



# **Amazon FSx for NetApp ONTAP documentation**

Amazon FSx for NetApp ONTAP

NetApp  
February 11, 2024

This PDF was generated from <https://docs.netapp.com/us-en/bluexp-fsx-ontap/index.html> on February 11, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

Amazon FSx for NetApp ONTAP documentation	1
What's new with Amazon FSx for NetApp ONTAP	2
30 July 2023	2
02 July 2023	2
04 June 2023	2
07 May 2023	2
02 April 2023	2
05 March 2023	2
01 January 2023	2
18 September 2022	2
31 July 2022	3
3 July 2022	3
27 February 2022	3
31 October 2021	3
4 October 2021	3
2 September 2021	4
Get started	5
Learn about Amazon FSx for NetApp ONTAP	5
Quick start for Amazon FSx for NetApp ONTAP	6
Requirements	7
Set up permissions for FSx for ONTAP	7
Security group rules for FSx for ONTAP	10
Use Amazon FSx for NetApp ONTAP	17
Create or discover an FSx for ONTAP working environment	17
Manage an FSx for ONTAP working environment	20
Create volumes for FSx for ONTAP	25
Manage volumes for FSx for ONTAP	31
Add and manage storage VMs for FSx for ONTAP	33
Knowledge and support	37
Register for support	37
Get help	41
Legal notices	47
Copyright	47
Trademarks	47
Patents	47
Privacy policy	47
Open source	47

# Amazon FSx for NetApp ONTAP documentation

# What's new with Amazon FSx for NetApp ONTAP

Learn what's new in FSx for ONTAP.

## 30 July 2023

Customers can now create Amazon FSx for NetApp ONTAP file systems in three new AWS Regions: Europe (Zurich), Europe (Spain), and Asia Pacific (Hyderabad).

Refer to [Amazon FSx for NetApp ONTAP is now available in three additional regions](#) for full details.

## 02 July 2023

- You can now [add a storage VM](#) to the Amazon FSx for NetApp ONTAP file system using BlueXP.
- The **My Opportunities** tab is now **My estate**. The documentation is updated to reflect the new name.

## 04 June 2023

- When [creating a working environment](#), you can specify the start time for the weekly 30-minute maintenance window to ensure maintenance does not conflict with critical business activities.
- When [creating a volume](#), you can enable data optimization by creating a FlexGroup to distribute data across volumes.

## 07 May 2023

- When creating a working environment, you can now have BlueXP [generate a security group](#) that allows traffic within the selected VPC only. This feature [requires additional permissions](#).
- You can optionally [add](#) and [modify](#) tags to categorize volumes.

## 02 April 2023

The IOPS limit is increased to allow manual or automatic provisioning up to 160,000.

## 05 March 2023

User interface improvements have been made and screenshots have been updated in the documentation.

## 01 January 2023

You can now choose to enable [automatic capacity management](#) to add incremental storage based on demand. Automatic capacity management polls the cluster at regular intervals to assess demand and automatically increases storage capacity in increments of 10% up to 80% of the the cluste's maximum capacity.

## 18 September 2022

You can now [change the storage capacity and IOPS](#) at any time after you create the FSx for ONTAP working environment.

## 31 July 2022

- If you previously provided your AWS credentials to Cloud Manager, the new **My estate** feature can automatically discover and suggest FSx for ONTAP file systems to add and manage using Cloud Manager. You can also review available data services through the **My estate** tab.

[Discover FSx for ONTAP using My estate](#)

- You can now [change throughput capacity](#) at any time after you create the FSx for ONTAP working environment.
- You can now [replicate and sync data](#) to on-premises and other FSx for ONTAP systems using FSx for ONTAP as the source.
- You can now [create iSCSI volumes in FSx for ONTAP using Cloud Manager](#).

## 3 July 2022

- You can now select a single or multiple Availability Zone HA deployment model.

[Create an FSx for ONTAP working environment](#)

- AWS GovCloud account authentication is now supported in Cloud Manager.

[Set up the IAM role](#)

## 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 NetApp ONTAP

- [Amazon FSx for NetApp 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 NetApp ONTAP](#).

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

[Create an Amazon FSx for NetApp 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 NetApp ONTAP](#).

# Get started

## Learn about Amazon FSx for NetApp ONTAP

[Amazon FSx for NetApp ONTAP](#) is a fully managed service allowing customers to launch and run file systems powered by the NetApp 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, iSCSI, 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 BlueXP

- FSx for ONTAP is supported when using BlueXP in *standard* or *restricted* mode.
  - Standard mode leverages the BlueXP SaaS layer to provide full functionality.
  - Restricted mode is available for organizations that have connectivity restrictions.

Refer to [BlueXP deployment modes](#) for more information.

- Using [BlueXP](#) and a Connector in AWS, you can create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as BlueXP classification and BlueXP copy and sync.
- Using Artificial Intelligence (AI) driven technology, BlueXP classification can help you understand data context and identify sensitive data that resides in your FSx for ONTAP accounts. [Learn more](#).
- Using BlueXP copy and 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 BlueXP. Refer to [Amazon FSx for NetApp ONTAP getting started guide](#).

There is an additional cost associated with using the Connector in AWS and the optional data services such as BlueXP copy and sync and BlueXP classification.

### Supported regions

[View supported Amazon regions](#).

## Getting help

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

For general questions about BlueXP or BlueXP storage solutions and services, you can start with the in-line BlueXP chat.

For technical support issues specific to BlueXP or BlueXP storage solutions and services, you can open a NetApp support ticket using your BlueXP account level serial number. You will need to [register your BlueXP account](#) to activate support.

## Quick start for Amazon FSx for NetApp ONTAP

Using [BlueXP](#), you can get started with FSx for ONTAP in just a few steps.

1

### Set up an IAM role in AWS

To create or manage an FSx for ONTAP working environment, you need to add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP the permissions needed to create an FSx for ONTAP working environment. To do this, you must [set up an IAM role that enables the BlueXP SaaS to assume the role](#).

2

### Create an FSx for ONTAP working environment

You must [create an FSx for ONTAP working environment](#) before adding volumes.

3

### Create a Connector for AWS

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, BlueXP will prompt you if one is not already active.

4

### Add and mount a volume

You can [create and mount FSx for ONTAP volumes](#) using BlueXP.

### What's next

You can now use BlueXP to manage your volumes and configure additional services such as replication, copy and sync, and classification.



# Requirements

## Set up permissions for FSx for ONTAP

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

### Set up the IAM role

Set up an IAM role that enables BlueXP to assume the role.

#### Steps

1. Go to the IAM console in the target account.
2. Grant BlueXP access to the AWS account. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.
  - Under **Trusted entity type**, select **AWS account**.
  - Select **Another AWS account** and enter the BlueXP **Account ID**:
    - For BlueXP SaaS: 952013314444
    - For AWS GovCloud (US): 033442085313



For increased security, we suggest you specify an [External ID](#). To access your AWS account, BlueXP will have to provide the role ARN (Amazon Resource Name) and the external ID you specified. This prevents the [confused deputy problem](#).

3. Create a policy that includes the following required minimum permissions and optional permissions, as needed.

### Required permissions

The following minimum permissions are required to allow BlueXP to create your FSx for NetApp ONTAP file system.

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

### Automatic capacity

The following additional permissions are required to enable [automatic capacity management](#).

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

### Security groups

The following additional permissions are required to allow BlueXP to [generate security groups](#).

```
"ec2:AuthorizeSecurityGroupEgress",  
"ec2:AuthorizeSecurityGroupIngress",  
"ec2:RevokeSecurityGroupEgress",  
"ec2:RevokeSecurityGroupIngress",  
"ec2:CreateSecurityGroup",  
"ec2:DeleteSecurityGroup",  
"cloudformation:CreateStack",  
"cloudformation:ValidateTemplate",  
"cloudformation:DescribeStacks",  
"cloudformation:DescribeStackEvents"
```

4. Copy the role ARN of the IAM role so that you can paste it in BlueXP 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 BlueXP.

### Before you get started

If you just created the IAM role, wait a few minutes for the new credentials to become available.

### Steps

1. In the upper right of the BlueXP 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 > BlueXP**.
  - b. **Define Credentials:** Provide a **Credentials name** and the **Role ARN** and **External ID** (if specified) you created when you [Set up the IAM role](#).

- If you use an AWS GovCloud (US) account, check **I use an AWS GovCloud (US) account**.



☒ I use an AWS GovCloud (US) account

When creating the IAM role for AWS GovCloud (US), enter the Cloud Manager account ID:

<account ID>

- Authenticating using AWS GovCloud will disable the SaaS platform. This is a permanent change to your account and cannot be undone.

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

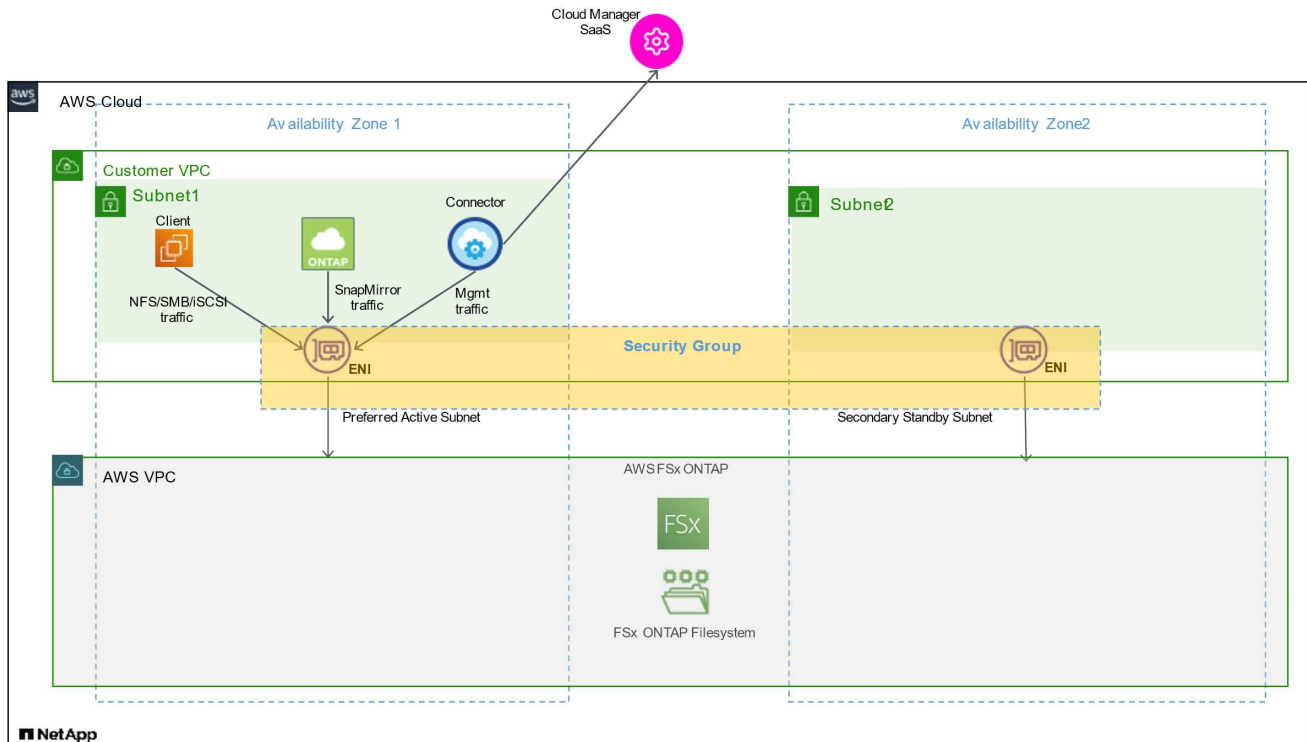
- [AWS credentials and permissions](#)
- [Managing AWS credentials for BlueXP](#)

# Security group rules for FSx for ONTAP

BlueXP creates AWS security groups that include the inbound and outbound rules that BlueXP 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 FSx for ONTAP security group requires both inbound and outbound rules. This diagram illustrates FSx for ONTAP networking configuration and security group requirements.

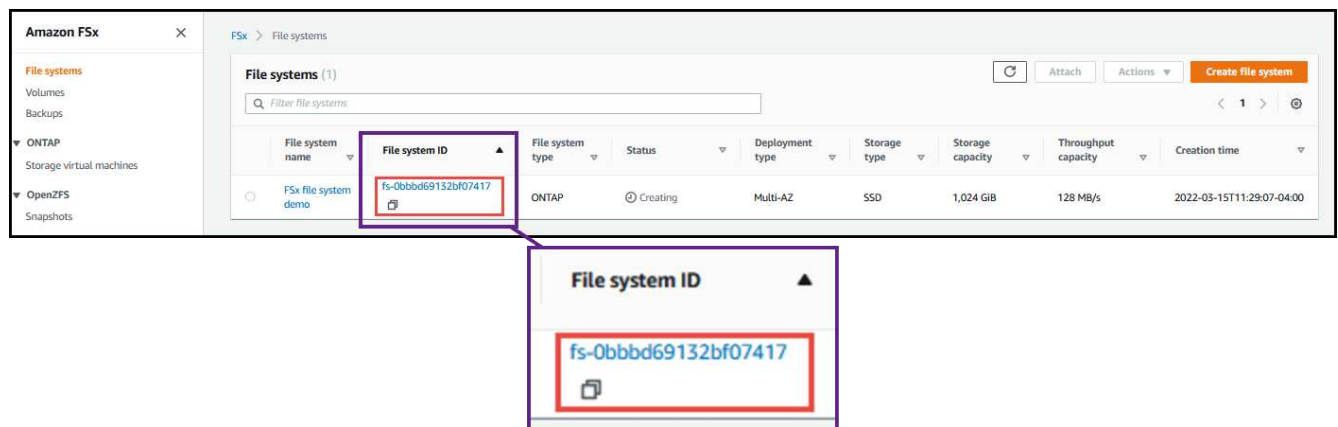


## Before you begin

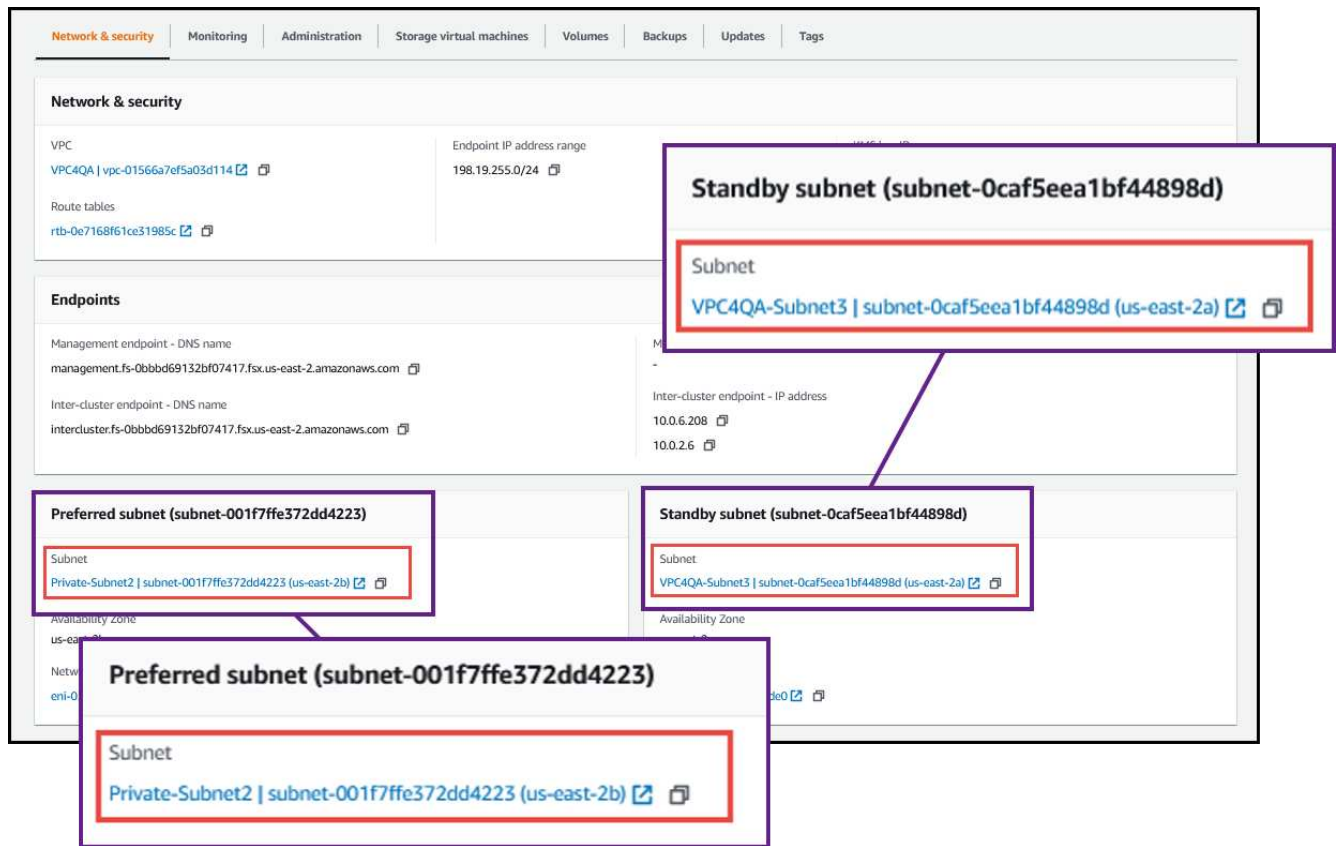
You need to locate the security groups associated with the ENIs using the AWS Management Console.

## Steps

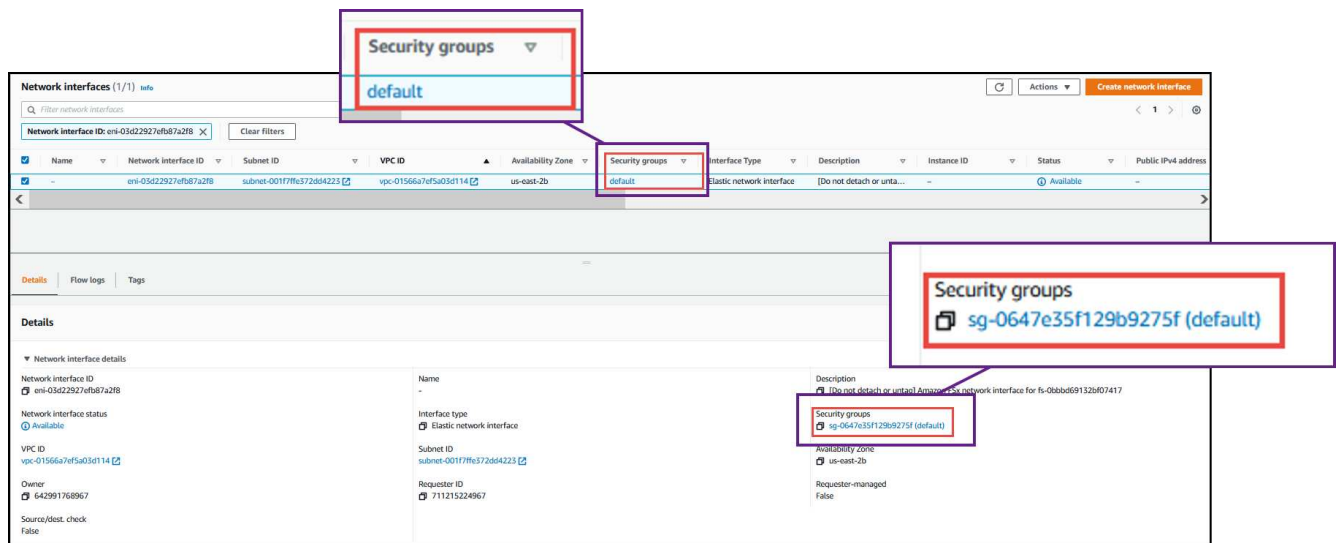
1. Open the FSx for ONTAP file system in the AWS Management Console and click the file system ID link.



2. On the **Network & security** tab, click the network interface ID for the preferred or standby subnet.



3. Click the security group in the network interface table or the **Details** section for the network interface.



## Inbound rules

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTPS	443	Access from the Connector to fsxadmin management LIF to send API calls to FSx
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF

Protocol	Port	Purpose
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

You do not need to open specific ports for the mediator or between nodes in FSx for ONTAP.



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
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	1860 0–18 699	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	1110 4	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	1110 5	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
HTTP	80	Provides HTTP access from client web browsers to the local user interface and connections from BlueXP classification instance
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the BlueXP classification 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
API calls	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP
BlueXP classification	HTTP	80	BlueXP classification	BlueXP classification for Cloud Volumes ONTAP

# Use Amazon FSx for NetApp ONTAP

## Create or discover an FSx for ONTAP working environment

Using BlueXP you can create or discover an FSx for ONTAP working environment to add and manage volumes and additional data services.

### Create an 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 BlueXP](#).

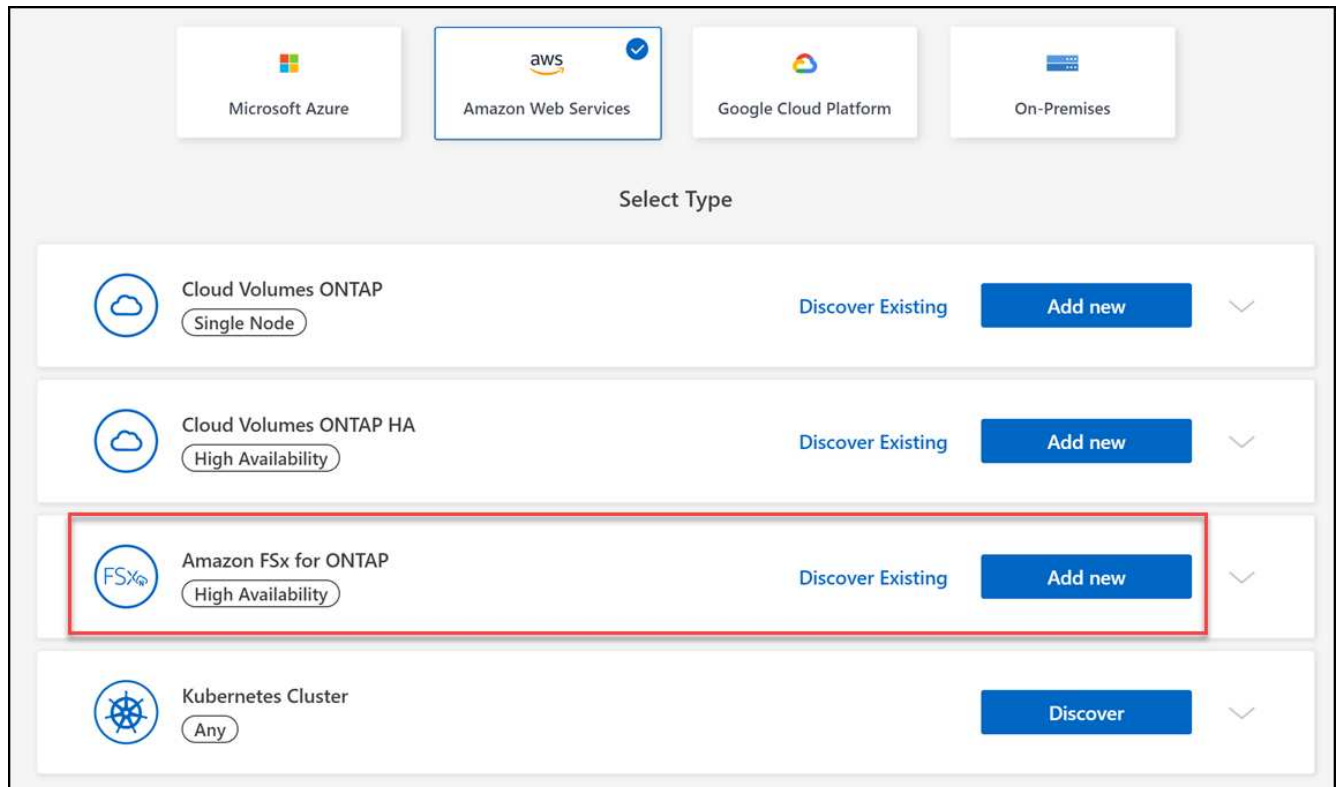
#### Before you begin

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

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

#### Steps

1. In BlueXP, add a new Working Environment, select **Amazon Web Services**, and click **Add new** for Amazon FSx for NetApp ONTAP.



#### 2. FSx for ONTAP Authentication

- 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** 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 BlueXP](#) for details.

### 3. Details and Credentials

- 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. Optionally, you can specify the start time for FSx for ONTAP to perform 30-minute weekly maintenance. This can be used to ensure maintenance does not coincide with critical business activities. If you select **No preference**, a random start time will be assigned. You can change this at any time.
- d. Enter and confirm the ONTAP Cluster password you want to use.
- e. Optionally, deselect the option to use the same password for your SVM user and set a different password.

### 4. HA deployment model

- a. Select a **Single Availability Zone** or **Multiple Availability Zones** HA deployment model. For multiple Availability Zones, select subnets in at least two Availability Zones so each node is in a dedicated Availability Zone.
- b. Select the Virtual Private Cloud (VPC) you want to associate with your file system.
- c. Use an existing security group or select **Generated security group** to enable BlueXP to generate a security group that allows traffic within the selected VPC only.



[AWS security groups](#) control inbound and outbound traffic. These are configured by your AWS admin and are associated with your [AWS elastic network interface \(ENI\)](#).

### 5. Floating IP (Multiple Availability Zones only)

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



#### IPs in the following ranges are not supported:

- 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

### 6. Route Tables (Multiple Availability Zones only)

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), BlueXP automatically adds the floating IP addresses to that route table.

### 7. Data Encryption

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](#).

## 8. Storage Configuration

- Select the throughput, capacity, and unit. You can change throughput, storage capacity, and IOPS at any time.
- You can optionally specify an IOPS value. If you don't specify an IOPS value, BlueXP 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. You can change the IOPS value at any time.



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

## 9. Review

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

## Result

BlueXP displays your FSx for ONTAP configuration on the Canvas. You can now add volumes to your FSx for ONTAP working environment using BlueXP.



## Discover an existing FSx for ONTAP file system

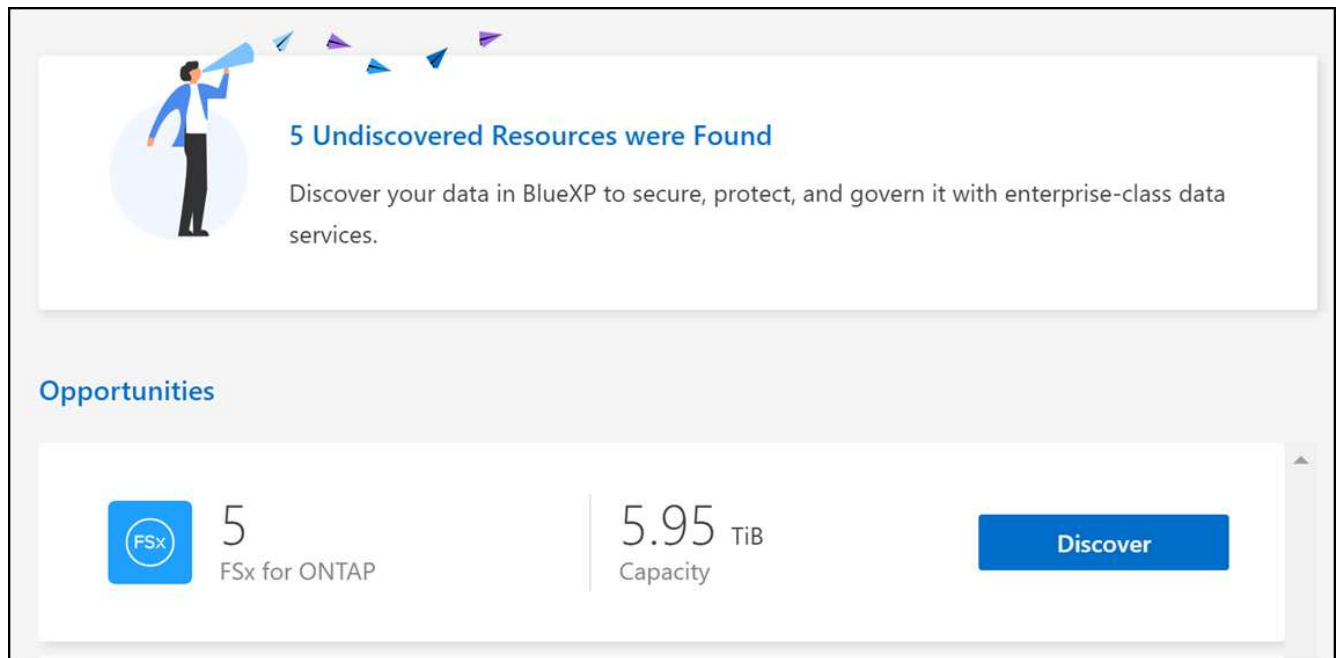
If you previously provided your AWS credentials to BlueXP, **My estate** can automatically discover and suggest FSx for ONTAP file systems to add and manage using BlueXP. You can also review available data services.

### About this task

You can discover FSx for ONTAP file systems when you [Create an FSx for ONTAP working environment](#) or by using the **My estate** page. This task describes discovery using **My estate**

### Steps

- In BlueXP, click the **My estate** tab.
- The count of discovered FSx for ONTAP file systems displays. Click **Discover**.



3. Select one or more file systems and click **Discover** to add them to the Canvas.



- If you select an un-named cluster, you will receive a prompt to enter a name for the cluster.
- If you select a cluster that doesn't have the credentials required to allow BlueXP to manage the FSx for ONTAP file system, you'll receive a prompt to select credentials with the required permissions.

### Result

BlueXP displays your discovered FSx for ONTAP file system on the Canvas. You can now add volumes to your FSx for ONTAP working environment using BlueXP.



## Manage an FSx for ONTAP working environment

BlueXP enables you to manage your FSx for ONTAP working environment. You can enable automatic capacity management, change throughput and storage capacity and IOPS, remove or delete the working environment, and manage data services such as backup and recovery, copy and sync, classification, replication, and volume caching.

## Manage automatic capacity

You can choose to enable automatic capacity management to add incremental storage based on demand. Automatic capacity management polls the cluster at regular intervals to assess demand and automatically increases storage capacity in increments of 10% up to 80% of the the cluster's maximum capacity.




If you did not manually specify an IOPS value when creating the working environment, BlueXP will increase the IOPS by 3 IOPS per GiB of the new total capacity. If you specified an IOPS value, BlueXP will not adjust the IOPS. For details on configuring IOPS, refer to [create a working environment](#).

Automatic capacity management is disabled by default. You can manage automatic capacity with or without an active Connector in AWS.

### Manage automatic capacity without an active Connector

You can manage automatic capacity without an active Connector in AWS.

#### Steps

1. Select the working environment on the canvas and select **Enter Working Environment**.
2. Select the pencil icon () to open the **Automatic capacity management** page.




All other options require a Connector and are disabled.

- Select the box to enable automatic capacity management.
  - Deselect the box to disable automatic capacity management if it was previously enabled.
3. Select **Apply**.

### Manage automatic capacity with an active Connector

You can manage automatic capacity with an active Connector in AWS.

#### Steps

1. Open the FSx for ONTAP working environment.
2. From the **Overview** tab, select **Features**.
3. Select the pencil icon () to open the **Automatic capacity management** page.
4. On the **Automatic capacity management** page:
  - Select the box to enable automatic capacity management.
  - Deselect the box to disable automatic capacity management if it was previously enabled.
5. Select **Apply**.

## Change throughput capacity

You can change the throughput capacity at any time after you create the FSx for ONTAP working environment.

### Before you begin

You need an active [Connector in AWS](#).

## Steps

1. Open the FSx for ONTAP working environment.
2. From the **Overview** tab, select **Features**.
3. Select the pencil icon (✎) to open the **Throughput Capacity** edit page.
4. Select a new throughput capacity from the dropdown and select **Update**. This change can take up to 25 minutes to take effect and does not disrupt data access.

## Change storage capacity and IOPS




You can change the storage capacity and IOPS at any time after you create the FSx for ONTAP working environment.

### Before you begin

You need an active [Connector in AWS](#).

## Steps

1. Open the FSx for ONTAP working environment.
2. From the **Overview** tab, select **Features**.
3. Select the pencil icon (✎) to open the **Storage Capacity & IOPS** edit page.
4. You can change the storage capacity and IOPS once every six hours. If you attempt to make changes more frequently, you will receive an error.

 Update storage capacity	 Update IOPS
Current storage capacity: 1 TiB	Current IOPS: 6000
Change storage capacity by:	Change IOPS by:
<input checked="" type="radio"/> Percentage <input type="radio"/> Absolute	<input checked="" type="radio"/> Automatic <input type="radio"/> User provisioned
Desired % increase  <input type="text" value="Minimum 10"/> %	"Automatic" maintains a ratio of 3 provisioned SSD IOPS per GiB of primary storage (up to 160,000).



- The recommended maximum storage capacity utilization is 80% to maintain Data Tiering performance and allow capacity for additional data.
- Selecting **Automatic** IOPS maintains a ratio of three provisioned SSD IOPS per GiB of primary storage up to 160,000. You cannot manually provision an IOPS value of greater than 160,000.

5. Select the checkbox to confirm you understand changing storage capacity impacts the cost of the FSx for ONTAP service and that additional changes cannot be made for six hours.
6. Select **Update** to confirm your changes.

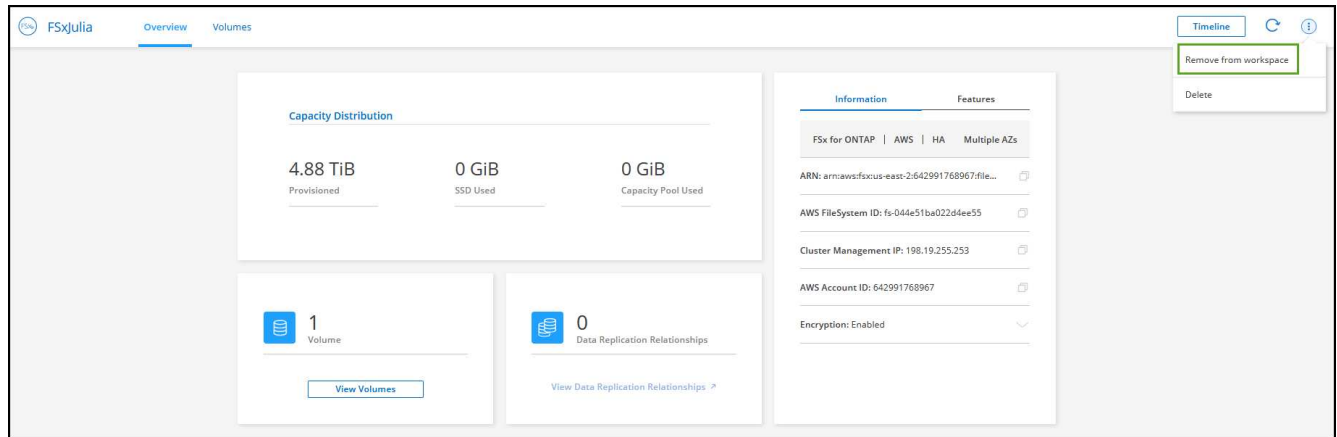


## Remove FSx for ONTAP from the workspace

You can remove FSx for ONTAP from BlueXP without deleting your account or volumes. You can add the FSx for ONTAP working environment back to BlueXP 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 select **Remove from workspace**.



3. Select **Remove** to remove FSx for ONTAP from BlueXP.

## Delete the FSx for ONTAP working environment

You can delete the FSx for ONTAP from BlueXP.



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

### Before you begin

Before deleting the working environment, you must:

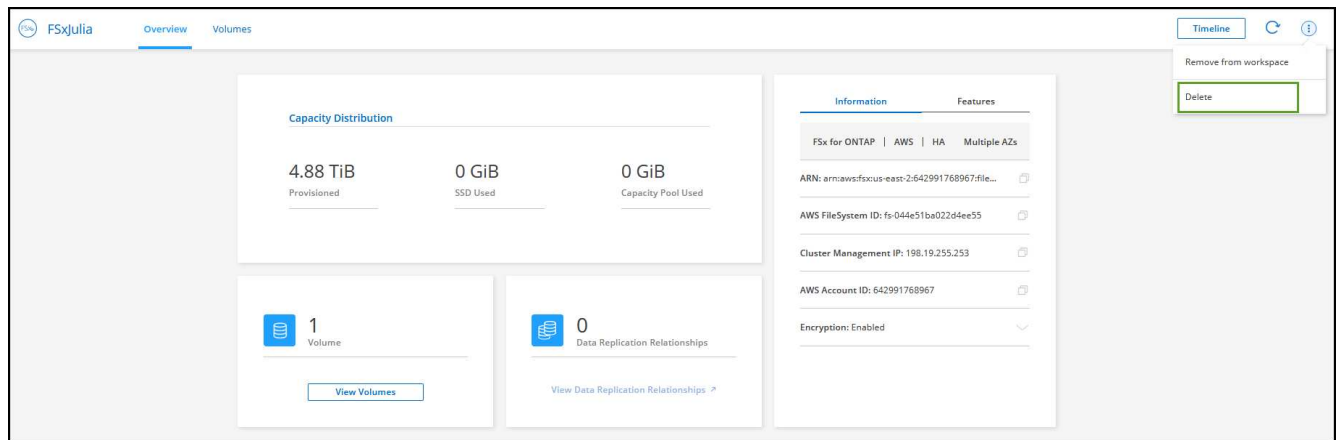
- Break all replication relationships with this working environment.
- [Delete all volumes](#) associated with the file system. You will need an active Connector in AWS to remove or delete volumes.



Failed volumes must be deleted using the AWS Management Console or CLI.

### Steps

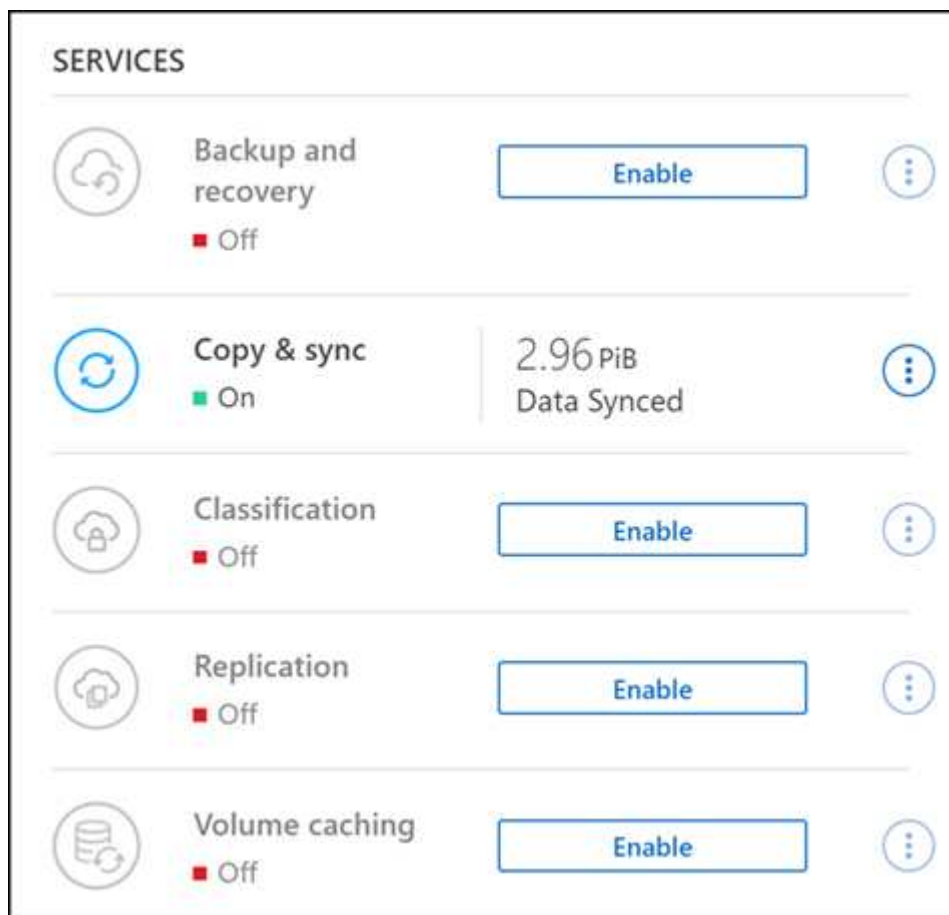
1. Open the working environment. If you don't have a Connector in AWS, you will see the prompt screen. You can ignore this and proceed to deleting the working environment.
2. At the top right of the page, select the actions menu and select **Delete**.



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

## Manage data services

You can manage additional data services from the FSx for ONTAP working environment.



For details on configuring data services, refer to:

- [BlueXP backup and recovery](#) provides efficient, secure, and cost-effective data protection for NetApp ONTAP data, Kubernetes persistent volumes, databases, and virtual machines, both on premises and in the cloud.
- [BlueXP copy and sync](#) is a cloud replication and synchronization service for transferring NAS data between on-premises and cloud object stores.

- [BlueXP classification](#) enables you to scan and classify data across your organization's hybrid multicloud.
- [Replicate data](#) between ONTAP storage systems to support backup and disaster recovery to the cloud or between clouds.
- [Volume caching](#) provides a persistent, writable volume in a remote place. You can use BlueXP volume caching to speed up access to data or to offload traffic from heavily accessed volumes.

## Create volumes for 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, CIFS, and iSCSI volumes from your FSx for ONTAP working environment in BlueXP. Volumes created using ONTAP CLI will also be visible in your FSx for ONTAP working environment.

#### About this task

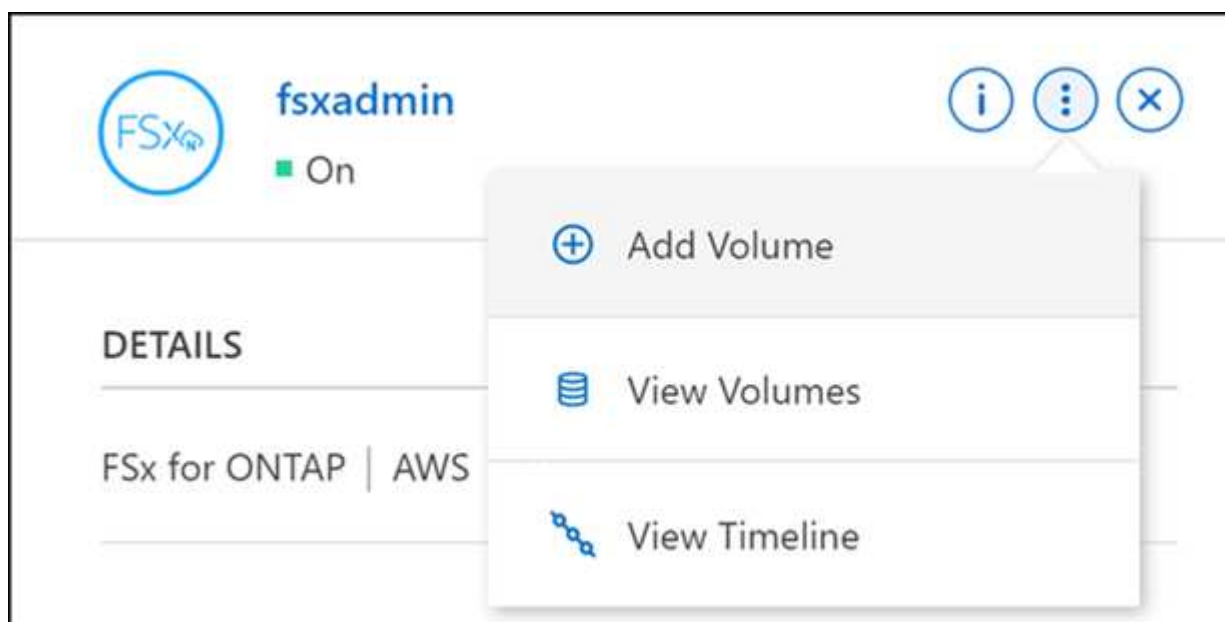
You can add volumes by opening the working environment and selecting the **Volumes** tab or simply using working environment **Details** panel from the Canvas. This task describes adding volumes using the **Details** panel.

#### 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. Select the FSx for ONTAP working environment on the Canvas. If you don't have a Connector enabled, you'll be prompted to add one.
2. In the **Details** panel, use the three dots (⋮) to open the options menu. Click **Add Volume**.



### 3. Volume details, protection, & tags

- a. Enter a name for your new volume.
- b. The Storage VM (SVM) field auto-populates the SVM based on the name of your working environment.
- c. Enter the volume size and select a unit (GiB or TiB). Note that the volume size will grow with usage.
- d. Select a snapshot policy. By default, a snapshot is taken every hour (keeping the last six copies), every day (keeping the last two copies), and every week (keeping the last two copies).
- e. Optionally, create tags to categorize your volumes by clicking the plus sign and entering a tag name and value.
- f. Optionally, select the optimization option to create a FlexGroup and distribute volume data across the cluster.



FlexGroup distribution is available for NFS and CIFS volume protocols only.

### 4. Volumes protocol:

- a. Select an NFS, CIFS, or iSCSI volume protocol.

## NFS

1. Select an Access Control policy.
2. Select the NFS versions.
3. Select a Custom Export Policy. Click the information icon for valid value criteria.

The screenshot shows the 'Volumes Protocol' configuration window. At the top, there's a section 'Select the volume's protocol:' with three radio buttons: 'NFS Protocol' (selected), 'CIFS Protocol', and 'iSCSI Protocol'. Below this, there are two main sections. The left section is 'Access Control' with a dropdown menu showing 'Custom\_export\_policy'. The right section is 'Select NFS Version' with two checked checkboxes: 'NFSv3' and 'NFSv4'. At the bottom, there's a 'Custom Export Policy' section with a text input field containing '0.0.0.0/0' and an information icon to its right.

## CIFS

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

The screenshot shows the 'Volumes Protocol' configuration window. At the top, there's a section 'Select the volume's protocol:' with three radio buttons: 'NFS Protocol', 'CIFS Protocol' (selected), and 'iSCSI Protocol'. Below this, there are two main sections. The left section is 'Share Name' with a text input field containing 'tami\_share'. The right section is 'Users/Groups' with a text input field containing 'Everyone;' and an information icon to its right. At the bottom, there's a 'Permissions' section with a dropdown menu showing 'Full Control'.

4. 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 a Workgroup setup, enter the server and workgroup name for a workgroup configured for CIFS.
  - 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 <b>Enable NTP Server Configuration</b> 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 <a href="#">BlueXP automation docs</a> for details.

## iSCSI

You can connect your LUN using an existing initiator group or by creating a new one. To map an existing initiator group, select your operating system and one or more initiator groups.

To create a new initiator group:

1. Select **Create new**.
2. Select your operating system.
3. Click to add one or more host iSCSI qualified names (IQN). You can select existing IQNs or add new IQNs. For details on how to find the IQN for a volume, see [Connect a host to a LUN](#).
4. Enter an **Initiator Group Name**.

**Volumes Protocol**

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

Initiator Group [Learn about Initiator group and LUNs](#)

Select the Initiator Group: ☐ Map Existing ☒ Create New

Operating System Type Host Initiator - IQN

Linux [+ Select an existing, or add a new IQN](#)

Initiator Group Name

## 5. 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.

**Usage Profile & Tiering Policy**

**Usage Profile**

**Storage Efficiency**

☐ Enabled - Deduplication, compression and compaction

☒ Disabled - No Efficiency

**Tiering data to object storage**

**Tiering policy**

☐ Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.

☒ Snapshot Only - Tiers cold Snapshot copies to object storage.

☐ None - Data tiering is disabled.

☐ All - Immediately tiers all data (not including metadata) to object storage.

- c. If you selected optimization (FlexGroup), you must specify the number of constituents to distribute

volume data across. We strongly recommend using an even number of constituents to ensure even data distribution.

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

## Result

The new volume is added to the working environment.

## Mount volumes

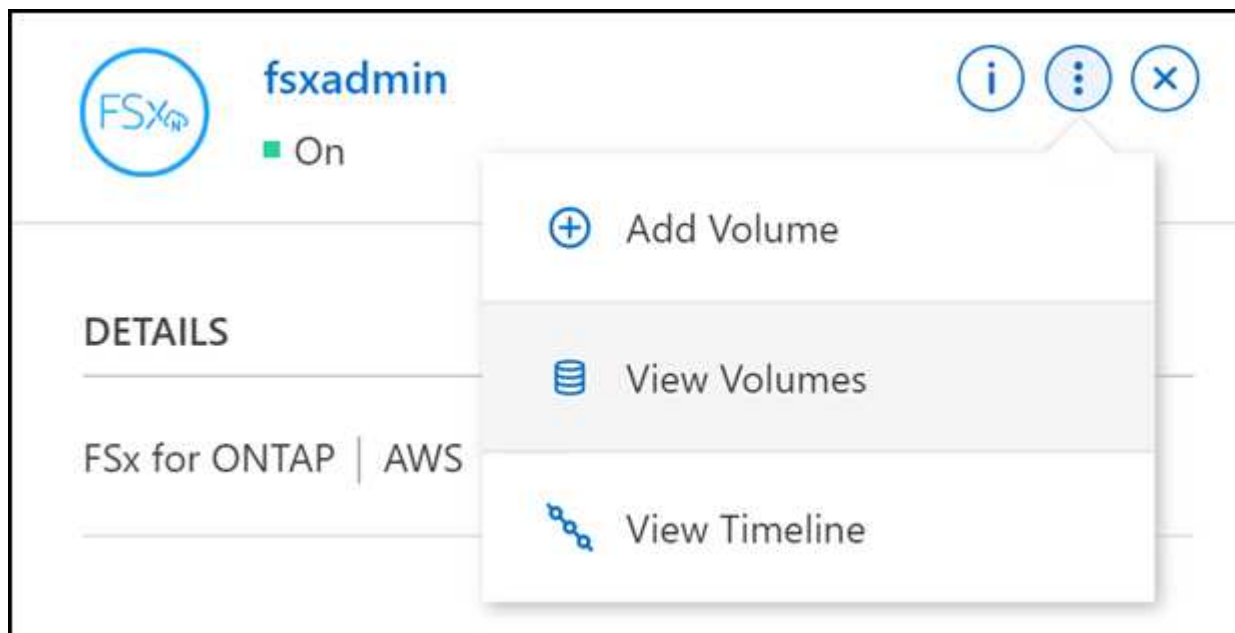
Access mounting instructions from within BlueXP so you can mount the volume to a host.

### About this task

You can mount volumes by opening the working environment and selecting the **Volumes** tab or simply using working environment **Details** panel from the Canvas. This task describes adding volumes using the **Details** panel.

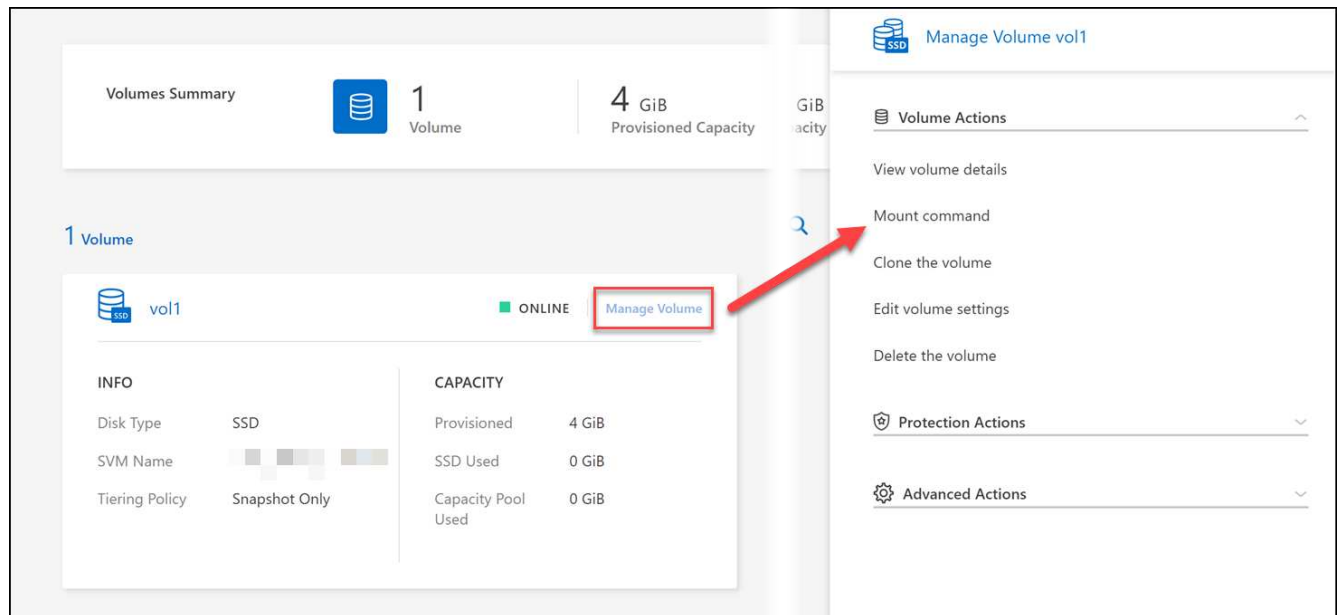
### Steps

1. Select the FSx for ONTAP working environment on the Canvas.
2. In the **Details** panel, use the three dots icon (⋮) to open the options menu. Click **View Volumes**.



3. Use **Manage Volumes** to open the **Volume Actions** menu. Click **Mount command** and follow the instructions to mount the volume.





## Result

Your volume is now mounted to the host.

# Manage volumes for FSx for ONTAP

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

## View volume details

After you create a volume, you can view the configuration details.

1. Open the working environment.



You can hover over the volume name to display the volume type.

2. Open the volume tab and select **Manage Volume** to open the **Volume Actions** menu.
3. Select **View volume details**.

## Edit volumes

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

### Steps

1. Open the working environment.
2. Open the volume tab and select **Manage Volume** to open the **Volume Actions** menu.
3. Select **Edit volume settings**.
4. Select **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 tab and select **Manage Volume** to open the **Volume Actions** menu.
3. Select **Clone the volume**.
4. Enter a name for the cloned volume.
5. Select **Clone**.

## Manage volume tags

You can add, modify, or delete volume tags. Tags added in BlueXP are reflected in the AWS Management Console. It can take up to an hour to synchronize tags with the AWS Management Console.



You cannot edit volume tags you created in BlueXP until they sync with AWS. This can take up to an hour. If the **Manage volume tags** option is grayed out, AWS has not yet synced the volume tags.

### Steps

1. Open the working environment.
2. Open the volume tab and select **Manage Volume** to open the **Volume Actions** menu.
3. Select **Manage volume tags**.
4. Select **Save** to apply your changes.

## 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 tab and select **Manage Volume** to open the **Protection Actions** menu.
3. Select one of the available options to manage Snapshot copies:
  - **Create a Snapshot copy**
  - **Restore from a Snapshot copy**
4. 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 tab and select **Manage Volume** to open the **Advanced Actions** menu.

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

## 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 BlueXP. SnapMirror volumes must be deleted using the AWS Management Console or CLI.

### Steps

1. Open the working environment.
2. Open the volume tab and select **Manage Volume** to open the **Volume Actions** menu.
3. Select **Delete the volume**.
4. 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 BlueXP.



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

## Add and manage storage VMs for FSx for ONTAP

After you create your working environment, you can add, view, and manage a storage virtual machine (VM)--also referred to as an *SVM*--on a managed FSx for ONTAP cluster.

### Add a storage VM

Using BlueXP, you can add storage VMs to the FSx for ONTAP file system up to the maximum number allowed. Refer to [AWS: Managing FSx for ONTAP storage virtual machines](#) for details.

### About this task

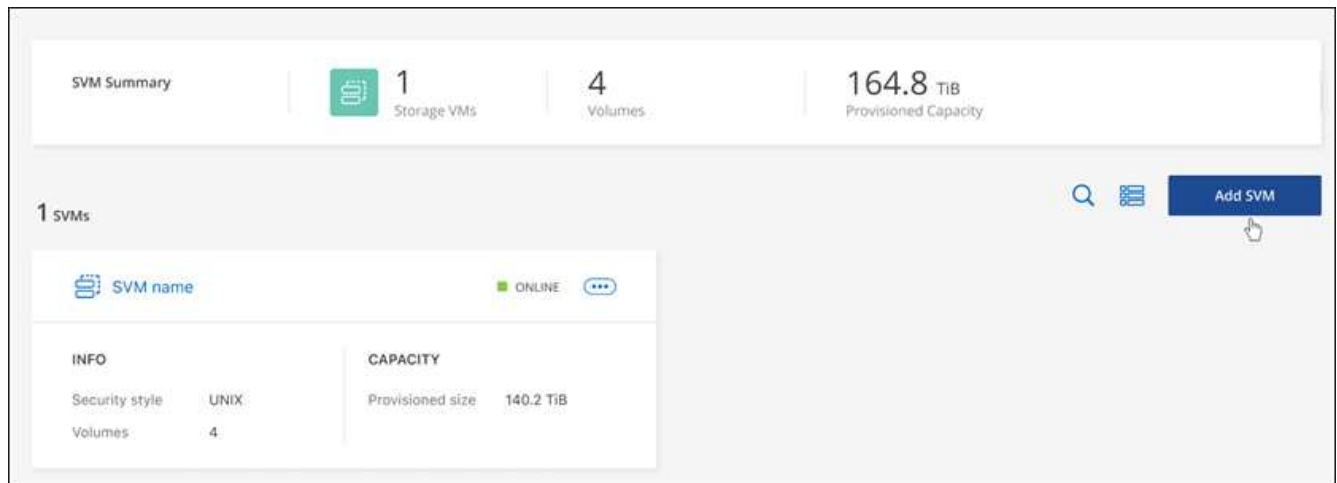
You can add a storage VM by opening the working environment and selecting the **Storage VMs** tab or from the working environment **Overview** panel. This task describes adding a storage VM using the **Storage VMs** panel.

### Before you begin

- You need an active [Connector in AWS](#).
- Create one or more storage VMs. Refer to [Manage storage VMs in BlueXP](#) for details.

### Steps

1. Select the FSx for ONTAP working environment on the Canvas. If you don't have a Connector enabled, you'll be prompted to add one.
2. Select the **Storage VMs** panel. Existing SVMs are displayed. Select **Add SVM** to add a new SVM.



### 3. Add storage virtual machine

- Enter the name of your storage VM.
- Select the configured storage VM root volume security style. Valid values are **UNIX**, **NTFS**, or **Mixed**.
- Optionally, specify a storage VM administrative password.
- Optionally, create up to fifty tags to categorize your SVM by clicking the plus sign and entering a tag name and value.
- Select **Add** to add the storage VM.

#### Result

The new storage VM is added to the working environment and the FSx for ONTAP file system.

## Manage a storage VM

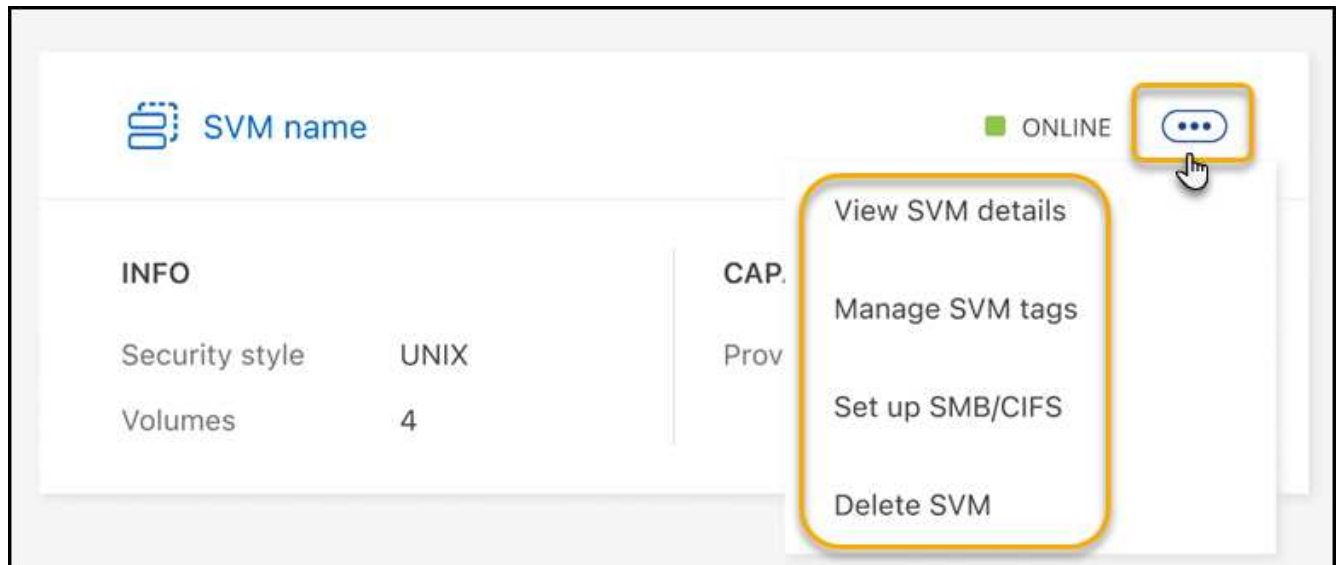
You can view storage VM details, manage tags, set up an SMB/CIFS connection, or delete a storage SVM.

#### Before you begin

You need an active [Connector in AWS](#).

#### Steps

- Select the FSx for ONTAP working environment on the Canvas. If you don't have a Connector enabled, you'll be prompted to add one.
- Select the **Storage VMs** panel.
- Use the three dots (⋮) to open the options menu for the storage VM.



4. Select a menu option to view or manage the storage VM settings.

- **View SVM details:** You can review details including root volume, security style, allowed protocols, Active Directory domain, and tags.
- **Manage SVM tags:** You can add, edit, or remove storage VM tags. Changes you make will sync with the AWS Management Console.
- **Set up SMB/CIFS:** If this is the first CIFS connection for this working environment, you will be prompted to configure CIFS connectivity using an *Active Directory* or *Workgroup* setup.
  - If you select a Workgroup setup, enter the server and workgroup name for a workgroup configured for CIFS.
  - If you select an Active Directory setup, you'll need to provide the following configuration information.

## Active Directory configuration

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 <b>Enable NTP Server Configuration</b> 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 <a href="#">BlueXP automation docs</a> for details.

- **Delete SVM:** You can delete the storage VM. You must verify the storage VM name to delete it.



You must delete all volumes on the storage VM before deleting the storage VM.

# Knowledge and support

## Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

## Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

## Register your BlueXP account for NetApp support

To register for support and activate support entitlement, one user in your BlueXP account must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

### Existing customer with an NSS account

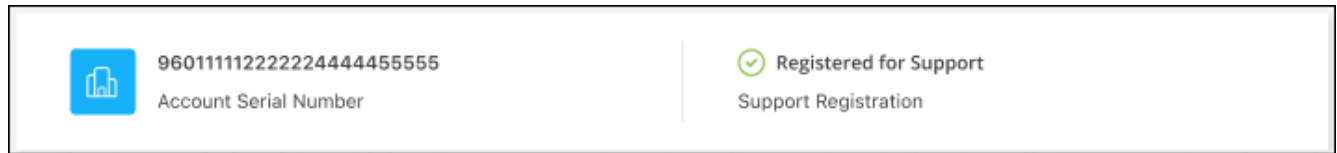
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

#### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

The **Resources** page should show that your account is registered for support.



Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP account is not registered for support. As long as one user in the account has followed these steps, then your account has been registered.

### Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

#### Steps

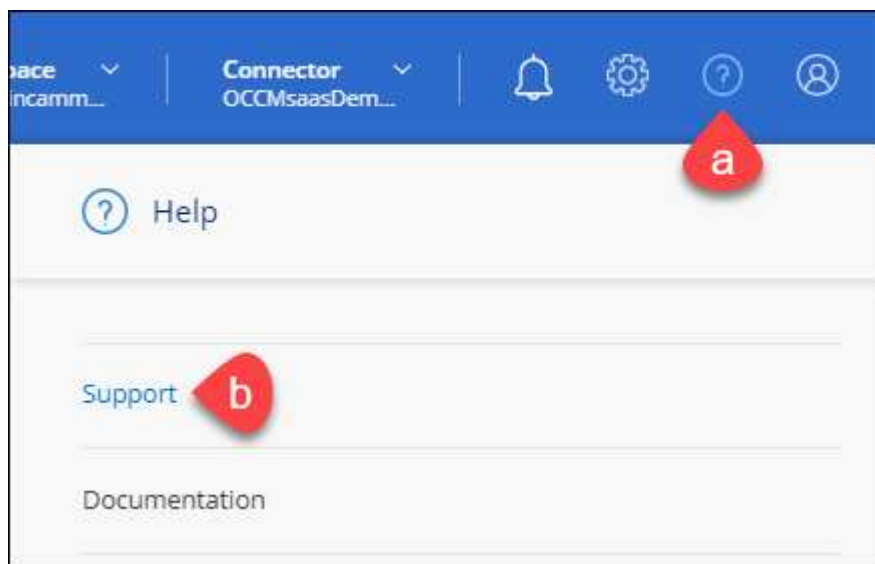
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

### Brand new to NetApp

If you are brand new to NetApp and you don't have an NSS account, follow each step below.



#### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.





2. Locate your account ID serial number from the Support Registration page.

 96015585434285107893 Account serial number	 Not Registered Add your NetApp Support Site (NSS) <a href="#">credentials</a> to BlueXP Follow these <a href="#">instructions</a> to register for support in case you don't have an NSS account yet.
--	--

3. Navigate to [NetApp's support registration site](#) and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

### After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

## Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP account is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

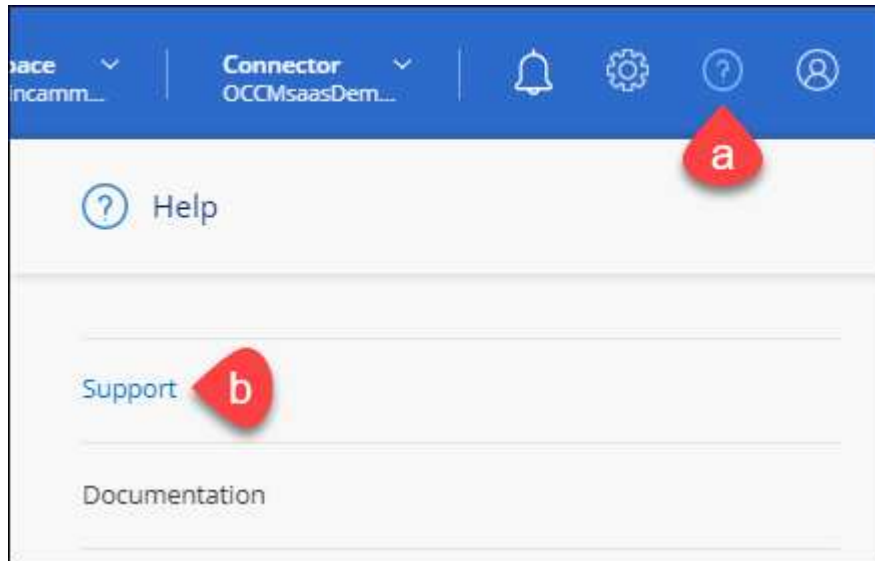
Associating NSS credentials with your BlueXP account is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP account ID. Users who belong to the BlueXP account can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

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

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.


Note the following:


- The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

- Upon successful login, NetApp will store the NSS user name.

This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the  menu.

- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the  menu.

Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

## Get help

NetApp provides support for BlueXP 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.

### Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

### Use self-support options

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

- **Documentation**

The BlueXP documentation that you're currently viewing.

- [Knowledge base](#)

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

- [Communities](#)

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

### Create a case with NetApp support

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

#### Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. [Learn how to manage credentials associated with your BlueXP login.](#)
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be associated with the serial number for that system.

## Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:
  - a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.
  - b. Select **Create a Case** to open a ticket with a NetApp Support specialist:
    - **Service:** Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
    - **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.


The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.

- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.
- **Attachment (Optional):** Upload up to five attachments, one at a time.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

ntapitdemo 

NetApp Support Site Account


---

Service

Select ▼

Working Enviroment


Select ▼

Case Priority 

Low - General guidance ▼

Issue Description



Provide detailed description of problem, applicable error messages and troubleshooting steps taken.



Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

### After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

## Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

### Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
  - Under **Organization's cases**, select **View** to view all cases associated with your company.
  - Modify the date range by choosing an exact date range or by choosing a different time frame.

Search: Cases opened on the last 3 months Create a case

Date created	Last updated		Status (5)	
December 22, 2022	December 29, 2022	Last 7 days	Assigned	...
December 21, 2022	December 28, 2022	Last 30 days	Active	...
December 15, 2022	December 27, 2022	Last 3 months	Pending customer	...
December 14, 2022	December 26, 2022	Medium (P3)	Solution proposed	...
		Low (P4)		

Apply Reset

- Filter the contents of the columns.

Search: Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Active	...
December 28, 2022	High (P2)	Pending customer	...
December 27, 2022	Medium (P3)	Solution proposed	...
December 26, 2022	Low (P4)	Pending closed	...
		Closed	...

Apply Reset

- Change the columns that appear in the table by selecting + and then choosing the columns that you'd like to display.

Search: Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Last updated	...
December 28, 2022	High (P2)	Priority	...
December 27, 2022	Medium (P3)	Cluster name	...
December 26, 2022	Low (P4)	Case owner	...
		Opened by	...

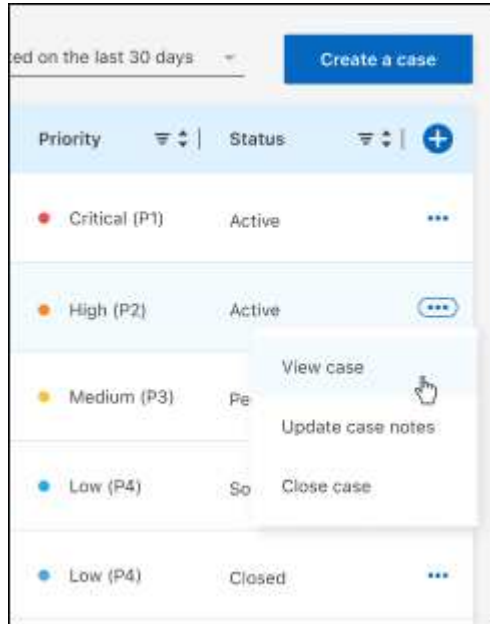
Apply Reset

4. Manage an existing case by selecting ... and selecting one of the available options:

- **View case:** View full details about a specific case.
- **Update case notes:** Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

- **Close case:** Provide details about why you're closing the case and select **Close case**.





# Legal notices

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

## Copyright

<https://www.netapp.com/company/legal/copyright/>

## 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.

<https://www.netapp.com/company/legal/trademarks/>

## Patents

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

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

## Open source

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

[Notice for BlueXP](#)

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.