linked role.

> **Note**
> If the Amazon FSx service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

**To manually delete the service-linked role using IAM**

Use the IAM console, the IAM CLI, or the IAM API to delete the AWSServiceRoleForAmazonFSx service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

## Supported regions for Amazon FSx service-linked roles

Amazon FSx supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.

# AWS managed policies for Amazon FSx

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

# AWS managed policy: AmazonFSxFullAccess

You can attach AmazonFSxFullAccess to your IAM entities. Amazon FSx also attaches this policy to a service role that allows Amazon FSx to perform actions on your behalf.

Provides full access to Amazon FSx and access to related AWS services.

**Permissions details**

This policy includes the following permissions.

- `fsx` – Allows principals full access to perform all Amazon FSx actions.
- `ds` – Allows principals to view information about the AWS Directory Service directories.
- `iam` – Allows principles to create an Amazon FSx service linked role on the user's behalf. This is required so that Amazon FSx can manage AWSresources on the user's behalf.
- `logs` – Allows principals to create log groups, log streams, and write events to log streams. This is required so that users can monitor FSx for Windows File Server file system access by sending audit access logs to CloudWatch Logs.
- `firehose` – Allows principals to write records to a Amazon Kinesis Data Firehose. This is required so that users can monitor FSx for Windows File Server file system access by sending audit access logs to Kinesis Data Firehose.
- `ec2` – Allows principals to create tags under the specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "fsx:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "s3.data-source.lustre.fsx.amazonaws.com"
```

```
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/fsx/*:log-group:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "firehose:PutRecord"
            ],
            "Resource": [
                "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonFSx": "ManagedByAmazonFSx"
                },
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": ["fsx.amazonaws.com"]
                }
            }
        }
    ]
}
```

# AWS managed policy: AmazonFSxConsoleFullAccess

You can attach the `AmazonFSxConsoleFullAccess` policy to your IAM identities.

This policy grants administrative permissions that allow full access to Amazon FSx and access to related AWS services via the AWS Management Console.

**Permissions details**

This policy includes the following permissions.

- `fsx` – Allows principals to perform all actions in the Amazon FSx management console.
- `cloudwatch` – Allows principals to view CloudWatch Alarms in the Amazon FSx management console.
- `ds` – Allows principals to list information about an AWS Directory Service directory.
- `ec2` – Allows principals to create tags on route tables, list network interfaces, route tables, security groups, subnets and the VPC associated with an Amazon FSx file system.

- `kms` – Allows principals to list aliases for AWS Key Management Service keys.
- `s3` – Allows principals to list some or all of the objects in an Amazon S3 bucket (up to 1000).
- `iam` – Grants permission to create a service linked role that allows Amazon FSx to perform actions on the user's behalf.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "ds:DescribeDirectories",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "firehose:ListDeliveryStreams",
                "fsx:*",
                "kms:ListAliases",
                "logs:DescribeLogGroups",
                "s3:ListBucket"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "s3.data-source.lustre.fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonFSx": "ManagedByAmazonFSx"
                },
                "ForAnyValue:StringEquals": {
```

```
                    "aws:CalledVia": ["fsx.amazonaws.com"]
                }
            }
        }
    ]
}
```

# AWS managed policy: AmazonFSxConsoleReadOnlyAccess

You can attach the `AmazonFSxConsoleReadOnlyAccess` policy to your IAM identities.

This policy grants read-only permissions to Amazon FSx and related AWS services so that users can view information about these services in the AWS Management Console.

**Permissions details**

This policy includes the following permissions.

- `fsx` – Allows principals to view information about Amazon FSx file systems, including all tags, in the Amazon FSx Management Console.
- `cloudwatch` – Allows principals to view CloudWatch Alarms in the Amazon FSx Management Console.
- `ds` – Allows principals to view information about an AWS Directory Service directory in the Amazon FSx Management Console.
- `ec2` – Allows principals to view network interfaces, security groups, subnets and the VPC associated with an Amazon FSx file system in the Amazon FSx Management Console.
- `kms` – Allows principals to view aliases for AWS Key Management Service keys in the Amazon FSx Management Console.
- `log` – Allows principals to describe the Amazon CloudWatch Logs log groups associated with the account making the request. This is required so that principals can view the existing file access auditing configuration for an FSx for Windows File Server file system.
- `firehose` – Allows principals to describe the Amazon Kinesis Data Firehose delivery streams associated with the account making the request. This is required so that principals can view the existing file access auditing configuration for an FSx for Windows File Server file system.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "ds:DescribeDirectories",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "firehose:ListDeliveryStreams",
                "fsx:Describe*",
                "fsx:ListTagsForResource",
                "kms:DescribeKey",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

# Amazon FSx updates to AWS managed policies

View details about updates to AWS managed policies for Amazon FSx since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon FSx Document History for Amazon FSx for NetApp ONTAP (p. 115) page.

| Change | Description | Date |
|---|---|---|
| AmazonFSxServiceRolePolicy (p. 96) – Update to an existing policy | Amazon FSx added new permisions to allow Amazon FSx to manage network configurations for Amazon FSx for NetApp ONTAP file systems. | September 2, 2021 |
| AmazonFSxFullAccess (p. 99) – Update to an existing policy | Amazon FSx added new permisions to allow Amazon FSx to create tags on EC2 route tables for scoped down calls. | September 2, 2021 |
| AmazonFSxConsoleFullAccess (p. 100) – Update to an existing policy | Amazon FSx added new permissions to allow Amazon FSx to create Amazon FSx for NetApp ONTAP Multi-AZ file systems. | September 2, 2021 |
| AmazonFSxConsoleFullAccess (p. 100) – Update to an existing policy | Amazon FSx added new permisions to allow Amazon FSx to create tags on EC2 route tables for scoped down calls. | September 2, 2021 |
| AmazonFSxServiceRolePolicy (p. 96) – Update to an existing policy | Amazon FSx added new permissions to allow Amazon FSx to describe and write to CloudWatch Logs log streams.<br><br>This is required so that users can view file access audit logs for FSx for Windows File Server file systems using CloudWatch Logs. | June 8, 2021 |
| AmazonFSxServiceRolePolicy (p. 96) – Update to an existing policy | Amazon FSx added new permissions to allow Amazon FSx to describe and write to Amazon Kinesis Data Firehose delivery streams.<br><br>This is required so that users can view file access audit logs for an FSx for Windows File Server file system using Amazon Kinesis Data Firehose. | June 8, 2021 |
| AmazonFSxFullAccess (p. 99) – Update to an existing policy | Amazon FSx added new permissions to allow principals | June 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| | to describe and create CloudWatch Logs log groups, log streams, and write events to log streams.<br><br>This is required so that principals can view file access audit logs for FSx for Windows File Server file systems using CloudWatch Logs. | |
| AmazonFSxFullAccess (p. 99) – Update to an existing policy | Amazon FSx added new permissions to allow principals to describe and write records to a Amazon Kinesis Data Firehose.<br><br>This is required so that users can view file access audit logs for an FSx for Windows File Server file system using Amazon Kinesis Data Firehose. | June 8, 2021 |
| AmazonFSxConsoleFullAccess (p. 100) – Update to an existing policy | Amazon FSx added new permissions to allow principals to describe the Amazon CloudWatch Logs log groups associated with the account making the request.<br><br>This is required so that principals can choose an existing CloudWatch Logs log group when configuring file access auditing for an FSx for Windows File Server file system. | June 8, 2021 |
| AmazonFSxConsoleFullAccess (p. 100) – Update to an existing policy | Amazon FSx added new permissions to allow principals to describe the Amazon Kinesis Data Firehose delivery streams associated with the account making the request.<br><br>This is required so that principals can choose an existing Kinesis Data Firehose delivery stream when configuring file access auditing for an FSx for Windows File Server file system. | June 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AmazonFSxConsoleReadOnlyAccess (p. 102) – Update to an existing policy | Amazon FSx added new permissions to allow principals to describe the Amazon CloudWatch Logs log groups associated with the account making the request.<br><br>This is required so that principals can view the existing file access auditing configuration for an FSx for Windows File Server file system. | June 8, 2021 |
| AmazonFSxConsoleReadOnlyAccess (p. 102) – Update to an existing policy | Amazon FSx added new permissions to allow principals to describe the Amazon Kinesis Data Firehose delivery streams associated with the account making the request.<br><br>This is required so that principals can view the existing file access auditing configuration for an FSx for Windows File Server file system. | June 8, 2021 |
| Amazon FSx started tracking changes | Amazon FSx started tracking changes for its AWS managed policies. | June 8, 2021 |

# File System Access Control with Amazon VPC

You access your Amazon FSx for NetApp ONTAP file systems and SVMs using the DNS name or the IP address of one of their endpoints, depending on what type of access it is. The DNS name maps to the private IP address of the file system's or SVM's elastic network interface in your VPC. Only resources within the associated VPC, resources connected with the associated VPC by AWS Direct Connect or VPN can access your file system's network interface. For more information, see What is Amazon VPC? in the *Amazon VPC User Guide*.

**Warning**
You must not modify or delete the elastic network interface(s) associated with your file system. Modifying or deleting the network interface can cause a permanent loss of connection between your VPC and your file system.

## Amazon VPC security groups

A security group acts as a virtual firewall for your FSx for ONTAP file systems to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your file system, and outbound rules control the outgoing traffic from your file system. When you create a file system, you specify the VPC that it gets created in, and the default security group for that VPC is applied. You can add rules to each security group that allow traffic to or from its associated file systems and SVMs. You can modify the rules for a security group at any time. New and modified rules are automatically applied to all resources that are associated with the security group. When Amazon FSx decides whether to allow traffic to reach a resource, it evaluates all of the rules from all of the security groups that are associated with the resource.

To use a security group to control access to your Amazon FSx file system, add inbound and outbound rules. Inbound rules control incoming traffic, and outbound rules control outgoing traffic from your file system. Make sure that you have the right network traffic rules in your security group to map your Amazon FSx file system's file share to a folder on your supported compute instance.

For more information on security group rules, see Security Group Rules in the *Amazon EC2 User Guide for Linux Instances.*

## Creating a VPC security group

**To create a security group for Amazon FSx**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2.
2. In the navigation pane, choose **Security Groups**.
3. Choose **Create Security Group**.
4. Specify a name and description for the security group.
5. For **VPC**, choose the Amazon VPC associated with your file system to create the security group within that VPC.
6. For outbound rules, allow all traffic on all ports.
7. Add the following rules to the inbound ports of your security group.

| Protocol | Ports | Role |
|---|---|---|
| All ICMP | All | Pinging the instance |
| SSH | 22 | SSH access to the IP address of the cluster management LIF or a node management LIF |
| TCP | 111 | Remote procedure call for NFS |
| TCP | 139 | NetBIOS service session for CIFS |
| TCP | 161-162 | Simple network management protocol (SNMP) |
| TCP | 443 | ONTAP REST API access to the IP address of the cluster management LIF or an SVM management LIF |
| TCP | 445 | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| TCP | 635 | NFS mount |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS server daemon |
| TCP | 3260 | iSCSI access through the iSCSI data LIF |
| TCP | 4045 | NFS lock daemon |
| TCP | 4046 | Network status monitor for NFS |
| TCP | 11104 | Management of intercluster communication sessions for SnapMirror |
| TCP | 11105 | SnapMirror data transfer using intercluster LIFs |
| UDP | 111 | Remote procedure call for NFS |

| Protocol | Ports | Role |
|---|---|---|
| UDP | 139 | NetBIOS service session for CIFS |
| UDP | 161-162 | Simple network management protocol (SNMP) |
| UDP | 635 | NFS mount |
| UDP | 2049 | NFS server daemon |
| UDP | 4045 | NFS lock daemon |
| UDP | 4046 | Network status monitor for NFS |
| UDP | 4049 | NFS rquotad protocol |

### Disallow access to a file system

To temporarily disallow network access to your file system from all clients, you can remove all the security groups associated with your file system's elastic network interface(s) and replace them with a group that has no inbound/outbound rules.

# Compliance Validation for Amazon FSx for NetApp ONTAP

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether Amazon FSx or other AWS services are in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance Whitepaper – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

  **Note**
  Not all services are compliant with HIPAA.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

# Resilience in Amazon FSx for NetApp ONTAP

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Amazon FSx offers several features to help support your data resiliency and backup needs.

## Backup and restore

Amazon FSx creates and saves automated backups of the volumes in your Amazon FSx for NetApp ONTAP file system. Amazon FSx creates automated backups of your volumes during the backup window of your Amazon FSx for NetApp ONTAP file system. Amazon FSx saves the automated backups of your volumes according to the backup retention period that you specify. You can also back up your volumes manually, by creating a user-initiated backup. You restore a volume backup at any time by creating a new volume with the backup specified as the source.

For more information, see Working with backups (p. 29).

## Snapshots

Amazon FSx creates snapshot copies of the Amazon FSx for NetApp ONTAP volumes. Snapshot copies offer protection against accidental deletion or modification of files in your volumes by end users. For more information, see Working with snapshots (p. 34).

## Multi-AZ file systems

Amazon FSx for NetApp ONTAP file systems are highly available and durable across AWS Availability Zones, and are designed to provide continuous availability to data even in the event that an availability zone is unavailable. Each file system is powered by two file servers in separate availability zones, each with its own storage. Amazon FSx automatically replicates your data across availability zones to protect it from component failure, continuously monitors for hardware failures, and automatically replaces infrastructure components in the event of a failure. File systems automatically fail over and back as needed (typically within 60 seconds), and clients automatically fail over and back with the file system.

For more information, see Availability and durability (p. 27).

# Infrastructure security in Amazon FSx for NetApp ONTAP

As a managed service, Amazon FSx for NetApp ONTAP is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Amazon FSx through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

# Quotas

Following, you can find out about quotas when working with Amazon FSx for NetApp ONTAP.

**Topics**



## Quotas that you can increase

Following are the quotas for Amazon FSx for NetApp ONTAP for each AWS account, per AWS Region, that you can increase.

| Resource | Default | Description |
|---|---|---|
| ONTAP file systems | 100 | The maximum number of Amazon FSx for NetApp ONTAP file systems that you can create in this account. |
| ONTAP SSD storage capacity | 524,288 | The maximum amount of SSD storage capacity (in GiB) for all Amazon FSx for NetApp ONTAP file systems that you can have in this account. |
| ONTAP throughput capacity | 10,240 | The maximum amount of throughput capacity (in MBps) for all Amazon FSx for NetApp ONTAP file systems that you can have in this account. |
| ONTAP SSD IOPS | 1,000,000 | The maximum amount of SSD IOPS for all Amazon FSx for NetApp ONTAP file systems that you can have in this account. |
| ONTAP backups | 10,000 | The maximum number of user-initiated volume backups for all Amazon FSx for NetApp ONTAP file systems that you can have in this account. |

### To request a quota increase

1. Open the AWS Support page, sign in if necessary, and then choose **Create case**.
2. For **Create case**, choose **Account and billing support**.
3. In the **Case details** panel make the following entries:

   - For **Type** choose **Account**.

- For **Category** choose **Other Account Issues**.
- For **Subject** enter **`Amazon FSx for NetApp ONTAP service limit increase request`**.
- Provide a detailed **Description** of your request, including:
  - The FSx quota that you want increased, and the value you want it increased to, if known.
  - The reason why you are seeking the quota increase.
  - The file system ID and region for each file system you are requesting an increase for.

4. Provide your preferred **Contact options** and choose **Submit**.

# Resource quotas for each file system

Following are the quotas on Amazon FSx for NetApp ONTAP resources for each file system in an AWS Region.

| Resource | Limit per file system |
|---|---|
| Minimum storage capacity | 1024 GiB |
| Maximum storage capacity | 192 TiB |
| Minimum throughput capacity | 512 MBps |
| Maximum throughput capacity | 2,048 MBps |
| Maximum number of volumes | 500 |
| Maximum number of SVMs | • 14 (512 MBps throughput capacity)<br>• 14 (1024 MBps throughput capacity)<br>• 24 (2048 MBps throughput capacity) |
| Maximum number of tags | 50 |
| Maximum retention period for automated backups | 90 days |
| Maximum retention period for user-initiated backups | no retention limit |

# Additional information

This section provides a reference of additional supported Amazon FSx features.

**Topics**



# Setting up a Harvest and Grafana environment

You can monitor your Amazon FSx for NetApp ONTAP file system by using Harvest and Grafana. NetApp Harvest monitors ONTAP datacenters by collecting performance, capacity, and hardware metrics from FSx for ONTAP file systems. Grafana provides a dashboard where the collected Harvest metrics can be displayed.

To get started, you can deploy an AWS CloudFormation template that automatically launches an Amazon EC2 instance running Harvest and Grafana. As an input to the AWS CloudFormation template, you specify the `fsxadmin` user and the Amazon FSx management endpoint for the file system which will be added as part of this deployment. After the deployment is completed, you can log in to the Grafana dashboard to monitor your file system.

## AWS CloudFormation template

This solution uses AWS CloudFormation to automate the deployment of the Harvest and Grafana solution. The template creates an Amazon EC2 Linux instance and installs Harvest and Grafana software. To use this solution, download the fsx-ontap-harvest-grafana.template AWS CloudFormation template.

> **Note**
> Implementing this solution incurs billing for the associated AWS services. For more information, see the pricing details pages for those services.

## Amazon EC2 instance types

When configuring the template, you provide the Amazon EC2 instance type. NetApp's recommendation for the instance size depends on how many file systems you monitor and the number of metrics you choose to collect. With the default configuration, for each 10 file systems you monitor, NetApp recommends:

- CPU: 2 cores
- Memory: 1 GB
- Disk: 500 MB (mostly used by log files)

Following are some sample configurations and the `t3` instance type you might choose.

| File systems | CPU | Disk | Instance type |
|---|---|---|---|
| Under 10 | 2 cores | 500 MB | `t3.micro` |
| 10–40 | 4 cores | 1000 MB | `t3.xlarge` |

| File systems | CPU | Disk | Instance type |
|---|---|---|---|
| 40+ | 8 cores | 2000 MB | `t3.2xlarge` |

For more information on Amazon EC2 instance types, see General purpose instances in the *Amazon EC2 User Guide for Linux Instances*.

# Deployment procedure

The following procedure configures and deploys the Harvest/Grafana solution. It takes about five minutes to deploy. Before you start, you must have an FSx for ONTAP file system running in an Amazon Virtual Private Cloud (Amazon VPC) in your AWS account, and the parameter information for the template listed below. For more information on creating a file system, see Creating FSx for ONTAP file systems (p. 37).

### To launch the Harvest/Grafana solution stack

1. Download the fsx-ontap-harvest-grafana.template AWS CloudFormation template. For more information on creating an AWS CloudFormation stack, see Creating a stack on the AWS CloudFormation console in the *AWS CloudFormation User Guide*.

   **Note**
   By default, this template launches in the US East (N. Virginia) AWS Region. You must launch this solution in an AWS Region where Amazon FSx is available. For more information, see Amazon FSx endpoints and quotas in the *AWS General Reference*.

2. For **Parameters**, review the parameters for the template and modify them for the needs of your file system. This solution uses the following default values.

| Parameter | Default | Description |
|---|---|---|
| InstanceType | `t3.micro` | The Amazon EC2 instance type. Following are the `t3` instance types.<br>• `t3.micro`<br>• `t3.small`<br>• `t3.medium`<br>• `t3.large`<br>• `t3.xlarge`<br>• `t3.2xlarge`<br>For the complete list of allowed Amazon EC2 instance type values for this parameter, see the fsx-ontap-harvest-grafana.template. |
| KeyPair | No default value | The key pair that is used to access the Amazon EC2 instance. |
| SecurityGroup | No default value | The Security group ID for the Harvest/Grafana Instance. Ensure Inbound ports 3000 |

| Parameter | Default | Description |
|---|---|---|
| | | and 9090 are open from the clients you wish to use to access your Grafana dashboard. |
| Subnet | No default value | Specify the same subnet as your Amazon FSx for NetApp ONTAP file system's preferred subnet. You can find the file system's **Preferred subnet** ID in the Amazon FSx console, in the **Network & security** tab of the FSx for ONTAP file system details page |
| LatestLinuxAmiId | `/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2` | The latest version of the Amazon Linux 2 AMI in a given AWS Region. |
| FSxEndPoint | No default value | The file system's Management endpoint IP address. You can find the file system's management endpoint **IP address** in the Amazon FSx console, in the **Administration** tab of the FSx for ONTAP file system details page. |
| SecretName | No default value | AWS Secrets Manager secret name containing the password for the file system's `fsxadmin` user. This is the password you provided when you created the file system. |

3. Choose **Next**.
4. For **Options**, choose **Next**.
5. For **Review**, review and confirm the settings. You must select the check box acknowledging that the template create IAM resources.
6. Choose **Create** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should see a status of **CREATE_COMPLETE** in about five minutes.

# Logging in to Grafana

After the deployment has finished, use your browser to log in to the Grafana dashboard at the IP and port 3000 of the Amazon EC2 instance:

```
http://EC2_instance_IP:3000
```

When prompted, use the Grafana default user name (`admin`) and password (`pass`). We recommend that you change your password as soon as you log in.

For more information, see Monitor all of your ONTAP clusters with Harvest on the NetApp website..

# Document History for Amazon FSx for NetApp ONTAP

The following table describes the documentation for this release of Amazon FSx for NetApp ONTAP.

- **API version:** 2018-03-01
- **Latest documentation update:** September 02, 2021

| Change | Description | Date |
| --- | --- | --- |
| Amazon FSx for NetApp ONTAP is now generally available | FSx for ONTAP provides NetApp ONTAP file systems that are fully managed, backed by a fully native Windows file system. Amazon FSx for NetApp ONTAP provides the features, performance, and compatibility to easily lift and shift enterprise applications to AWS. | September 02, 2021 |