Amazon FSx for NetApp ONTAP management

Amazon FSx for NetApp ONTAP

NetApp
February 17, 2026

Table of Contents

Amazon FSx for NetApp ONTAP management

What’s new with Amazon FSx for NetApp ONTAP

Learn what’s new in FSx for ONTAP.

16 February 2026

Support for storage VM migration

NetApp Workload Factory now supports migration for storage VMs. This feature allows migration of ONTAP storage system data and configurations from on-premises ONTAP systems or first-generation FSx for ONTAP file systems to second-generation FSx for ONTAP file systems. You can replicate storage VM data and configuration settings to move to the new file system with minimal downtime and disruption to users and applications.

To use this feature, create a replication relationship and select **Migration** as the use case. To complete the migration process, you must cut over the storage VM and its replicated volumes immediately to permanently migrate data and storage VM configuration settings to the target FSx for ONTAP file system.

09 February 2026

Support for replicating data between Cloud Volumes ONTAP and FSx for ONTAP

Data replication is now available between a Cloud Volumes ONTAP system and an FSx for ONTAP file system from the NetApp Console.

Replicate data

17 November 2025

System Manager available when using an AWS Lambda link

The ONTAP System Manager interface can be used with an AWS Lambda link to perform advanced ONTAP operations. This provides an alternative to using a Console agent with System Manager for managing an FSx for ONTAP file system directly from the Console. Learn about using links for advanced ONTAP operations

11 November 2025

Support for replication between on-premises ONTAP systems and FSx for ONTAP file systems

Data replication is available between an on-premises ONTAP system and an FSx for ONTAP file system from the NetApp Console Systems page.

Replicate data

06 October 2025

BlueXP is now NetApp Console

The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration, that is highly secure and compliant.

For details on what’s changed, see the NetApp Console release notes.

03 August 2025

Enhancements to Replication relationships tab

We’ve added several new columns to the replication relationships table to give you more information about your replication relationships in the **Replication relationships** tab. The table now includes the following columns:

- SnapMirror policy
- Source file system
- Target file system
- State of the relationship
- Last transfer time

14 July 2025

Support for replicating data between two FSx for ONTAP file systems

Data replication is now available between two FSx for ONTAP file systems from the canvas in the BlueXP console.

Replicate data

29 June 2025

Credentials update

After you set up credentials and permissions for your FSx for ONTAP file system, you’ll be redirected to the BlueXP Credentials page. From this page, you can rename or remove your FSx for ONTAP credentials.

Set up permissions for FSx for ONTAP file systems

04 May 2025

Tracker response support

Tracker now provides API responses so that you can see the REST API output related to the task.

Link authentication support for AWS Secrets Manager

You now have the option to use secrets from AWS Secrets Manager to authenticate links so that you don’t have to use credentials stored in BlueXP Workloads.

Connect to an FSx for ONTAP file system with a Lambda link

Implement best practices for an FSx for ONTAP file system

BlueXP Workloads provides a dashboard where you can review the well-architected status of your file system configurations. You can leverage this analysis to implement best practices for your FSx for ONTAP file systems. File system configuration analysis includes the following configurations: SSD capacity threshold, scheduled local snapshots, scheduled FSx for ONTAP backups, data tiering, and remote data replication.

- Learn about the well-architected analysis for file system configurations
- Implement best practices for your file systems

Well-architected notification for file system issues

In the BlueXP console, FSx for ONTAP file systems with well-architected issues now display a notification in the Canvas indicating when file systems have issues to fix.

Updated permissions terminology

The workload factory user interface and documentation now use "read-only" to refer to read permissions and "read/write" to refer to automate permissions.

30 March 2025

iam:SimulatePermissionPolicy permission update

Now you can manage the `iam:SimulatePrincipalPolicy` permission from the BlueXP console when you add additional AWS account credentials or add a new workload capability such as the GenAI workload.

Permissions reference change log

02 March 2025

CloudShell events in Tracker

Anytime you use CloudShell to execute FSx for ONTAP operations from BlueXP Workloads, the events appear in Tracker.

Learn how to monitor and track FSx for ONTAP operations in BlueXP

02 February 2025

Associate FSx for ONTAP file system with a workspace in BlueXP

After BlueXP integration in November 2024, newly created FSx for ONTAP file systems were not associated with one workspace in BlueXP. Now when you create or discover FSx for ONTAP file systems, they are associated with one workspace within a BlueXP account.

If you have existing FSx for ONTAP file systems that are not associated with a workspace, we will help you associate them with a workspace in BlueXP. You can create a case with NetApp Support from within the BlueXP console. Select **Workload Factory** as the service.

File system removal from BlueXP canvas

You can now remove an FSx for ONTAP file system from a workspace in the BlueXP canvas. This operation dissociates the file system from one workspace so that you can associate it with another workspace within the same BlueXP account.

Learn how to remove an FSx for ONTAP file system from a workspace in BlueXP

Tracker available for monitoring and tracking operations

Tracker, a new monitoring capability, is available in BlueXP Amazon FSx for NetApp ONTAP. You can use Tracker to monitor and track the progress and status of credentials, storage, and link operations, review details for operation tasks and subtasks, diagnose any issues or failures, edit parameters for failed operations, and retry failed operations.

Learn how to monitor and track FSx for ONTAP operations in BlueXP

CloudShell available in BlueXP Workloads

CloudShell is available when you're in BlueXP Workloads within the BlueXP console. CloudShell allows you to use the AWS and ONTAP credentials you've provided in your BlueXP account and execute AWS CLI commands or ONTAP CLI commands in a shell-like environment.

Use CloudShell

06 January 2025

NetApp releases additional CloudFormation resources

NetApp now provides CloudFormation resources that allow customers to utilize advanced ONTAP components which are not exposed within the AWS console. CloudFormation is the infrastructure-as-code mechanism for AWS. You'll be able to create replication relationships, CIFS shares, NFS export policies, snapshots, and more.

Manage Amazon FSx for NetApp ONTAP file systems using CloudFormation

11 November 2024

FSx for ONTAP integrates with Storage in BlueXP Workload Factory

FSx for ONTAP file system management tasks such as adding volumes, expanding file system capacity, and managing storage VMs are now managed in BlueXP workload factory, a new service offered by NetApp and Amazon FSx for NetApp ONTAP. You can use your existing credentials and permissions just as before. The difference is that you can now do more from BlueXP workload factory to manage your file systems. When you open an FSx for ONTAP working environment from the BlueXP canvas, you will go directly to BlueXP workload factory.

Learn about FSx for ONTAP features in BlueXP workload factory

If you're looking for the *advanced view* option, which enables you to manage an FSx for ONTAP file system using ONTAP System Manager, you can now find that option from the BlueXP canvas after you select the working environment.

30 July 2023

Support for three additional regions

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

Add a storage VM

You can now add a storage VM to the Amazon FSx for NetApp ONTAP file system using BlueXP.

My Opportunities tab is now My estate

The **My Opportunities** tab is now **My estate**. The documentation is updated to reflect the new name.

04 June 2023

Maintenance window start time

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.

Distribute volume data using FlexGroups

When creating a volume, you can enable data optimization by creating a FlexGroup to distribute data across volumes.

07 May 2023

Generate a security group

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.

Add or modify tags

You can optionally add and modify tags to categorize volumes.

02 April 2023

Increase in IOPS limit

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

05 March 2023

User interface enhanced

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

01 January 2023

Automatic capacity management

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 cluster's maximum capacity.

18 September 2022

Change storage capacity and IOPS

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

31 July 2022

My estate feature

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

Change throughput capacity

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

Replicate and sync data

You can now replicate and sync data to on-premises and other FSx for ONTAP systems using FSx for ONTAP as the source.

Create iSCSI volume

You can now create iSCSI volumes in FSx for ONTAP using Cloud Manager.

3 July 2022

Support for single or multiple Availability Zon

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

Create an FSx for ONTAP working environment

Support for GovCloud account authentication

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 elect 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.

NetApp Console

Amazon FSx for NetApp ONTAP management is accessible through the NetApp Console.

The NetApp Console provides centralized management of NetApp storage and data services across on-premises and cloud environments at enterprise grade. The Console is required to access and use NetApp data services. As a management interface, it enables you to manage many storage resources from one interface. Console administrators can control access to storage and services for all systems within the enterprise.

You don't need a license or subscription to start using NetApp Console and you only incur charges when you need to deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

Learn more about the NetApp Console.

Using FSx for ONTAP from the NetApp Console

From the NetApp Console systems page, you can create and discover FSx for ONTAP systems and use System Manager and other NetApp services. If you want to manage FSx for ONTAP systems and workloads running on Amazon FSx for NetApp ONTAP, use NetApp Workload Factory.

Learn how to create and discover FSx for ONTAP systems from the NetApp Console.

Features

- No need to configure or manage storage devices, software, or backups.
- Support for CIFS, iSCSI, NFSv3, NFSv4.x, S3, 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 NetApp Console

- FSx for ONTAP is supported when using NetApp Console in *standard* mode, which leverages the NetApp Console SaaS layer to provide full functionality. *Restricted* mode and *private* mode are not supported.

Refer to NetApp Console deployment modes for more information.

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

Console agents and links unlock all FSx for ONTAP features

Console agents and links enable connectivity and trust relationships between the NetApp Console and Amazon FSx for NetApp ONTAP working environments. A Console agent is NetApp software that runs in your cloud or on-premises network, and a link uses AWS Lambda to execute NetApp code. You don’t need a Console agent or link to get started in the Console or create FSx for ONTAP systems, but you do need to use a Console agent or link to make full use of FSx for ONTAP features.

You need a Console agent or link to use the following features:

- Well-architected status of FSx for ONTAP file system configurations for proactive maintenance, reliability, and cost-performance optimization
- NetApp Autonomous Ransomware Protection (ARP/AI)
- Enhanced holistic capacity observability across FSx for ONTAP file systems
- Volume and storage VM data replication, management, and monitoring
- SMB/CIFS shares and NFS export policy provisioning and management
- Management of iSCSI volumes on an FSx for ONTAP file system
- Creation and management of snapshot policies for custom protection SLA
- Inode management enhancements for automatic capacity management
- Volume autogrow for elastic scaling
- Clone creation and management, for instant, in-place, data cloning
- Displaying additional metrics directly from ONTAP such as the ONTAP version

Learn more about Console agents and links and when you should use them:

- Learn more about Console agents.
- Learn more about links.

Cost

Your FSx for ONTAP account is maintained by AWS and not by NetApp. Refer to Amazon FSx for NetApp ONTAP getting started guide.

There is an additional cost associated with using the Console agent or link in AWS, and the optional data services such as NetApp Data Classification and NetApp Copy and Sync.

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 and technical support issues specific to the NetApp Console or NetApp storage solutions and services, you can open a NetApp support ticket using your NetApp organization level serial number. You will need to register your NetApp organization to activate support.

Quick start for Amazon FSx for NetApp ONTAP

Get started with Amazon FSx for NetApp ONTAP in the NetApp Console by adding credentials, creating a Console agent or link, and by creating or discovering a file system.

❶ Add credentials and permissions

Adding AWS credentials is required to provide the NetApp Console with the permissions needed to create and manage FSx for ONTAP file systems. You can choose between *read-only* and *read/write* permissions.

❷ Optional: Create a Console agent or a link

To perform some management tasks from the NetApp Console, you either need a Console agent or a NetApp Workloads link. A *Console agent* is a virtual machine that you deploy in your VPC to manage your FSx for ONTAP file systems. A *link* leverages AWS Lambda to create a trust relationship and connectivity to your FSx for ONTAP file systems.

- Learn when a Console agent or link is required for FSx for ONTAP management
- Learn how to create a Console agent in AWS
- Learn how to create a Console agent on-premises
- Learn how to create a link

❸ Create or discover an FSx for ONTAP system

Create your FSx for ONTAP file system directly from the NetApp Console or discover a file system that you've already created in your AWS environment.

Set up permissions for FSx for ONTAP

To create or manage an FSx for ONTAP file system, you need to add AWS credentials in the NetApp Console by providing the ARN of an IAM role that gives the permissions needed to create an FSx for ONTAP system from the NetApp Console.

Why AWS credentials are required

AWS credentials are required to create and manage FSx for ONTAP systems from the NetApp Console. You can create new AWS credentials or add AWS credentials to an existing organization. Credentials provide the permissions needed to manage resources and processes within your AWS cloud environment from the NetApp Console.

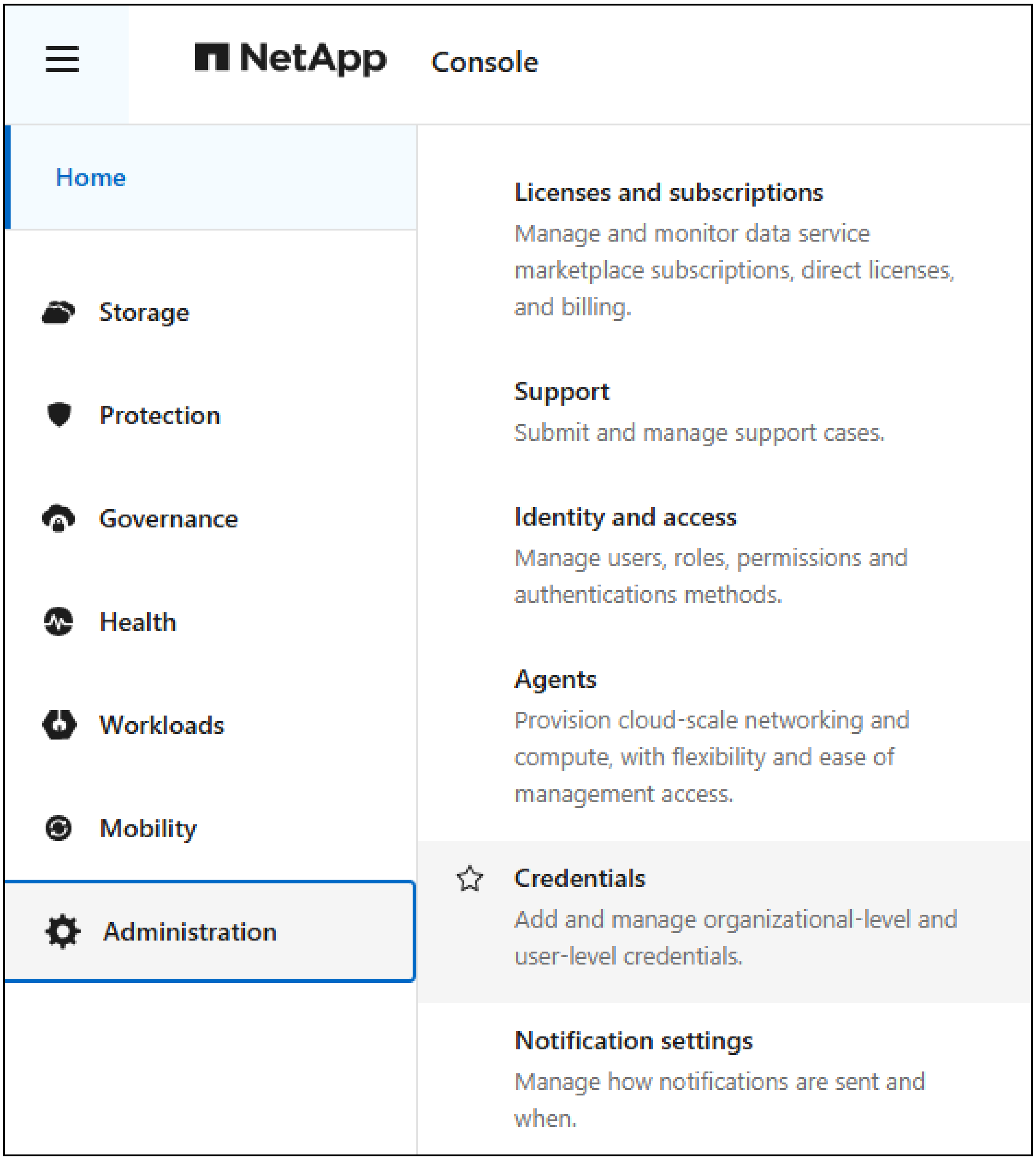
Credentials and permissions are managed via NetApp Workload Factory. Workload Factory is a life-cycle management platform designed to help users optimize workloads using Amazon FSx for NetApp ONTAP file systems. The NetApp Console uses the same set of AWS credentials and permissions as Workload Factory.

The Workload Factory interface provides FSx for ONTAP users with options to enable workload capabilities like Storage, VMware, Databases, and GenAI, and to select permissions for the workloads. *Storage* is the storage management capability in Workload Factory and it is the only capability you need to enable and add credentials for to create and manage your FSx for ONTAP file systems.

About this task

When adding new credentials for FSx for ONTAP from Storage in Workload Factory, you’ll need to decide which permission policies you’d like to grant. To discover AWS resources like FSx for ONTAP file systems, you’ll need *view, planning, and analysis* permissions. To deploy FSx for ONTAP file systems, you’ll need *file system creation and deletion* permissions. You can do basic operations for FSx for ONTAP without permissions. Learn more about permissions.

New and existing AWS credentials are viewable from the Administration menu on the **Credentials** page.



Licenses and subscriptions
Manage and monitor data service marketplace subscriptions, direct licenses, and billing.

Support
Submit and manage support cases.

Identity and access
Manage users, roles, permissions and authentications methods.

Agents
Provision cloud-scale networking and compute, with flexibility and ease of management access.

☆ **Credentials**
Add and manage organizational-level and user-level credentials.

Notification settings
Manage how notifications are sent and when.

You can add credentials using two methods:

- **Manually**: You create the IAM policy and the IAM role in your AWS account while adding credentials in Workload Factory.
- **Automatically**: You capture a minimal amount of information about permissions and then use a CloudFormation stack to create the IAM policies and role for your credentials.

Add credentials to an account manually

You can add AWS credentials to the NetApp Console manually to give your account the permissions needed to manage the AWS resources that you'll use to run your unique workloads. Each set of credentials that you add will include one or more IAM policies based on the workload capabilities you want to use, and an IAM role that is assigned to your account.

There are three parts to creating the credentials:

- Select the services and permissions level that you would like to use and then create IAM policies from the AWS Management Console.
- Create an IAM role from the AWS Management Console.
- From Workloads in the NetApp Console, enter a name and add the credentials.

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

Before you begin

You'll need to have credentials to log in to your AWS account.

Steps

1. From the NetApp Console menu, select **Administration** and then **Credentials**.
2. From the **Organization credentials** page, select **Add credentials**.
3. Select **Amazon Web Services**, then **FSx for ONTAP**, and then **Next**.

   You're now on the **Add Credentials** page in NetApp Workloads.

4. Select **Add manually** and then follow the steps below to fill out the three sections under *Permissions configuration*.

Step 1: Select the storage capability and create the IAM policy

In this section, you'll choose the storage capability to be managed as part of these credentials, and the permissions enabled for storage. You also have the option to select other workloads like Databases, GenAI, or VMware. Once you've made your selections, you'll need to copy the policy permissions for each selected workload from the Codebox and add them into the AWS Management Console within your AWS account to create the policies.

Steps

1. From the **Create policies** section, enable each of the workload capabilities that you want to include in these credentials. Enable **Storage** to create and manage file systems.

   You can add additional capabilities later, so just select the workloads that you currently want to deploy and manage.

2. For those workload capabilities that offer a choice of permission policies, select the type of permissions that will be available with these credentials. Learn about the permissions.
3. Optional: Select **Enable automatic permissions check** to check if you have the required AWS account permissions to complete workload operations. Enabling the check adds the `iam:SimulatePrincipalPolicy permission` to your permission policies. The purpose of this permission is to confirm permissions only. You can remove the permission after adding credentials, but we recommend keeping it to prevent resource creation for partially successful operations and to save you from any required manual resource cleanup.
4. In the Codebox window, copy the permissions for the first IAM policy.
5. Open another browser window and log in to your AWS account in the AWS Management Console.
6. Open the IAM service, and then select **Policies** > **Create Policy**.
7. Select JSON as the file type, paste the permissions you copied in step 3, and select **Next**.

8. Enter the name for the policy and select **Create Policy**.
9. If you've selected multiple workload capabilities in step 1, repeat these steps to create a policy for each set of workload permissions.

Step 2: Create the IAM role that uses the policies

In this section you'll set up an IAM role that Workload Factory will assume that includes the permissions and policies that you just created.

Steps

1. In the AWS Management Console, select **Roles > Create Role**.
2. Under **Trusted entity type**, select **AWS account**.
   a. Select **Another AWS account** and copy and paste the account ID for FSx for ONTAP workload management from the Workloads user interface.
   b. Select **Required external ID** and copy and paste the external ID from the Workloads user interface.
3. Select **Next**.
4. In the Permissions policy section, choose all the policies that you defined previously and select **Next**.
5. Enter a name for the role and select **Create role**.
6. Copy the Role ARN.
7. Return to the Workloads Add credentials page, expand the **Create role** section, and paste the ARN in the *Role ARN* field.

Step 3: Enter a name and add the credentials

The final step is to enter a name for the credentials in Workloads.

Steps

1. From the Workloads Add credentials page, expand **Credentials name**.
2. Enter the name that you want to use for these credentials.
3. Select **Add** to create the credentials.

Result

The credentials are created and viewable on the Credentials page. You can now use the credentials when creating an FSx for ONTAP working environment. Whenever required, you can rename credentials or remove them from the NetApp Console.

Add credentials to an account using CloudFormation

You can add AWS credentials to Workloads using an AWS CloudFormation stack by selecting the workload capabilities that you want to use, and then launching the AWS CloudFormation stack in your AWS account. CloudFormation will create the IAM policies and IAM role based on the workload capabilities you selected.

Before you begin

- You'll need to have credentials to log in to your AWS account.
- You'll need to have the following permissions in your AWS account when adding credentials using a CloudFormation stack:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

Steps

1. From the NetApp Console menu, select **Administration** and then **Credentials**.
2. Select **Add credentials**.
3. Select **Amazon Web Services**, then **FSx for ONTAP**, and then **Next**.

   You’re now on the **Add Credentials** page in NetApp Workloads.

4. Select **Add via AWS CloudFormation**.
5. Under **Create policies**, enable each of the workload capabilities that you want to include in these credentials and choose a permission level for each workload.

   You can add additional capabilities later, so just select the workloads that you currently want to deploy and manage.

6. Optional: Select **Enable automatic permissions check** to check if you have the required AWS account permissions to complete workload operations. Enabling the check adds the `iam:SimulatePrincipalPolicy` permission to your permission policies. The purpose of this

permission is to confirm permissions only. You can remove the permission after adding credentials, but we recommend keeping it to prevent resource creation for partially successful operations and to save you from any required manual resource cleanup.

7. Under **Credentials name**, enter the name that you want to use for these credentials.
8. Add the credentials from AWS CloudFormation:
    a. Select **Add** (or select **Redirect to CloudFormation**) and the Redirect to CloudFormation page is displayed.
    b. If you use single sign-on (SSO) with AWS, open a separate browser tab and log in to the AWS Console before you select **Continue**.

       You should log in to the AWS account where the FSx for ONTAP file system resides.
    c. Select **Continue** from the Redirect to CloudFormation page.
    d. On the Quick create stack page, under Capabilities, select **I acknowledge that AWS CloudFormation might create IAM resources**.
    e. Select **Create stack**.
    f. Return to **Administration** > **Credentials** page from the main menu to verify that the new credentials are in progress, or that they have been added.

Result

The credentials are created and viewable on the Credentials page. You can now use the credentials when creating an FSx for ONTAP working environment. Whenever required, you can rename credentials or remove them from the NetApp Console.

Create or discover an FSx for ONTAP file system

Create or discover an FSx for ONTAP file system to add and manage volumes and additional data services from the NetApp Console.

Create an FSx for ONTAP system

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

About this task

A storage VM is created when you create a file system.

Before you begin

Before creating your FSx for ONTAP file system, you will need:

- The ARN of an IAM role that gives Workload Factory the permissions needed to create an FSx for ONTAP file system. Learn how to grant permissions to an AWS account.
- The region and VPC information for where you will create the FSx for ONTAP instance.

Create an FSx for ONTAP file system

You can create an FSx for ONTAP file system using *Quick create* or *Advanced create*. You can also use the following tools available in the Codebox: REST API, CloudFormation, and Terraform. Learn how to use Codebox for automation.

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

Quick create

Quick create enables you to use a recommended best-practice configuration. You can change most settings after you create an FSx for ONTAP file system.

Steps

1. From the NetApp Console menu, select **Storage** and then **Management**.
2. Select **Add system** from the Systems page.
3. Select **Amazon Web Services** as the location, and then select **Add new** for Amazon FSx for NetApp ONTAP.
4. On the Create FSx for ONTAP file system page, select **Quick create**.

   You can also load a saved configuration.

5. Under File system general configuration, provide the following:
   a. **AWS credentials**: Select to add AWS credentials in Workload Factory or continue without credentials.
   b. **File system name**: Enter a name for the file system.
   c. **Region & VPC**: Select the region and VPC for the file system.
   d. **Deployment type**: Select a deployment type.
      - Single Availability Zone (Single-AZ) deployment: provides availability by monitoring for hardware failures and automatically replacing infrastructure components in the event of a failure. Achieves high durability by automatically replicating your data within an Availability Zone to protect it from component failure.

        This configuration is recommended for high performance workloads or when workloads start small and incrementally scale out to 72 GB/s of throughput and 2.4 million IOPS.

      - Multiple Availability Zones (Multi-AZ) deployment: provides continuous availability to data even when an Availability Zone is unavailable. A Multi-AZ file system is designed for business-critical production workloads that require high availability to shared ONTAP file data and need storage with built-in replication across Availability Zones.

        This single HA-pair configuration is recommended for workloads that require up to 6 GB/s of throughput or 200,000 IOPS.

   e. **Tags**: Optionally, you can add up to 50 tags.
6. Under **File system details**, provide the following:
   a. **SSD storage capacity**: Enter the storage capacity and select the storage capacity unit.
      - For first-generation deployments, you can’t decrease capacity after file system creation.
      - For second-generation deployments, you can increase capacity after file system creation.

   b. **ONTAP credentials**: Optional. Enter your ONTAP user name and password. The password can be set now or later.

      If the user you provide is not the fsxadmin user, and later you need to reset the fsxadmin password, you’ll be able to do this from the AWS console.

   c. **SMB/CIFS setup**: Optional. If you plan to use SMB/CIFS protocol to access volumes, you must configure the Active Directory for the storage VM during file system creation. Provide the following details for the storage VM that is created for this file system.

i. **Active Directory domain to join**: Enter the fully qualified domain name (FQDN) for the Active Directory.
ii. **DNS IP addresses**: Enter up to three DNS IP addresses separated by commas.
iii. **SMB server NetBIOS name**: Enter the SMB server NetBIOS name of the Active Directory computer object to create for your storage VM. This is the name of this storage VM in the Active Directory.
iv. **User name**: Enter the user name of the service account in your existing Active Directory.

    Do not include a domain prefix or suffix. For `EXAMPLE\ADMIN`, use `ADMIN`.

v. **Password**: Enter the password for the service account.
vi. **Organization unit**: Optionally, enter the name of the Organizational Unit where you intend to create the computer account for FSx for ONTAP. The OU is the distinguished path name of the organizational unit to which you want to join the file system.
vii. **Delegated administrators group**: Optionally, enter the name of the group in your Active Directory that can administer your file system.

    If you are using AWS Managed Microsoft AD, you must specify a group such as AWS Delegated FSx Administrators, AWS Delegated Administrators, or a custom group with delegated permissions to the OU.

    If you are joining to a self-managed AD, use the name of the group in your AD. The default group is `Domain Admins`.

7. Open the **Summary** to review the configuration that you defined. If needed, you can change any setting at this time before saving or creating the file system.
8. Save or create the file system.

Result

If you created the file system, the new FSx for ONTAP configuration appears on the Systems page.

You can manage your FSx for ONTAP file systems in several ways, such as from Workloads in the NetApp Console, using ONTAP System Manager, and using AWS CloudFormation. Learn how to manage an FSx for ONTAP file system.

Advanced create

With Advanced create, you set all of the configuration options, including availability, security, backups, and maintenance.

Steps

1. From the NetApp Console menu, select **Storage** and then **Management**.
2. Select **Add system** from the Systems page.
3. Select **Amazon Web Services** as the location, and then select **Add new** for Amazon FSx for NetApp ONTAP.
4. On the Create FSx for ONTAP file system page, select **Advanced create**.

    You can also load a saved configuration.

5. Under File system general configuration, provide the following:
    a. **AWS credentials**: Select to add AWS credentials in Workload Factory or continue without credentials.
    b. **File system name**: Enter a name for the file system.
    c. **Region & VPC**: Select the region and VPC for the file system.
    d. **Deployment type**: Select a deployment type and file system generation. The availability of a second-generation file system depends on the selected region. If the selected region doesn't support second-generation FSx for ONTAP file systems, the deployment type switches to first-generation.
        - Single Availability Zone (Single-AZ) deployment: provides availability by monitoring for hardware failures and automatically replacing infrastructure components in the event of a failure. Achieves high durability by automatically replicating your data within an Availability Zone to protect it from component failure.

          File system generation: Select one of the following:

            - **Second-generation**: This configuration is recommended for high performance workloads or when workloads start small and incrementally scale out to 72 GB/s of throughput and 2.4 million IOPS.
            - **First-generation**: This configuration is ideal for workloads that require up to 4 GB/s or 160,000 IOPS. First-generation file systems can only increase capacity.
        - Multiple Availability Zones (Multi-AZ) deployment: provides continuous availability to data even when an Availability Zone is unavailable. A Multi-AZ file system is designed for business-critical production workloads that require high availability to shared ONTAP file data and need storage with built-in replication across Availability Zones.

          File system generation: Select one of the following:

            - **Second-generation**: This single HA-pair configuration is recommended for workloads that require up to 6 GB/s of throughput or 200,000 IOPS. In a Multi-AZ and second-generation file system, capacity can increase or decrease to match workload demands.
            - **First-generation**: This configuration is ideal for workloads that require up to 4 GB/s or 160,000 IOPS. First-generation file systems can only increase capacity.
    e. **Tags**: Optionally, you can add up to 50 tags.
6. Under File system details, provide the following:
    a. **SSD storage capacity**: Enter the storage capacity and select the storage capacity unit.
        - For first-generation deployments, you can't decrease capacity after file system creation.
        - For second-generation deployments, you can adjust capacity.
    b. **Throughput capacity per HA pair**: Select throughput capacity per number of HA pairs. First-generation file systems support only one HA pair.
    c. **Provisioned IOPS**: Select one of the following options:
        - **Automatic**: For automatic, for every GiB created, 3 IOPS are added.
        - **User-provisioned**: For user-provisioned, enter the IOPS value.
    d. **ONTAP credentials**: Optional. Enter your ONTAP user name and password. The password can be set now or later.

If the user you provide is not the fsxadmin user, and later you need to reset the fsxadmin password, you'll be able to do this from the AWS console.

e. **Storage VM Credentials**: Optional. Enter your user name. Password can be specific to this file system or you can use the same password entered for ONTAP credentials. The password can be set now or later.

f. **SMB/CIFS setup**: Optional. If you plan to use SMB/CIFS protocol to access volumes, you must configure the Active Directory for the storage VM during file system creation. Provide the following details for the storage VM that is created for this file system.

   i. **Active Directory domain to join**: Enter the fully qualified domain name (FQDN) for the Active Directory.

   ii. **DNS IP addresses**: Enter up to three DNS IP addresses separated by commas.

   iii. **SMB server NetBIOS name**: Enter the SMB server NetBIOS name of the Active Directory computer object to create for your storage VM. This is the name of this storage VM in the Active Directory.

   iv. **User name**: Enter the user name of the service account in your existing Active Directory.

   Do not include a domain prefix or suffix. For `EXAMPLE\ADMIN`, use `ADMIN`.

   v. **Password**: Enter the password for the service account.

   vi. **Organization unit**: Optionally, enter the name of the Organizational Unit where you intend to create the computer account for FSx for ONTAP. The OU is the distinguished path name of the organizational unit to which you want to join the file system.

   vii. **Delegated administrators group**: Optionally, enter the name of the group in your Active Directory that can administer your file system.

   If you are using AWS Managed Microsoft AD, you must specify a group such as AWS Delegated FSx Administrators, AWS Delegated Administrators, or a custom group with delegated permissions to the OU.

   If you are joining to a self-managed AD, use the name of the group in your AD. The default group is `Domain Admins`.

7. Under Network & security, provide the following:

   a. **Security group**: Create or use an existing security group.

   For a new security group, refer to security group details for a description of the security group protocols, ports, and roles.

   b. **Availability Zones**: Select availability zones and subnets.

   - For Cluster configuration node 1: Select an availability zone and subnet.
   - For Cluster configuration node 2: Select an availability zone and subnet.

   c. **VPC route tables**: Select the VPC route table to enable client access to volumes.

   d. **Endpoint IP address range**: Select **Floating IP address range outside your VPC** or **Enter an IP address range** and enter an IP address range.

   e. **Encryption**: Select the encryption key name from the dropdown.

8. Under Backup and maintenance, provide the following:

   a. **FSx for ONTAP Backup**: Daily automatic backups are enabled by default. Disable if desired.

    i. **Automatic backup retention period**: Enter the number of days to retain automatic backups.

    ii. **Daily automatic backup window**: Select either **No preference** (a daily backup start time is selected for you) or **Select start time for daily backups** and specify a start time.

  b. **Weekly maintenance window**: Select either **No preference** (a weekly maintenance window start time is selected for you) or **Select start time for 30-minute weekly maintenance window** and specify a start time.

9. Save or create the file system.
   .Result

If you created the file system, the new FSx for ONTAP configuration appears on the Systems page.

You can manage your FSx for ONTAP file systems in several ways, such as from Workloads in the NetApp Console, using ONTAP System Manager, and using AWS CloudFormation. Learn how to manage an FSx for ONTAP file system.

Discover an existing FSx for ONTAP file system

If you previously provided your AWS credentials in the NetApp Console, you can automatically discover FSx for ONTAP file systems from the Discoverable systems page. You can also review available data services.

About this task

You can discover an FSx for ONTAP file system only once within an account and attach it to one workspace. The file system can later be removed and re-associated to a different workspace.

Steps

1. From the NetApp Console menu, select **Storage**, then **Management**, and then **Discoverable systems**.
2. The count of discovered FSx for ONTAP file systems displays. Select **Discover**.
3. Select one or more file systems and select **Discover** to add them to the Systems page.

> - 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 manage the FSx for ONTAP file system from the Console, you’ll receive a prompt to select credentials with the required permissions.
> - The following regions aren’t supported for discovery: China regions, GovCloud (US) regions, Secret Cloud, and Top Secret Cloud.

Result

The Console displays your discovered FSx for ONTAP file system on the Systems page. You can manage your FSx for ONTAP file systems in several ways, such as from Workloads in the NetApp Console, using ONTAP System Manager, and using AWS CloudFormation. Learn how to manage an FSx for ONTAP file system.

Manage an FSx for ONTAP file system in the NetApp Console

After you create or discover an FSx for ONTAP system in the NetApp Console, you can manage the file system by creating volumes, managing storage VMs, protecting data, and administering the file system. The Console also enables you to use data services that provide capabilities like backup and recovery, data classification, data synchronization, and more.

Manage a file system using NetApp Workloads

When you open an FSx for ONTAP system from the NetApp Console Systems page, you’re brought to NetApp Workloads. Workloads is an intelligent optimization and automation service that uses industry best practices to plan, provision, and operate key workloads using Amazon FSx for NetApp ONTAP.

Learn how to manage a file system using NetApp Workloads

Manage a file system using ONTAP System Manager

You can manage an FSx for ONTAP file system directly from the Console by using the ONTAP System Manager interface. A Console agent or an AWS Lambda link is required to use System Manager.

Learn about using links

Manage a file system using Amazon CloudFormation

You can provision and manage FSx for ONTAP file system resources (volumes, CIFS shares, export policies, and more) using Amazon CloudFormation.

NetApp CloudFormation FSx for ONTAP provider GitHub repository

Use NetApp data services with a file system

Use NetApp data services with your FSx for ONTAP file systems to back up and recover your data, transfer and synchronize data, scan and classify your data, replicate data, and speed up access or offload traffic.

Back up and recover your data

NetApp Backup and Recovery provides efficient, secure, and cost-effective data protection for NetApp ONTAP data, databases, and virtual machines, both on-premises and in the cloud.

Get started with NetApp Backup and Recovery

Transfer and synchronize data

NetApp Copy and Sync is a cloud replication and synchronization service for transferring NAS data between on-premises and cloud object stores.

Get started with NetApp Copy and Sync

Scan and classify your data

NetApp Data Classification enables you to scan and classify data across your organization’s hybrid multicloud.

Get started with NetApp Data Classification

Speed up access or offload traffic

NetApp Volume Caching provides a persistent, writable volume in a remote place. You can use Volume Caching to speed up access to data or to offload traffic from heavily accessed volumes.

Get started with NetApp Volume Caching

Replicate data to FSx for ONTAP in NetApp Console

Replicate data to protect against data loss if the region where your data resides experiences a disaster. Data replication is supported between FSx for ONTAP file systems and on-premises ONTAP systems or Cloud Volumes ONTAP.

For storage VM migration, you must complete the cut over operation right after you create a replication relationship.

About this task

Replication protects your data from regional disasters and supports storage VM migration.

Replicated volumes in the target file system are data protection (DP) volumes and follow the naming format: `{OriginalVolumeName}_copy`.

If you replicate a source volume with immutable files, the target volume and file system remain locked until the source volume's retention period ends. The immutable files feature is available when you create a volume for an FSx for ONTAP file system.

ⓘ

- Replication isn't supported for block volumes using iSCSI or NVMe protocols.
- You can replicate one source (read/write) volume or one data protection (DP) volume. Cascading replication is supported, but a third hop isn't. Learn more about cascading replication.

Migration use cases

When you select the migration use case, you can optionally select to replicate storage VM data and configuration settings for a single storage VM. When migrating data and configuration settings simultaneously, ensure that the last replication for the volume completed in the last 24 hours. All volumes in the same storage VM must be selected to use this feature. The tiering policy for all volumes defaults to the tiering policy of the source volume, which is recommended for migration use cases.

Workload Factory supports migration replication between the following storage systems.

- On-premises ONTAP systems and FSx for ONTAP file systems
- Cloud Volumes ONTAP and FSx for ONTAP file systems
- FSx for ONTAP and FSx for ONTAP file systems
  - First to first generation
  - First to second generation
  - Second to second generation

To migrate storage VM data and configuration settings, you must complete two operations.

1. Create a replication relationship, select **Migration** as the use case and select **Replicate storage VM configuration**.
2. Cut over replication for migration use cases to permanently migrate data and configuration settings from

the source file system to the target FSx for ONTAP file system.

To use this feature, create a

Create a replication relationship

Replicate data between two FSx for ONTAP file systems, between an on-premises ONTAP system and an FSx for ONTAP file system, or between Cloud Volumes ONTAP and an FSx for ONTAP file system.

Before you begin

Review these requirements before you begin.

- To replicate data between FSx for ONTAP and on-premises ONTAP or Cloud Volumes ONTAP, you must associate a link to a file system. Learn how to associate an existing link or to create and associate a new link. After you associate the link, return to this operation.
- For replication from an on-premises ONTAP system to an FSx for ONTAP file system, make sure you have discovered the on-premises ONTAP system.
- Replication isn't supported for volumes in a state other than available, created, or misconfigured, and when the ONTAP version isn't compatible.
- For migration use cases ensure that the last replication for the volume completed in the last 24 hours before you create a replication relationship with storage VM data and configuration settings.

Steps

1. From the NetApp Console Systems page, drag the source FSx for ONTAP file system, on-premises ONTAP system, or Cloud Volumes ONTAP system on top of the target FSx for ONTAP file system and select **Replication**.
2. On the Create replication page, select source volumes to replicate and then **Next**.
3. Under Replication target, provide the following:
   a. **Target name**: You applied the target name when you dragged and dropped the source storage system on the target system in the Console Systems page.
   b. **Use case**: Select one of the following use cases for the replication. Depending on the selected use case, Workload Factory fills in the form with recommended values in accordance with best practices. You can accept the recommended values or make changes as you complete the form.
      - Migration: transfers your data to the target FSx for ONTAP file system

        Replicate storage VM configuration: Optionally, select to replicate storage VM data and configuration settings for a single storage VM. When migrating data and configuration settings simultaneously, ensure that the last replication for the volume completed in the last 24 hours. All volumes in the same storage VM must be selected to use this feature. The tiering policy for all volumes defaults to the tiering policy of the source volume, which is recommended for migration use cases.
      - Hot disaster recovery: ensures high availability and rapid disaster recovery for critical workloads
      - Cold or archive disaster recovery:
        - Cold disaster recovery: uses longer recovery time objectives (RTO) and recovery point objects (RPO) to lower costs
        - Archive: replicates data for long-term storage and compliance
      - Other

Additionally, the use case selection determines the replication policy, or SnapMirror policy (ONTAP). The terms used to describe replication policies come from ONTAP 9 documentation.

- For migration and other, the replication policy is called *MirrorAllSnapshots*. *MirrorAllSnapshots* is an asynchronous policy for mirroring all snapshots and the latest active file system.
- For hot, cold, or archive disaster recovery, the replication policy is called *MirrorAndVault*. *MirrorAndVault* is an asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots.

  For all use cases, if you enable snapshots for long-term retention, the default replication policy is *MirrorAndVault*.

c. **FSx for ONTAP file system**: Select credentials, region, and FSx for ONTAP file system name for the target FSx for ONTAP file system.

d. **Storage VM name**: Select the storage VM from the dropdown menu. The storage VM you select is the target for all selected volumes in this replication relationship.

e. **Volume name**: The target volume name is generated automatically with the following format `{OriginalVolumeName}_copy`. You can use the auto-generated volume name or enter another volume name.

f. **Tiering policy**: Select the tiering policy for the data stored in the target volume. The tiering policy defaults to the recommended tiering policy for the use case you selected.

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

   If you selected the migration use case, Workload Factory automatically selects to copy the tiering policy of source volume to the target volume. You can deselect to copy the tiering policy and select a tiering policy which applies to the volume selected for replication.

g. **Max transfer rate**: Select **Limited** and enter the max transfer limit in MB/s. Alternatively, select **Unlimited**.

   Without a limit, network and application performance may decline. Alternatively, we recommend an unlimited transfer rate for FSx for ONTAP file systems for critical workloads, for example, those that are used primarily for disaster recovery.

4. Under Replication settings, provide the following:

   a. **Replication interval**: Select the frequency that snapshots are transferred from the source volume to the target volume.

   b. **Long-term retention**: Optionally, enable snapshots for long-term retention. Long-term retention enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy.

   Replications without long-term retention use the *MirrorAllSnapshots* policy. Enabling long-term retention assigns the *MirrorAndVault* policy to the replication.

   If you enable long-term retention, then select an existing policy or create a new policy to define the snapshots to replicate and the number to retain.

> ⓘ Matching source and target labels are required for long-term retention. If desired, Workload factory can create missing labels for you.

  - **Choose an existing policy**: select an existing policy from the dropdown menu.
  - **Create a new policy**: enter a **policy name**.

c. **Immutable snapshots**: Optional. Select **Enable immutable snapshots** to prevent snapshots taken in this policy from being deleted during the retention period.

  - Set the **Retention period** in number of hours, days, months, or years.
  - **Snapshot policies**: In the table, select the snapshot policy frequency and the number of copies to retain. You can select more than one snapshot policy.

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

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

e. **S3 access point tags**: Optionally, you can add up to 50 tags.

5. Select **Create**.

Result

The replication relationship appears in the **Replication relationships** tab in the target FSx for ONTAP file system.

If you created a replication relationship for migration purposes, you must cut over all the volumes and their associated storage VM to complete migration of storage VM data and configuration settings to the target FSx for ONTAP file system.

Cut over replication for migration use cases

After creating a replication relationship for a migration use case, you must cut over replication to complete migration of storage VM data and configuration settings to a target FSx for ONTAP file system. Cutover replication permanently migrates data and storage VM configuration settings from the source file system to the target FSx for ONTAP file system. During the cutover, data gets replicated for the last time. The system deletes the source volume(s) after cutover completes. You can’t undo this action.

Before you begin

Review these requirements before you begin.

- Stop any client access to your storage VM before you cut over replication.

- Ensure all source volumes are not serving any data before you cut over replication.
- Ensure the data is synced between the source and target volumes before you cut over replication.
- The FSx for ONTAP file system you use for the replication relationship must have an associated link. Learn how to associate an existing link or to create and associate a new link. After you associate the link, return to this operation.

Steps

1. In the NetApp Console, select the menu and then select **Storage**.
2. From the Storage menu, select **FSx for ONTAP**.
3. From **FSx for ONTAP**, select the file system that contains the volume(s) to replicate.
4. Select the **Replication relationships** tab.
5. In the Replication relationships table, select the replication relationship to cut over and then select **Cut over replication**.
6. Review the information in the Cut over replication dialog and then type *cut over* to confirm.
7. Select **Cut over**.

Result

After cutover, the source volumes are deleted and the target volumes become read/write. You can modify the tiering policy for the target volume(s) after cutover.

Monitor FSx for ONTAP operations with Tracker in NetApp Console

Monitor and track the execution of FSx for ONTAP operations and monitor job progress with Tracker in NetApp Console.

About this task

NetApp Console provides Tracker, a job monitoring feature, so you can monitor and track the progress and status of credentials, FSx for ONTAP, and link operations, review details for operation tasks and subtasks, and diagnose any issues or failures.

Several actions are available in Tracker. You can filter jobs by time frame (last 24 hours, 7 days, 14 days, or 30 days), workload, status, and user; find jobs using the search function; and download the jobs table as a CSV file. You can refresh Tracker at any time. And you can quickly retry a failed operation or edit parameters for a failed operation and try the operation again.

Tracker supports two levels of monitoring depending on the operation. Each task, such as file system deployment, displays the task description, status, start time, task duration, user, region, proxy resource, task ID, and all related sub tasks. You can view API responses to understand what happened during the operation.

Tracker task levels with examples

- Level 1 (parent task): Tracks file system deployment.
- Level 2 (sub task): Tracks the sub tasks related to file system deployment.

Operation status

Operation status in Tracker is as follows *in progress*, *success*, and *failed*.

Operation frequency

Operation frequency is based on the task type and schedule.

Events retention

Events are retained in the user interface for 30 days.

Track and monitor operations

Track and monitor operations in the NetApp Console with Tracker.

Steps

1. From the NetApp Console menu, select **Workloads** and then **Administration**.
2. From the Administration menu, select **Tracker**.
3. In Tracker, view tasks or use the filters or search to narrow results. You can also download a report of all operations by selecting to **Export CSV**.

View API request

View the API request in the Codebox for a task in Tracker.

Steps

1. In Tracker, select a task.
2. Select the three-dot menu and then select **View API request**.

Retry a failed operation

Retry a failed operation in Tracker. Retrying the failed operation starts a new task that you can monitor in Tracker.

You can also copy the error message of a failed operation.

> ⓘ You can retry the failed operation only once.

Steps

1. In Tracker, select a failed operation.
2. Select the three-dot menu and then select **Retry**.

Result

The operation is re-initiated and appears as a new task in Tracker.

Edit and retry a failed operation

Edit the parameters of the failed operation and retry the operation outside Tracker.

Steps

1. In Tracker, select a failed operation.
2. Select the three-dot menu and then select **Edit and retry**.

   You are redirected to the operation page, volume creation for example, where you can edit the parameters and retry the operation.

Result

The operation is re-initiated. Go to Tracker to view the status of the operation.

Remove an FSx for ONTAP file system from a project

Remove an FSx for ONTAP file system from a project in the NetApp Console. This operation dissociates the file system from one project so that you can associate it with another project within the same account.

About this task

Removing an FSx for ONTAP file system from a project removes it from the NetApp Console. It does not delete the FSx for ONTAP file system. You can later rediscover the FSx for ONTAP file system in the same or in a different project from within the same account.

Steps

1. From the NetApp Console menu, select **Storage** and then **Management**.
2. Select the file system that you want to remove.
3. Select **Enter System**.
4. From FSx for ONTAP in Storage, select the three-dot menu and then select **Remove from project**.
5. Select **Remove** to confirm the removal of the file system from the project.

Delete an FSx for ONTAP file system

To delete an FSx for ONTAP file system, you must first delete any volumes, storage VMs, or replication relationships associated with the file system.

Steps

1. From the NetApp Console menu, select **Storage** and then **Management**.
2. Select the file system that you want to remove.
3. Select **Enter System**.
4. From FSx for ONTAP in Storage, select the three-dot menu and then select **Delete**.
5. Select **Delete** to confirm deletion.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to the NetApp Console and its storage solutions and data 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 documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your NetApp Console account serial number (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in the Console).

  This serves as your single support subscription ID for any service within the Console. Each Console account 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 the NetApp Console 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 the Console as described below.

Register NetApp Console for NetApp support

To register for support and activate support entitlement, one user in your NetApp Console account must associate a NetApp Support Site account with their Console 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 the Console.

Steps

1. Select **Administration** > **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 Console account is registered for support.

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

Steps

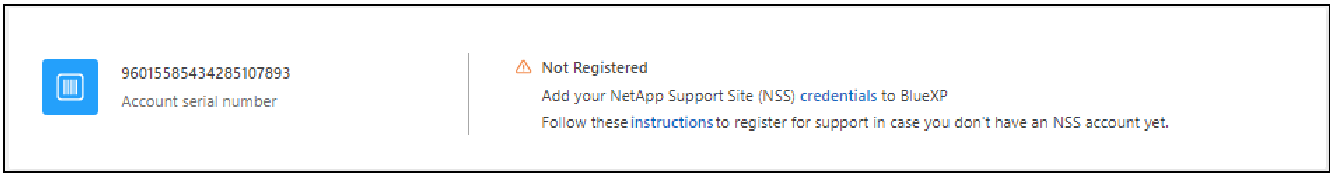
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the Console account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your Console 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 Console, select the Help icon, and select **Support**.
2. Locate your account ID serial number from the Support Registration page.



960155854342851O7893
Account serial number

⚠ Not Registered
Add your NetApp Support Site (NSS) credentials to BlueXP
Follow these instructions 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 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 Console 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 Console 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 the Console 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

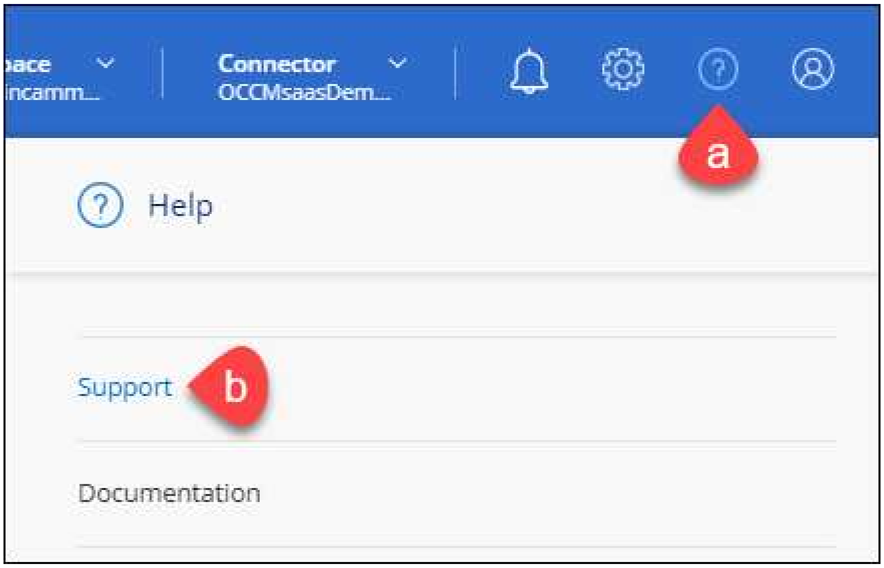
Associating NSS credentials with your NetApp Console account is different than the NSS account that is associated with a Console user login.

These NSS credentials are associated with your specific Console account ID. Users who belong to the Console organization 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 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 the Console 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 NetApp Console and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledge base (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 the documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

To receive technical support specific to NetApp and its storage solutions and data 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 NetApp Console documentation that you're currently viewing.

- Knowledge base

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

- Communities

  Join the NetApp Console 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 Console login. Learn how to manage credentials associated with your Console 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 NetApp Console, 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, **NetApp Console** when specific to a technical support issue with workflows or functionality within the Console.
   - **System**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

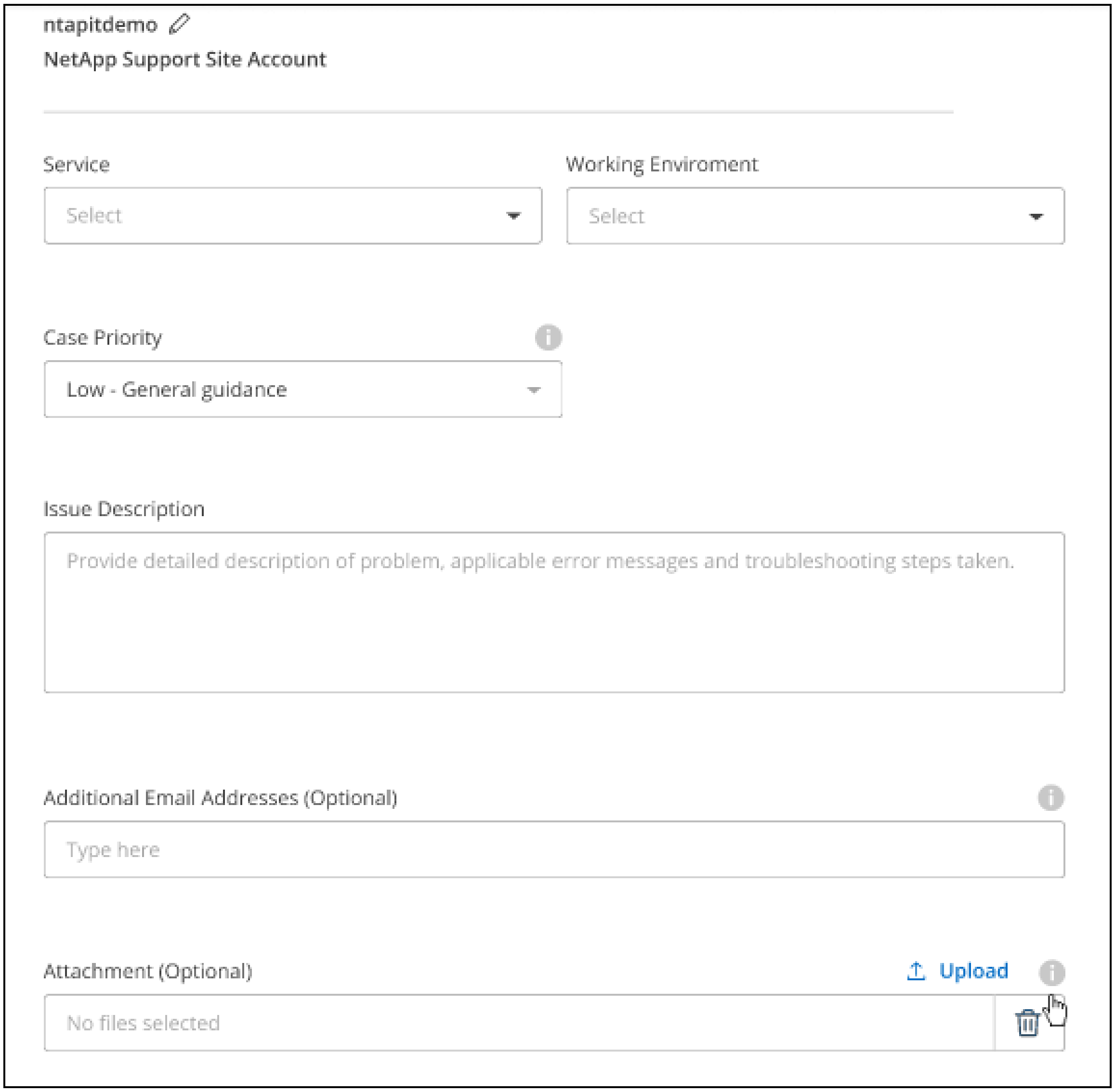
     The list of systems are within scope of the Console organization, and Console agent you have selected in the top banner.

   - **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

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 NetApp Console account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases

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

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 the NetApp Console, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to the Console.

   The **Case management** page shows open cases related to the NSS account that is associated with your Console 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.
    - Filter the contents of the columns.
    - Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.
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.

Legal notice for the NetApp Console

Copyright information

Trademark information