NetApp

Amazon FSx for ONTAP documentation

Amazon FSx for ONTAP

NetApp
April 05, 2022

Table of Contents

Amazon FSx for ONTAP documentation

What's new with Amazon FSx for ONTAP

Learn what's new in Amazon FSx for ONTAP.

27 February 2022

Assume IAM role

When you create an FSx for ONTAP working environment, you now must provide the ARN of an IAM role that Cloud Manager can assume to create an FSx for ONTAP working environment. You previously needed to provide AWS access keys.

Learn how to set up permissions for FSx for ONTAP.

31 October 2021

Create iSCSI volumes using Cloud Manager API

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

Select volume units when creating volumes

You can select volume units (GiB or TiB) when creating volumes in FSx for ONTAP.

4 October 2021

Create CIFS volumes using Cloud Manager

Now you can create CIFS volumes in FSx for ONTAP using Cloud Manager.

Edit volumes using Cloud Manager

Now you can edit FSx for ONTAP volumes using Cloud Manager.

2 September 2021

Support for Amazon FSx for ONTAP

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

  Learn about Amazon FSx for ONTAP.

- You can configure an FSx for ONTAP working environment in Cloud Manager.

  Create an Amazon FSx for ONTAP working environment.

- Using a Connector in AWS and Cloud Manager, you can create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as Data Sense and Cloud Sync.

Get started with Cloud Data Sense for Amazon FSx for ONTAP.

Get started

Learn about Amazon FSx for ONTAP

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

Features

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

Additional features in Cloud Manager

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

Cost

Your FSx for ONTAP account is maintained by AWS and not by Cloud Manager. Amazon FSx for ONTAP getting started guide

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

Supported regions

View supported Amazon regions.

Getting help

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

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

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

Limitations

- Cloud Manager can replicate data only from on-premises or Cloud Volumes ONTAP to FSx for ONTAP.

- At this time iSCSI volumes can be created using the ONTAP CLI, ONTAP API, or Cloud Manager API.

Get started with Amazon FSx for ONTAP

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

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

1 **Create an FSx for ONTAP working environment**

You must create an Amazon FSx for ONTAP working environment before adding volumes. You will need to set up an IAM role that enables the Cloud Manager SaaS to assume the role.

2 **Create a Connector**

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

3 **Add volumes**

You can create FSx for ONTAP volumes using Cloud Manager.

4 **Manage your volumes**

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

Related links

- Creating a Connector from Cloud Manager

- Launching a Connector from the AWS Marketplace

- Installing the Connector software on a Linux host

Requirements

Set up permissions for FSx for ONTAP

To create or manage an Amazon FSx for ONTAP working environment, you need to add AWS credentials to Cloud Manager by providing the ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment.

Set up the IAM role

Set up an IAM role that enables the Cloud Manager SaaS to assume the role.

Steps

1. Go to the IAM console in the target account.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the Cloud Manager SaaS: 952013314444
   - Create a policy that includes the following permissions:

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

3. Copy the Role ARN of the IAM role so that you can paste it in Cloud Manager in the next step.

Result

The IAM role now has the required permissions.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to Cloud Manager.

Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and follow the steps in the wizard.

   a. **Credentials Location**: Select **Amazon Web Services > Cloud Manager**.

   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.

   c. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now use the credentials when creating an FSx for ONTAP working environment.

Related links

- AWS credentials and permissions
- Managing AWS credentials for Cloud Manager

Security group rules for FSx for ONTAP

Cloud Manager creates AWS security groups that include the inbound and outbound rules that Cloud Manager and FSx for ONTAP need to operate successfully. You might want to refer to the ports for testing purposes or if you need to use your own.

Rules for FSx for ONTAP

The security group for FSx for ONTAP requires both inbound and outbound rules.

Inbound rules

The source for inbound rules in the predefined security group is 0.0.0.0/0.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF

Protocol	Port	Purpose
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
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
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	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
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

Outbound rules

The predefined security group for FSx for ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for FSx for ONTAP includes the following outbound rules.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by FSx for ONTAP.

> ℹ️ The source is the interface (IP address) on the FSx for ONTAP system.

Service	Protocol	Port	Source	Destination	Purpose
Active Directory	TCP	88	Node management LIF	Active Directory forest	Kerberos V authentication
	UDP	137	Node management LIF	Active Directory forest	NetBIOS name service
	UDP	138	Node management LIF	Active Directory forest	NetBIOS datagram service
	TCP	139	Node management LIF	Active Directory forest	NetBIOS service session
	TCP & UDP	389	Node management LIF	Active Directory forest	LDAP
	TCP	445	Node management LIF	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Node management LIF	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	UDP	464	Node management LIF	Active Directory forest	Kerberos key administration
	TCP	749	Node management LIF	Active Directory forest	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
	UDP	137	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
	UDP	138	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
	TCP	139	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
	TCP & UDP	389	Data LIF (NFS, CIFS)	Active Directory forest	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
	TCP	749	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (RPCSEC_GSS)
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

Rules for the Connector

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host

Protocol	Port	Purpose
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from Cloud Data Sense
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the Cloud Data Sense instance with internet access, if your AWS network doesn't use a NAT or proxy

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

ⓘ The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp

Service	Protocol	Port	Destination	Purpose
API calls	TCP	3000	ONTAP HA mediator	Communication with the ONTAP HA mediator
	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager
Cloud Data Sense	HTTP	80	Cloud Data Sense instance	Cloud Data Sense for Cloud Volumes ONTAP

Use Amazon FSx for ONTAP

Create and manage an Amazon FSx for ONTAP working environment

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

Create an Amazon FSx for ONTAP working environment

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

Before you begin

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

- The ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment. See adding AWS credentials to Cloud Manager for details.
- The region and VPN information for where you will create the FSx for ONTAP instance.

Steps

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

2. Select **Amazon FSx for ONTAP** and click **Next**.

3. Authenticate FSx for ONTAP in Cloud Manager.
   a. If there is an existing IAM role in your account with the correct AWS permissions for FSx for ONTAP,

select it from the dropdown.

b. If there is no IAM role in your account, click **Credentials Page** and follow the steps in the wizard to add an ARN for an AWS IAM role with FSx for ONTAP credentials. See adding AWS credentials to Cloud Manager for details.

4. Provide information about your FSx for ONTAP instance:

   a. Enter the working environment name you want to use.

   b. Optionally, you can create tags by clicking the plus sign and entering a tag name and value.

   c. Enter and confirm the ONTAP Cluster password you want to use.

d. Select the option to use the same password for your SVM user or set a different password.

e. Click **Next**.

5. Provide region and VPC information:

a. Select a region and VPC with subnets in at least two Availability Zones so each node is in a dedicated Availability Zone.

b. Accept the default security group or select a different one. AWS security groups control inbound and outbound traffic. These are configured by your AWS admin and are associated with your AWS elastic network interface (ENI).

c. Select an Availability Zone and subnet for each node.

d. Click **Next**.

6. Leave *CIDR Range* empty and click **Next** to automatically set an available range. Optionally, you can use AWS Transit Gateway to manually configure a range.

Add FSx for ONTAP   Floating IP

Floating IP addresses are required for cluster and SVM access and for
NFS and CIFS data access.

Floating IPs can migrate between HA nodes if failures occur. To access
the data from outside the VPC, you can set up an AWS transit gateway.

CIDR Range   *Optional*

[Example: 10.10.10.10/24   ]

Notice: You must specify a CIDR block that is outside of
the CIDR blocks for all VPCs in the selected AWS region.

                                         [Previous]   [Next]

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

Add FSx for ONTAP   Route Tables

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

2 Route table

☐	Name	⇕	Main	⇕	ID	⇕	Associate with Subnets	⇕	Tags	⇕
☑	VPC4QA		Yes		rtb-0880ec9d aeb55d630		2 Subnets		2	⌄
☐	*No tag name*		No		rtb-0e0c7d9e a4cf05d66		1 Subnet		1	⌄

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

                                         [Previous]   [Next]

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

9. Configure your storage:

    a. Select the throughput, capacity, and unit.

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

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

    c. Click **Next**.

10. Review your configuration:

   a. Click the tabs to review your ONTAP properties, provider properties, and networking configuration.

   b. Click **Previous** to make changes to any settings.

   c. Click **Add** to accept the settings and create your Working Environment.

Result

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

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

Discover an existing FSx for ONTAP file system

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

Steps

1. In Cloud Manager, click **Add Working Environment**, select **Amazon Web Services**.

2. Select **Amazon FSx for ONTAP** and click **Click Here**.
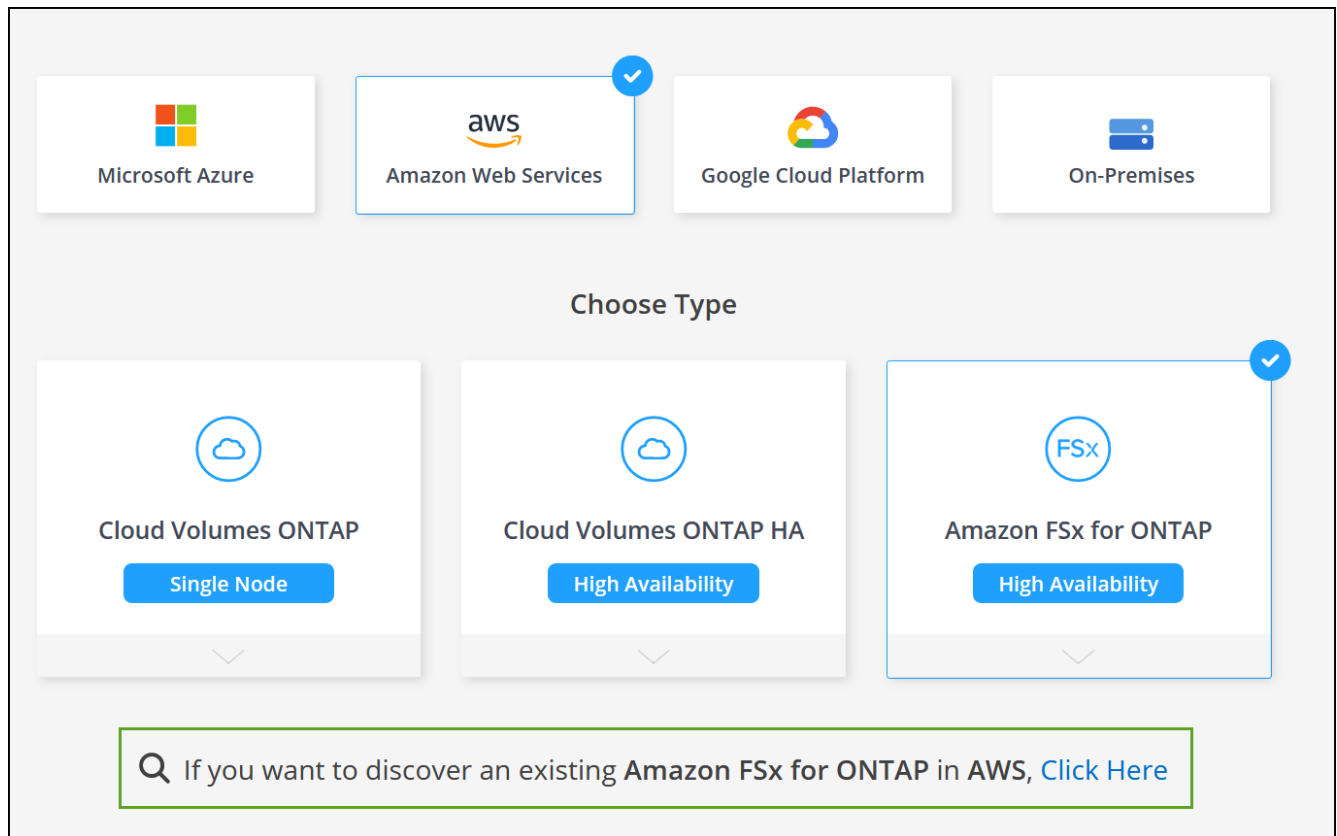
3. Select existing credentials or create new credentials. Click **Next**.

4. Select the AWS region and the working environment you want to add.


5. Click **Add**.

Result

Cloud Manager displays your discovered FSx for ONTAP file system.

Remove FSx for ONTAP from the workspace

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

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed with removing the working environment.

2. At the top right of the page, select the actions menu and click **Remove from workspace**.
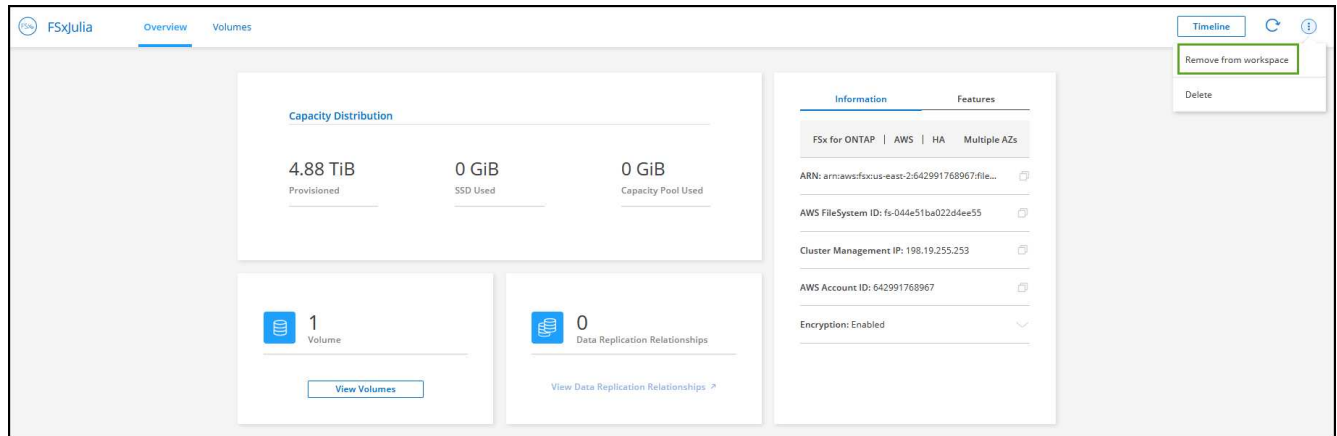
3. Click **Remove** to remove FSx for ONTAP from Cloud Manager.

Delete the FSx for ONTAP working environment

You can delete the FSx for ONTAP from Cloud Manager.

Before you begin

- You must delete all volumes associated with the file system.

  > ⓘ You will need an active Connector in AWS to remove or delete volumes.

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

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

Steps

1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed to deleting the working environment.

2. At the top right of the page, select the actions menu and click **Delete**.
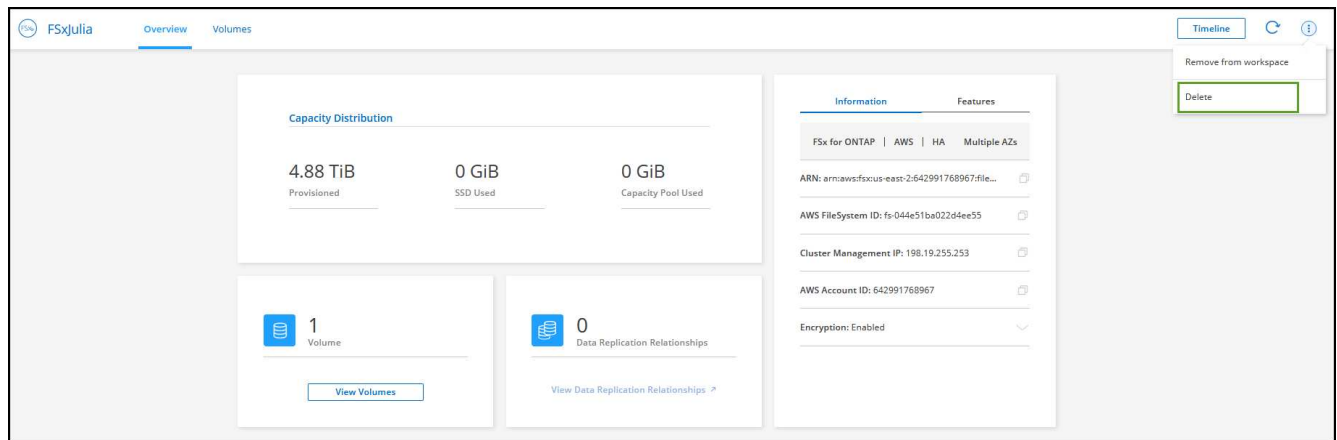
3. Enter the name of the working environment and click **Delete**.

Create volumes for Amazon FSx for ONTAP

After you set up your working environment, you can create and mount FSx for ONTAP volumes.

Create volumes

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

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

Before you begin

You need:

- An active Connector in AWS.
- If you want to use SMB, you must have set up DNS and Active Directory. For more information on DNS and Active Directory network configuration, see AWS: Prerequisites for using a self-managed Microsoft AD.

Steps

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

A Connector is required to manage your FSx for ONTAP instance

A Connector enables Cloud Manager to manage resources and processes within your public cloud environment. For FSx for ONTAP, this includes creating volumes, replicating data, managing snapshots, integrating with NetApp's cloud services, and more.

Add Connector

Back to Canvas
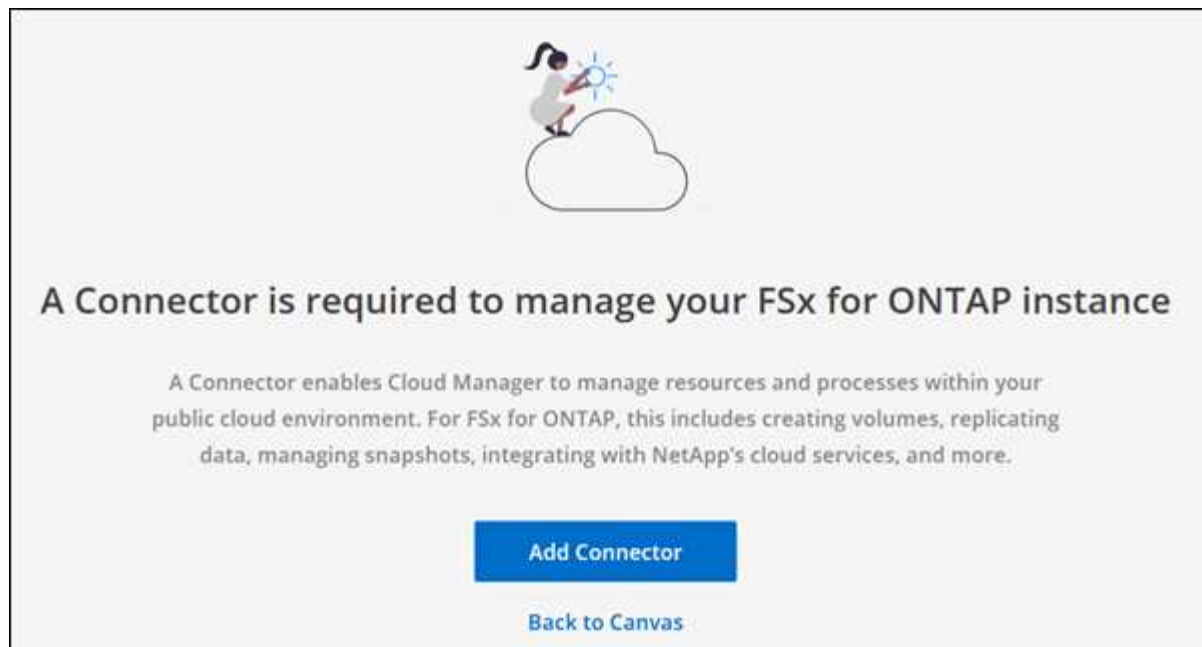
3. Click the **Volumes** tab

4. Click **Add Volume**.

There are no volumes

To start using FSx for ONTAP, add your first volume.

Add Volume

5. **Volume Details and Protection**:

   a. Enter a name for your new volume.

   b. The Storage VM (SVM) fields auto-populates the SVM based on the name of your working environment.

   c. Enter the volume size and select a unit (GiB or TiB). Note that the volume size will grow with usage.

   d. Select a snapshot policy. By default, a snapshot is taken every hour (keeping the last six copies), every day (keeping the last two copies), and every week (keeping the last two copies).

   e. Click **Next**.

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

   a. For NFS:

      ▪ Select an Access Control policy.

      ▪ Select the NFS versions.

      ▪ Select a Custom Export Policy. Click the information icon for valid value criteria.

   b. For CIFS:

      ▪ Enter a Share Name.

      ▪ Enter users or groups separated by a semicolon.

      ▪ Select the permission level for the volume.

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

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

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

▪ If you select a Workgroup setup, enter the server and workgroup name for a workgroup configured

for CIFS.

   c. Click **Next**.

7. **Usage Profile and Tiering**:

   a. By default, **Storage Efficiency** is disabled. You can change this setting to enable deduplication and compression.

   b. By default, **Tiering Policy** is set to **Snapshot Only**. You can select a different tiering policy based on your needs.

   c. Click **Next**.

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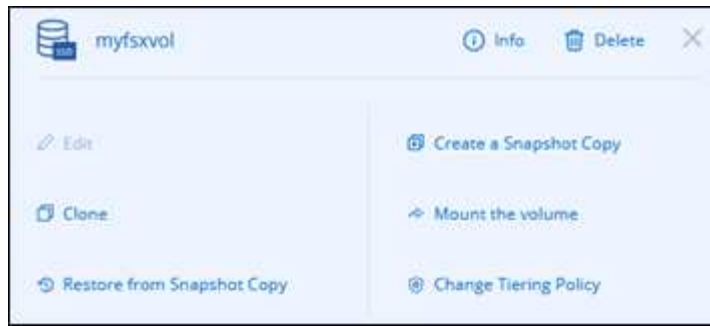
Result

The new volume is added to the working environment.

Mount volumes

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

Steps

1. Open the working environment.

2. Open the volume menu and select **Mount the volume**.

3. Follow the instructions to mount the volume.

Manage volumes for Amazon FSx for ONTAP

You can manage volumes, clones, and snapshots, and change tiering policies for FSx for ONTAP using Cloud Manager.

Edit volumes

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

Steps

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

Clone volumes

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

Steps

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

Manage Snapshot copies

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

Steps

1. Open the working environment.
2. Open the volume menu and choose one of the available options to manage Snapshot copies:
   ◦ **Create a Snapshot copy**

◦ **Restore from a Snapshot copy**

3. Follow the prompts to complete the selected action.

Change the tiering policy

Change the tiering policy for the volume.

Steps

1. Open the working environment.

2. Open the volume menu and select **Change Tiering policy**.

3. Select a new volume tiering policy and click **Change**.

Replicate and sync data

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

You can create sync relationships using Cloud Sync in Cloud Manager. To configure sync relationships, see create sync relationships.

Delete volumes

Delete the volumes that you no longer need.

Before you begin

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

Steps

1. Open the working environment.

2. Open the volume menu and select **Delete**.

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

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

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, register for one.

2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

3. Click **NSS Management > Add NSS Account**.

4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   This action enables Cloud Manager to use your NSS account.

   Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- Knowledge base

  Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Cloud Manager community to follow ongoing discussions or create new ones.

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.

2. Choose one of the available options under Technical Support:

    a. Click **Call Us** to find phone numbers for NetApp technical support.

    b. Click **Open an Issue**, select one the options, and then click **Send**.

    A NetApp representative will review your case and get back to you soon.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager 3.9
- Notice for the Cloud Backup
- Notice for Cloud Sync
- Notice for Cloud Tiering
- Notice for Cloud Data Sense