Get started

Setup and administration

NetApp
September 02, 2024

Table of Contents

Get started

Learn the basics

Learn about Workload Factory

NetApp Workload Factory is a powerful life-cycle management platform designed to help you optimize your workloads using Amazon FSx for NetApp ONTAP file systems. Workloads that can be streamlined using Workload Factory and FSx for ONTAP include databases, VMware migrations to VMware Cloud on AWS, AI chatbots, and more.

A workload encompasses a combination of resources, code, and services or applications, designed to serve a business goal. This could be anything from a customer-facing application to a backend process. Workloads may involve a subset of resources within a single AWS account or span across multiple accounts.

Amazon FSx for NetApp ONTAP provides fully managed, AWS-native NFS, SMB/CIFS, and iSCSI storage volumes for mission-critical applications, databases, containers, VMware Cloud datastores, and user files. You can manage FSx for ONTAP through Workload Factory and by using native AWS management tools.

Features

The Workload Factory platform provides the following major capabilities.

Flexible and low cost storage

Discover, deploy, and manage Amazon FSx for NetApp ONTAP file systems in the cloud. FSx for ONTAP brings the full capabilities of ONTAP to a native AWS managed service delivering a consistent hybrid cloud experience.

Migrate on-premises vSphere environments to VMware Cloud on AWS

The VMware Cloud on AWS migration advisor enables you to analyze your current virtual machine configurations in on-premises vSphere environments, generate a plan to deploy recommended VM layouts to VMware Cloud on AWS, and use customized Amazon FSx for NetApp ONTAP file systems as external datastores.

Optimized database deployment

Deploy Microsoft SQL Servers, databases, and database clones including AWS resources provisioning, storage provisioning, networking, and OS configurations, utilizing optimized deployment configurations ensuring a consistent and error-free setup process.

AI chatbot development

Leverage your FSx for ONTAP file systems for storing your organizations chatbot sources and the AI Engine databases. This allows you to embed your organization’s unstructured data into an enterprise chatbot application.

Storage calculators to save costs

Analyze your current deployments that use Amazon Elastic Block Store (EBS) or Elastic File System (EFS) storage, or Amazon FSx for Windows File Server, to see how much money you can save by moving to Amazon FSx for NetApp ONTAP. You can also use the calculator to perform a "what if" scenario for a future deployment that you’re planning.

Supported cloud providers

Workload Factory enables you to manage cloud storage and use workload capabilities in Amazon Web Services.

Cost

Workload Factory is free to use. The cost that you pay to Amazon Web Services (AWS) depends on the storage and workload services that you plan to deploy. This includes the cost of Amazon FSx for NetApp ONTAP file systems, VMware Cloud on AWS infrastructure, AWS services, and more.

How Workload Factory works

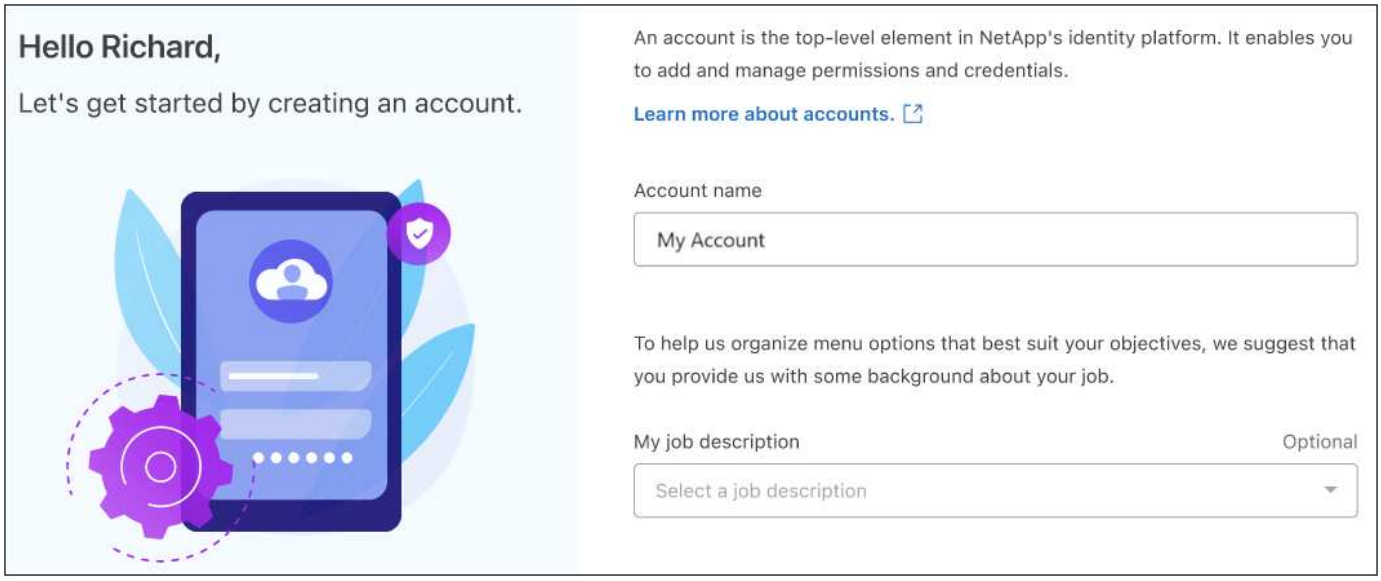
Workload Factory includes a web-based console that's provided through the SaaS layer, an account, operational modes that control access to your cloud estate, links that provide segregated connectivity between Workload Factory and an AWS account, and more.

Software-as-a-service

Workload Factory is accessible through a web-based console. This SaaS experience enables you to automatically access the latest features as they're released and to easily switch between your Workload Factory accounts and links.

Accounts

When you log in to Workload Factory for the first time, you're prompted to create an account. This account enables you to organize your resources, workloads, and workload access for your organization using credentials.



When you create an account, you are the single Account Admin user for that account.

If your organization requires additional account or user management, reach out to us by using the in-product chat.

If you use NetApp BlueXP, then you'll already belong to an account because Workload Factory leverages BlueXP accounts.

Operational modes

Workload Factory provides three operational modes that enables you to carefully control access to your cloud estate, and assign incremental trust to Workload Factory based on your IT policies.

- **Basic mode** represents a zero-trust relationship and is designed for early exploration of Workload Factory and usage of the various wizards to create the needed Infrastructure as Code. This code can be copied and used manually by the user along with their relevant AWS credentials.
- **Read mode** enhances the experience of Basic mode by assisting the user in detecting various resources and tools, and consequently, helping to complete relevant wizards.
- **Automate mode** represents a full-trust relationship and is designed to execute and automate on behalf of the user along with the assigned credentials that have the needed and validated permissions for execution.

Learn more about Workload Factory operational modes.

Connectivity links

A Workload Factory link creates a trust relationship and connectivity between Workload Factory and one or more FSx for ONTAP file systems. This enables you to monitor and manage certain file system features directly from the ONTAP REST API calls that are not available through the Amazon FSx for ONTAP API.

You don't need a link to get started with Workload Factory, but in some cases you'll need to create a link to unlock all Workload Factory features and workload capabilities.

Links currently leverage AWS Lambda.

Learn more about Links

Codebox automation

Codebox is an Infrastructure as Code (IaC) co-pilot that helps developers and DevOps engineers generate the code needed to execute any operation supported by Workload Factory. Code formats include Workload Factory REST API, AWS CLI, and AWS CloudFormation.

Codebox is aligned with the Workload Factory operation modes (Basic, Read, and Automate) and sets a clear path for execution readiness as well as an automation catalog for quick future reuse.

The Codebox pane shows the IaC that is generated by a specific job flow operation, and is matched by a graphical wizard or conversational chat interface. While Codebox supports color coding and search for easy navigation and analysis, it does not allow editing. You can only copy or save to the Automation Catalog.

Learn more about Codebox.

Savings calculators

Workload Factory provides a savings calculator so you can compare the costs of storage on FSx for ONTAP file systems against Elastic Block Store (EBS), Elastic File Systems (EFS), and FSx for Windows File Server. Depending on your storage requirements, you might find that FSx for ONTAP file systems are the most cost effective option for you.

The criteria that is compared between the different types of storage systems includes the total required capacity and the total performance, which includes the required IOPS and required throughput.

Learn how to explore savings using storage calculators

REST APIs

Workload Factory enables you to optimize, automate, and operate your FSx for ONTAP file systems for specific workloads. Each workload exposes an associated REST API. Collectively, these workloads and APIs form a flexible and extensible development platform you can use to administer your FSx for ONTAP file systems.

There are several benefits when using the Workload Factory REST APIs:

- The APIs have been designed based on REST technology and current best practices. The core technologies include HTTP and JSON.
- Workload Factory authentication is based on the OAuth2 standard. NetApp relies on the Auth0 service implementation.
- The Workload Factory web-based console uses the same core REST APIs so there is consistency between the two access paths.

View the Workload Factory REST API documentation

Learn about operational modes and AWS credentials

Workload Factory provides three operational modes that enable you to carefully control access between Workload Factory and your cloud estate based on your IT policies. The operational mode that you use is determined by the level of AWS permissions that you provide to Workload Factory.

Operational modes

Operational modes provide a logical organization of the functionality and capabilities delivered by Workload Factory, as correlated to the trust level that you assign. The main objective in operational modes is to clearly communicate which tasks Workload Factory can or cannot perform within your AWS account.

Basic mode

Represents a zero-trust relationship where no AWS permissions are assigned to Workload Factory. It is designed for early exploration of Workload Factory and usage of the various wizards to create the needed Infrastructure as Code (IaC). You can copy the code and use it in AWS by entering your AWS credentials manually.

Read mode

Enhances the experience of basic mode by adding read-only permissions so that the IaC templates are filled with your specific variables (for example, VPC, security groups, etc.). This enables you to execute the IaC directly from your AWS account without providing any modify permissions to Workload Factory.

Automate mode

Represents a full trust relationship so that Workload Factory gets assigned with full permissions. This allows Workload Factory to execute and automate operations in AWS on your behalf along with the assigned credentials that have the needed permissions for execution.

Operational mode features

The features available using each of the modes grows with each mode.

Mode	Automation from Workload Factory	Automation within AWS using IaC	AWS resource discovery and auto-complete	Progress monitoring
Basic	No	Minimally complete IaC template	No	No
Read	No	Moderately complete IaC template	Yes	Yes
Automate	Full automation	Complete IaC template with full automation	Yes	Yes

Operational mode requirements

There is no selector that you need to set in Workload Factory to identify which mode you are planning to use. The mode is determined based on the AWS credentials and permissions that you assign to your Workload Factory account.

Mode	AWS account credentials	Link
Basic	Not required	Not required
Read	Read-only	Not required
Automate	Read-write credentials	Required

Learn more about links

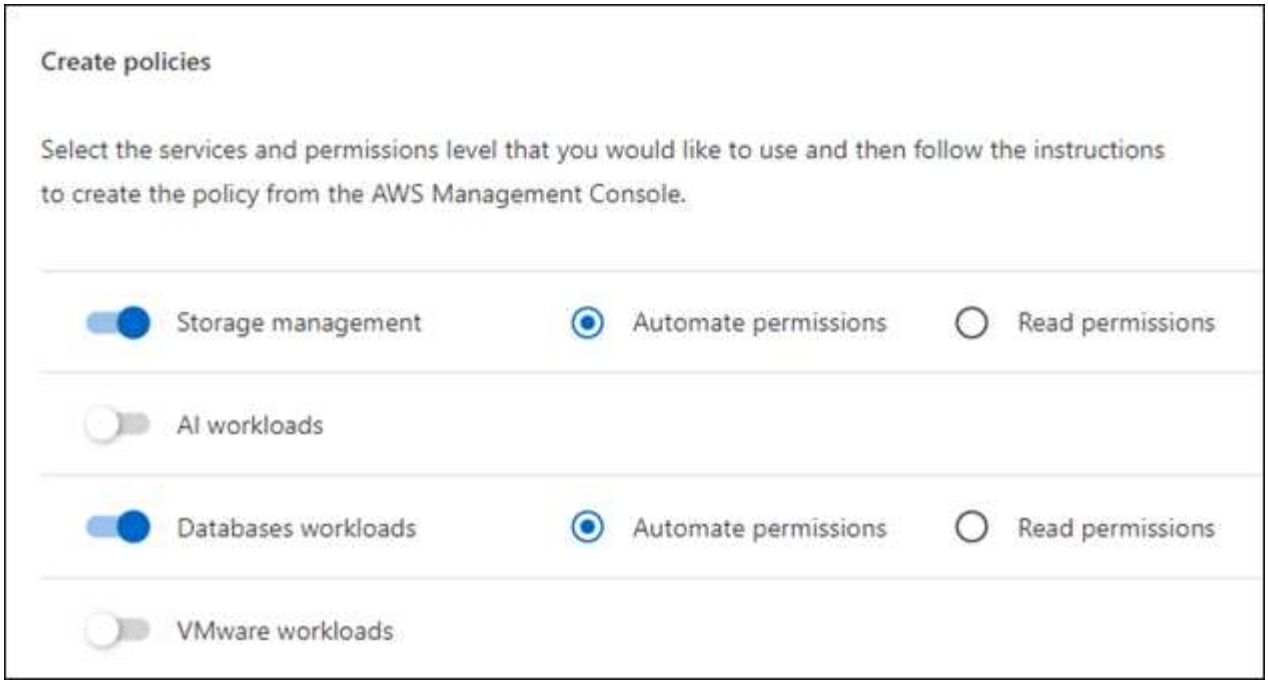
Operational mode examples

You can set up your credentials to provide one mode for one workload component and another mode for another component. For example, you can configure automate mode for operations where you are deploying and managing FSx for ONTAP file systems, but only configure read mode for creating and deploying database workloads using Workload Factory.

You can provide these capabilities within a single set of credentials in a Workload Factory account, or you can create multiple sets of credentials when each credential provides unique workload deployment capabilities.

Example 1

Account users who use the credentials that have been given the following permissions will have full control (automate mode) for creating FSx for ONTAP file systems, deploying databases, and viewing other types of AWS storage used in the account.

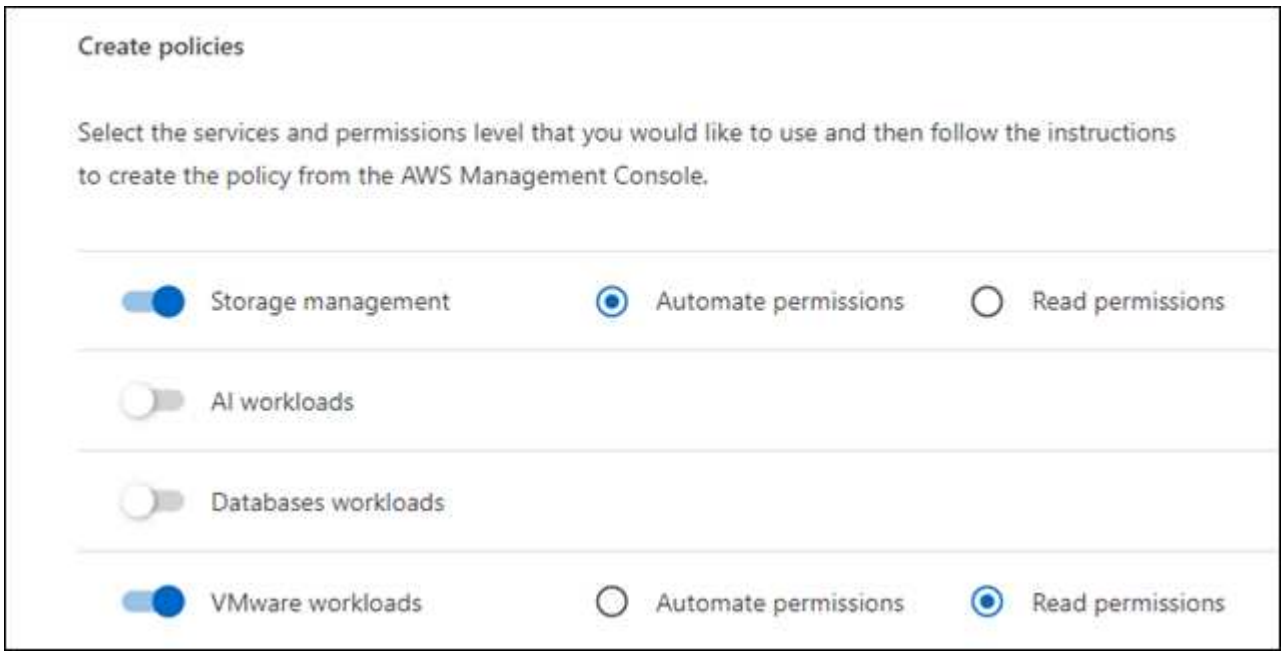


However, they will have no automation controls for creating and deploying VMware workloads (basic mode) from Workload Factory. If they want to create VMware workloads, they'll need to copy the code from the Codebox, log in to their AWS account manually, and manually populate missing entries in the generated code to use this functionality.

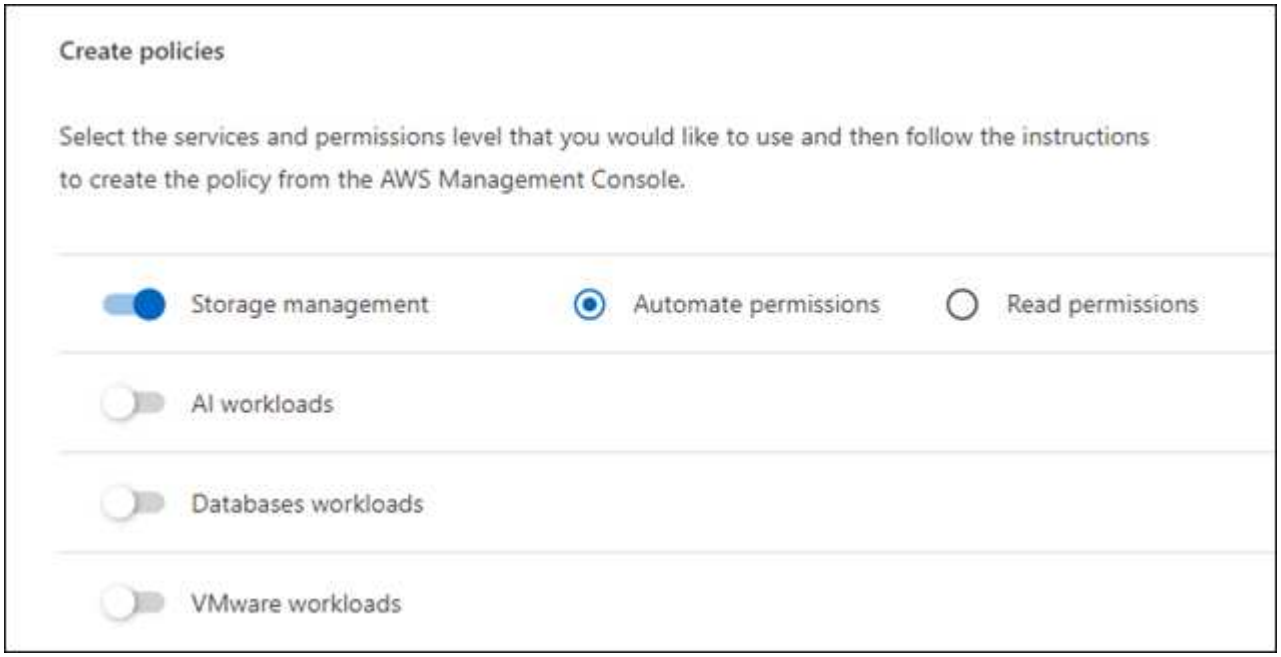
Example 2

Here the user has created two sets of credentials to allow different operational capabilities depending on which set of credentials has been selected. Typically, each set of credentials is paired to a different AWS account.

The first set of credentials includes permissions that give users full control for creating FSx for ONTAP file systems (and the ability to view other types of AWS storage used in the account), but only read permissions when working with VMware workloads.



The second set of credentials only provides permissions that give users full control for creating FSx for ONTAP file systems, and viewing other types of AWS storage used in the account.



AWS credentials

We have designed an AWS assume role credentials registration flow that:

- Supports more aligned AWS account permissions by allowing you to specify the workload capabilities that you want to use and providing IAM policy requirements according to those selections.
- Allows you to adjust the granted AWS account permissions as you opt-in or opt-out of specific workload capabilities.
- Simplifies manual IAM policy creation by providing tailored JSON policy files that you can apply in the AWS console.
- Further simplifies the credentials registration process by offering users with an automated option for required IAM policy and role creation using AWS CloudFormation stacks.
- Aligns better with FSx for ONTAP users who strongly prefer to have their credentials stored within the boundaries of the AWS cloud ecosystem by allowing storage of the FSx for ONTAP services credentials in an AWS-based secret management backend.

One or more AWS credentials

When you use your first Workload Factory capability (or capabilities), you'll need to create the credentials using the permissions required for those workload capabilities. You'll add the credentials to Workload Factory, but you'll need to access the AWS Management Console to create the IAM role and policy. These credentials will be available within your account when using any capability in Workload Factory.

Your initial set of AWS credentials can include an IAM policy for one capability or for many capabilities. It just depends on your business requirements.

Adding more than one set of AWS credentials to Workload Factory provides additional permissions needed to use additional capabilities, such as FSx for ONTAP file systems, deploy databases on FSx for ONTAP, migrate VMware workloads, and more.

Learn how to add AWS credentials to Workload Factory.

Quick start for Workload Factory

Get started with Workload Factory by signing up and creating an account, adding credentials so that Workload Factory can manage AWS resources directly, and then optimize your workloads by using Amazon FSx for NetApp ONTAP.

Workload Factory is accessible to users as a cloud service from the web-based console. Before you get started, you should have an understanding of Workload Factory and operational modes.

1 Sign up and create an account

Go to the Workload Factory console, sign up, and create an account.

Learn how to sign up and create an account.

2 Add AWS credentials to Workload Factory

This step is optional. You can use Workload Factory in *Basic* mode without adding credentials to access your AWS account. Adding AWS credentials to Workload Factory in either *Read* mode or *Automate* mode gives your Workload Factory account the permissions needed to create and manage FSx for ONTAP file systems and to deploy and manage specific workloads, such as databases and GenAI.

Learn how to add credentials to your account.

3 Optimize your workloads using FSx for ONTAP

Now that you've signed up, created an account, and optionally added AWS credentials, you can start using Workload Factory to optimize your workloads using FSx for ONTAP. Use the links below to follow step-by-step instructions for each type of workload.

- Amazon FSx for NetApp ONTAP

  Assess and analyze current data estates for potential cost savings by using FSx for ONTAP as the storage infrastructure, provision and templatize FSx for ONTAP deployments based on best practices, and access advanced management capabilities.

- GenAI

  Deploy and manage a Retrieval-Augmented Generation (RAG) infrastructure to improve the accuracy and uniqueness of your AI applications. Create a RAG knowledge base on FSx for ONTAP with built-in data security and compliance.

- Database workloads

  Detect your existing database estate on AWS, assess potential cost savings with FSx for ONTAP, deploy databases end-to-end with built-in best practices for optimization, and automate thin cloning for CI/CD pipelines.

- VMware workloads

Streamline migrations and operations with smart recommendations and automatic remediation. Deploy efficient backups and robust disaster recovery. Monitor and troubleshoot your VMs.

Sign up to Workload Factory

Workload Factory is accessible from a web-based console. When you get started with Workload Factory, your first step is to sign up using your existing NetApp Support Site credentials or by creating a NetApp cloud login.

About this task

You can sign up to Workload Factory using one of the following options:

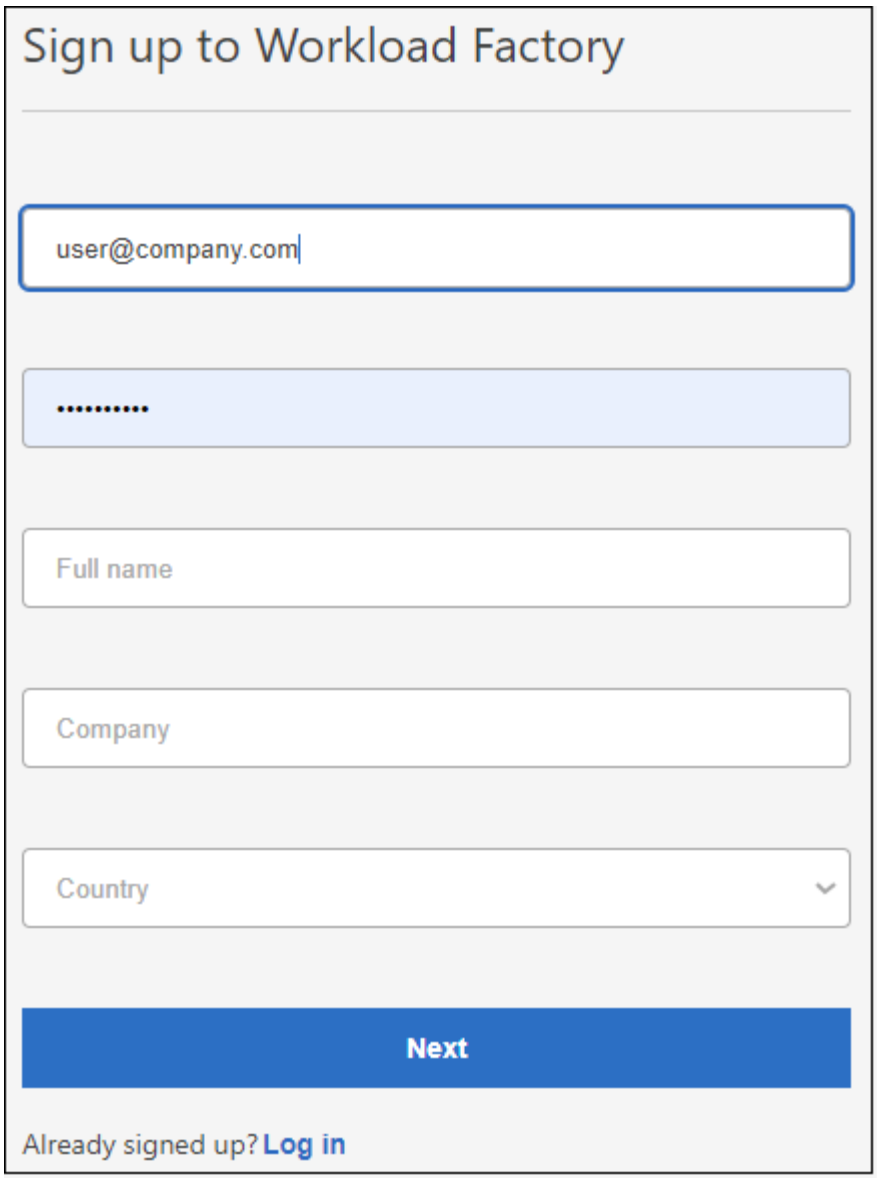
- Your existing NetApp Support Site (NSS) credentials
- A NetApp cloud login by specifying your email address and a password

Steps

1. Open a web browser and go to the Workload Factory console
2. If you have a NetApp Support Site account, enter the email address associated with your NSS account directly on the **Log in** page.

   You can skip the sign up page if you have an NSS account. Workload Factory will sign you up as part of this initial login.

3. If you don’t have an NSS account and you want to sign up by creating a NetApp cloud login, select **Sign up**.



4. On the **Sign up** page, enter the required information to create a NetApp cloud login and select **Next**.

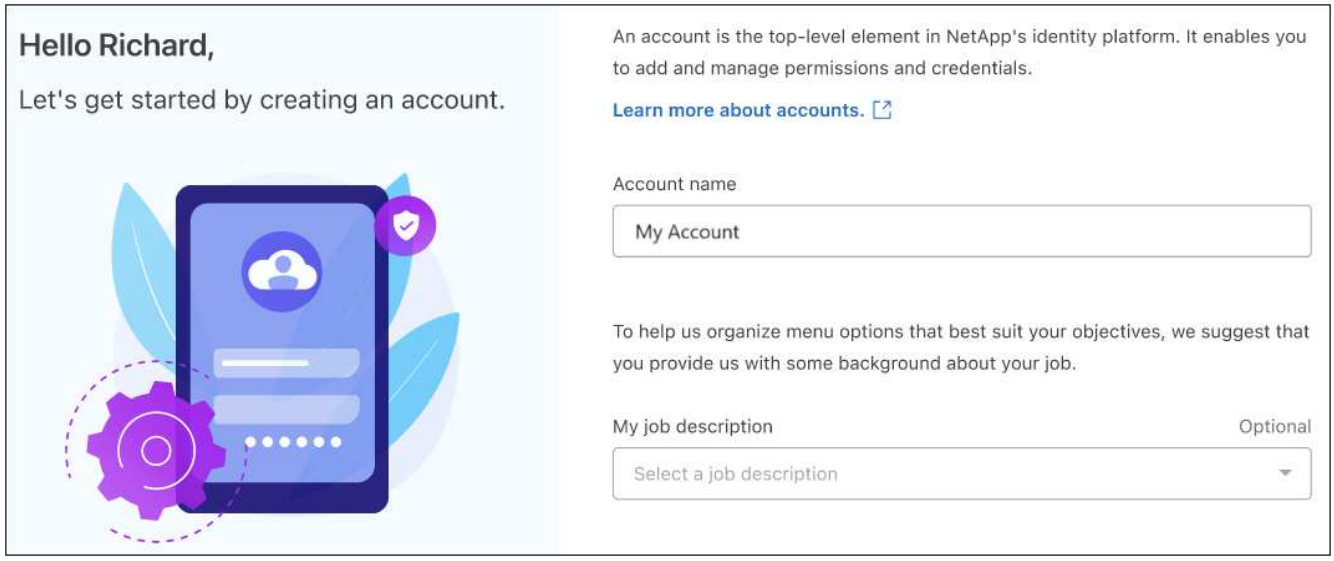
   Note that only English characters are allowed in the sign up form.

5. Enter the detailed information for your company and select **Sign up**.
6. Check your inbox for an email from NetApp that includes instructions to verify your email address.

   This step is required before you can log in.

7. When prompted, review the End User License Agreement and accept the terms, and select **Continue**.
8. On the **Account** page, enter a name for your account, and optionally select your job description.

   An account is the top-level element in NetApp's identity platform, and it enables you to add and manage permissions and credentials.



9. Select **Create** and the Workload Factory home page is displayed.

Result

You now have a Workload Factory login and an account. You are considered an Account Admin and you have access to all Workload Factory functionality.

Add AWS credentials to Workload Factory

Add and manage AWS credentials so that Workload Factory has the permissions that it needs to deploy and manage cloud resources in your AWS accounts.

Overview

Workload Factory will operate in *basic* mode unless you add AWS account credentials. You can add credentials to enable other operation modes, such as Read mode and Automate mode. Learn more about operational modes.

You can add AWS credentials to an existing Workload Factory account from the Credentials page. This provides Workload Factory with the permissions needed to manage resources and processes within your AWS cloud environment.

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 Workload Factory manually to give your Workload Factory 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 Workload Factory, enter a name and add the credentials.

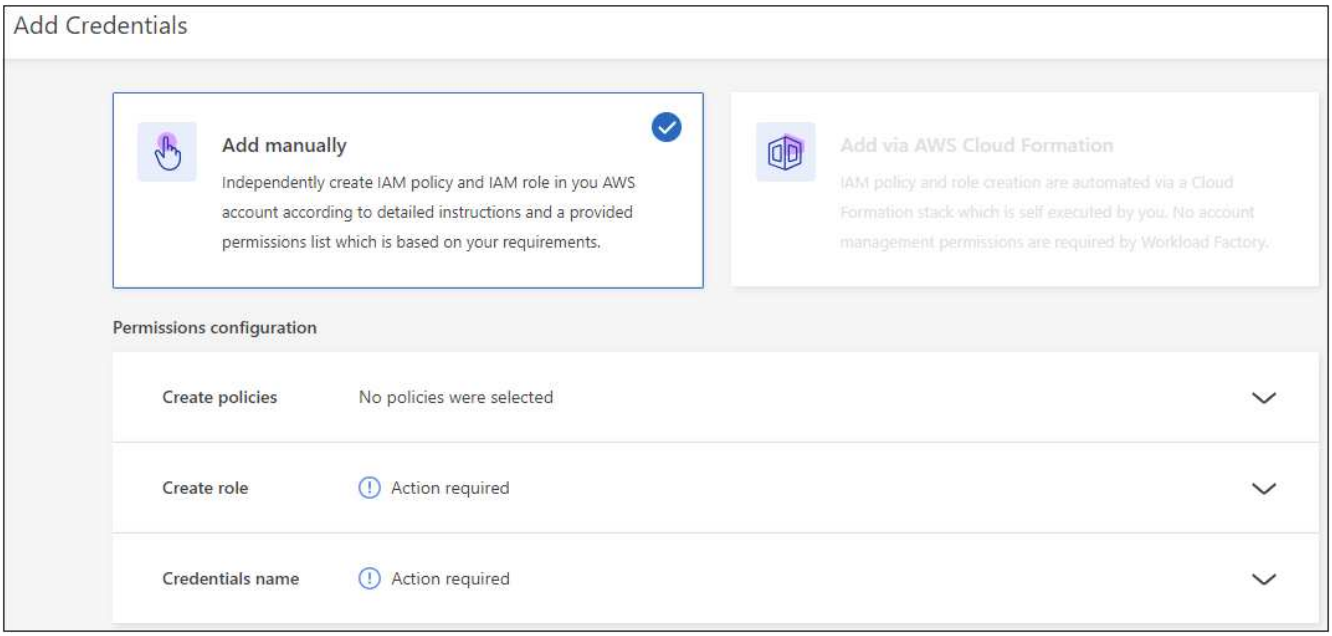
Before you begin

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

Steps

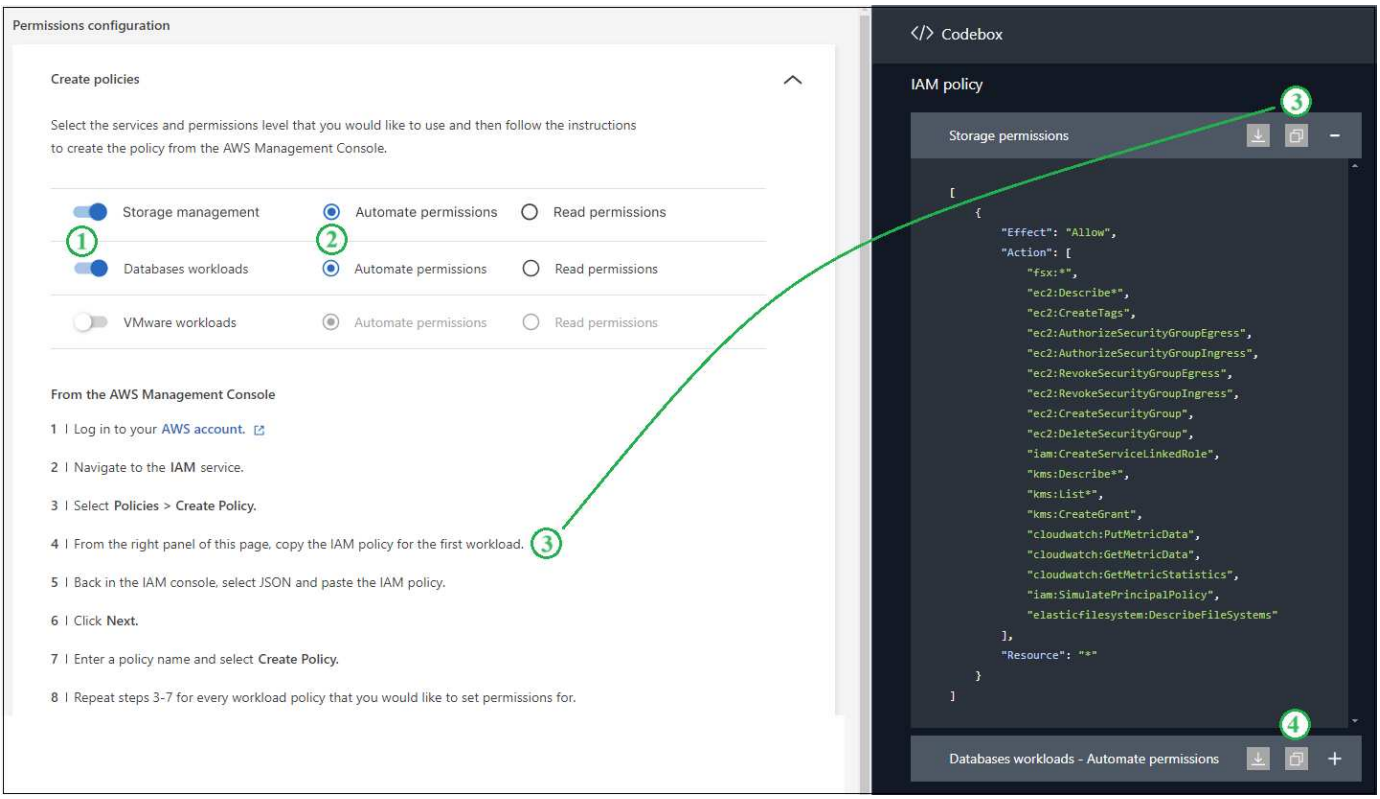
1. In the Workload Factory console, select the **Account** icon, and select **Credentials**.

2. On the **Credentials** page, select **Add credentials** and the Add credentials page is displayed.
3. Select **Add manually** and then follow the steps below to fill out the three sections under *Permissions configuration*.



Step 1: Select the workload capabilities and create the IAM policies

In this section you'll choose which types of workload capabilities will be manageable as part of these credentials, and the permissions enabled for each workload. 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

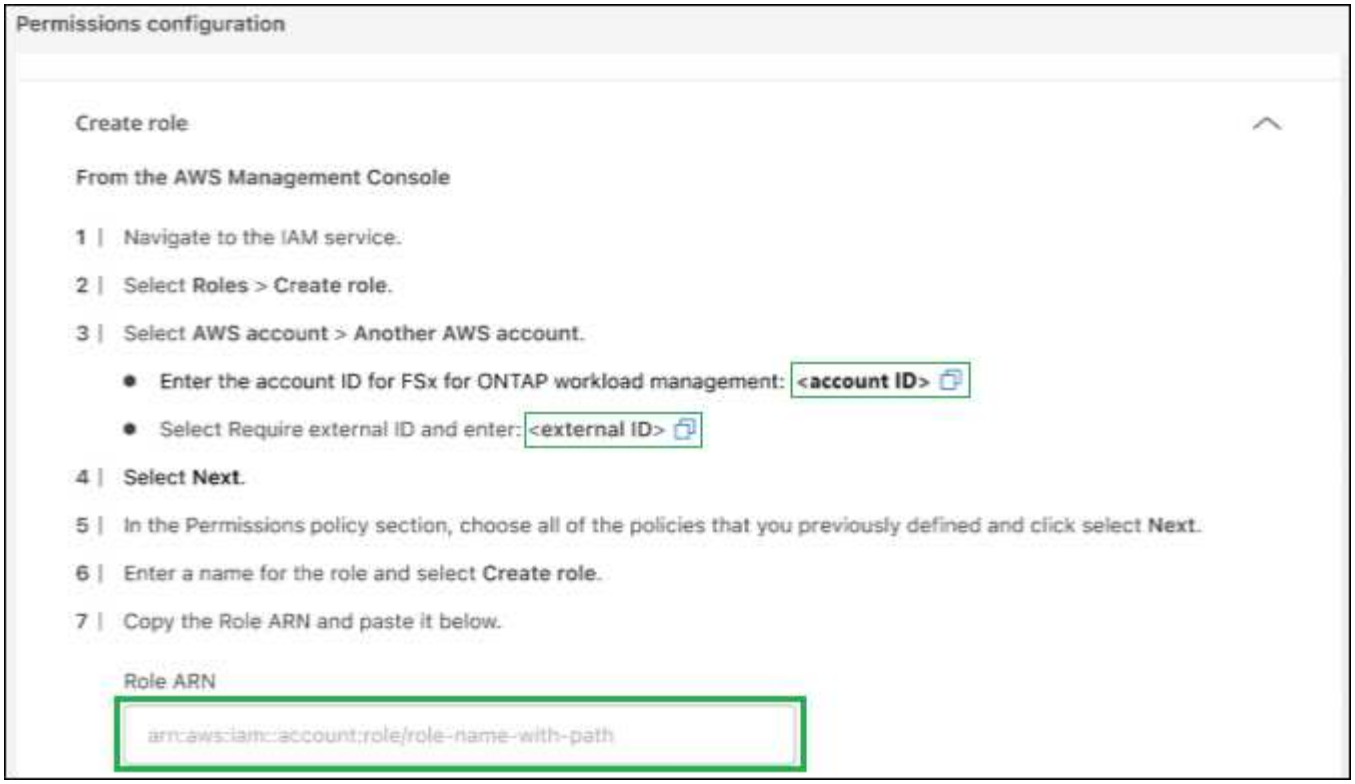
1. From the **Create policies** section, enable each of the workload capabilities that you want to include in these credentials.

   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 levels (operate, view, and so on), select the type of permissions that will be available with these credentials.
3. In the Codebox window, copy the permissions for the first IAM policy.
4. Open another browser window and log in to your AWS account in the AWS Management Console.
5. Open the IAM service, and then select **Policies** > **Create Policy**.
6. Select JSON as the file type, paste the permissions you copied in step 3, and select **Next**.
7. Enter the name for the policy and select **Create Policy**.
8. 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 Workload Factory UI.
   b. Select **Required external ID** and copy and paste the external ID from the Workload Factory UI.
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 Workload Factory, 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 Workload Factory.

Steps

1. From Workload Factory, 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 you are returned to the Credentials page.

Add credentials to an account using CloudFormation

You can add AWS credentials to Workload Factory using an AWS CloudFormation stack by selecting the Workload Factory 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.

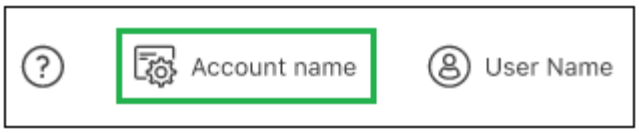
Before you begin

- 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:

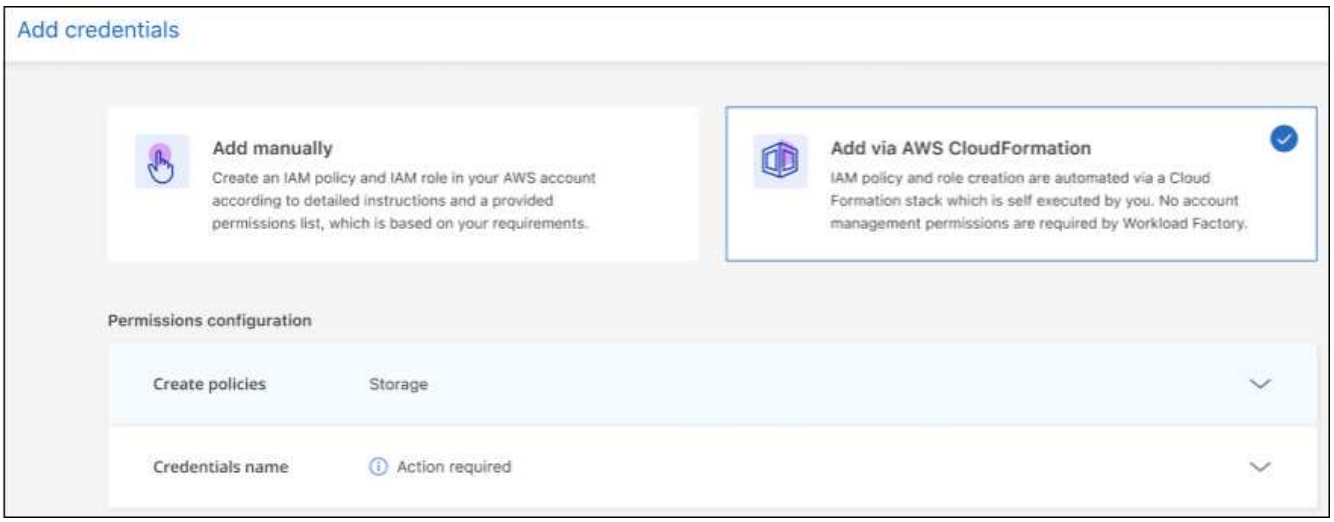
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:UpdateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "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. In the Workload Factory console, select the **Account** icon, and select **Credentials**.



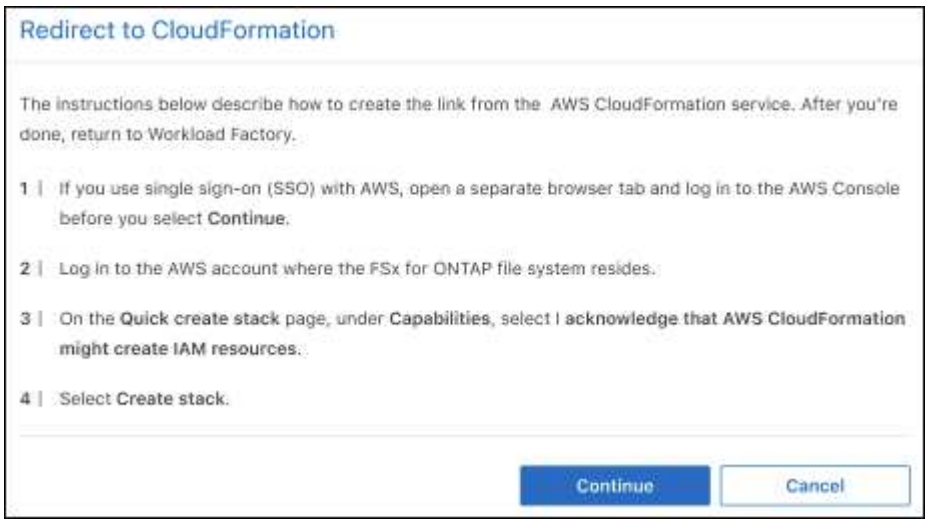
2. On the **Credentials** page, select **Add credentials**.
3. Select **Add via AWS CloudFormation**.



4. 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.

5. Under **Credentials name**, enter the name that you want to use for these credentials.
6. 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 Workload Factory and monitor to Credentials page to verify that the new credentials are in progress, or that they have been added.

What you can do next

Now that you've logged in and set up Workload Factory, you can start using several Workload Factory capabilities, such as creating Amazon FSx for ONTAP file systems, deploying databases on FSx for ONTAP file systems, and migrating virtual machine configurations to VMware Cloud on AWS using FSx for ONTAP file systems as external datastores.

- Amazon FSx for NetApp ONTAP

  Assess and analyze current data estates for potential cost savings by using FSx for ONTAP as the storage infrastructure, provision and templatize FSx for ONTAP deployments based on best practices, and access advanced management capabilities.

- GenAI

  Deploy and manage a Retrieval-Augmented Generation (RAG) infrastructure to improve the accuracy and uniqueness of your AI applications. Create a RAG knowledge base on FSx for ONTAP with built-in data security and compliance.

- Database workloads

  Detect your existing database estate on AWS, assess potential cost savings by moving to FSx for ONTAP, deploy databases end-to-end with built-in best practices for optimization, and automate thin cloning for CI/CD pipelines.

- VMware workloads

  Streamline migrations and operations with smart recommendations and automatic remediation. Deploy efficient backups and robust disaster recovery. Monitor and troubleshoot your VMs.

Copyright information

Trademark information