Get started

Amazon FSx for NetApp ONTAP

NetApp
January 12, 2026

Table of Contents

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.

1 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.

2 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

3 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.

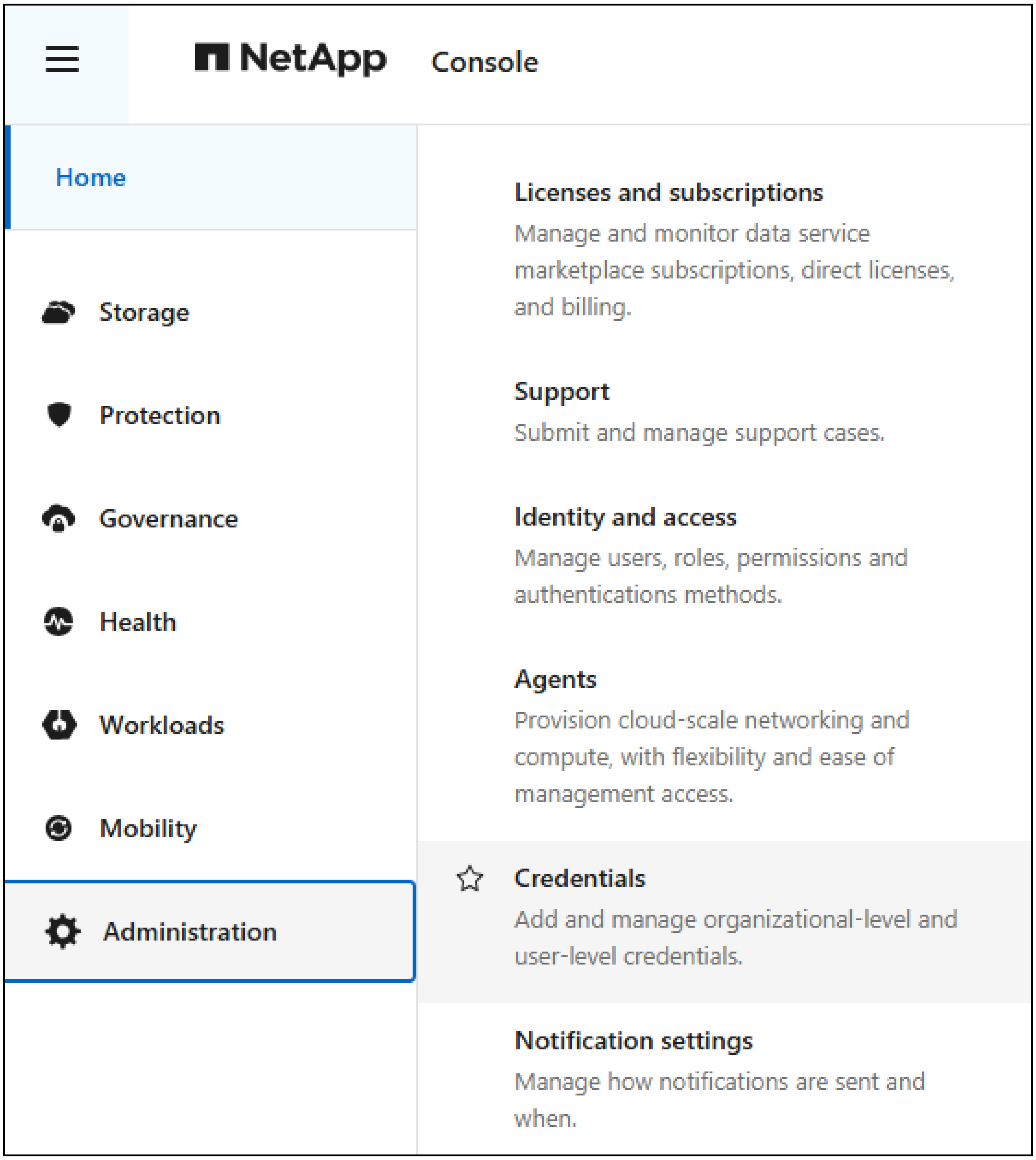
Credentials and permissions are managed via NetApp Workload Factory. Workload Factory is a life-cycle management platform designed to help users optimize workloads using Amazon FSx for NetApp ONTAP file systems. The NetApp Console uses the same set of AWS credentials and permissions as Workload Factory.

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.

Copyright information

Trademark information