BlueXP workload factory setup and administration documentation

Setup and administration

NetApp
May 13, 2025

Table of Contents

BlueXP workload factory setup and administration documentation

Release notes

What’s new with BlueXP workload factory administration features

Learn what’s new with workload factory administration features: cloud provider credentials, Codebox enhancements, and more.

04 May 2025

CloudShell autocomplete support

When using BlueXP workload factory CloudShell, you can start typing a command and press the Tab key to view available options. If multiple possibilities exist, the CLI will display a list of suggestions. This feature enhances productivity by minimizing errors and speeding up command execution.

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

CloudShell reports AI-generated error responses for ONTAP CLI commands

When using CloudShell, each time you issue an ONTAP CLI command and an error occurs, you can get AI-generated error responses that include a description of the failure, the cause of the failure, and a detailed resolution.

Use CloudShell

iam:SimulatePermissionPolicy permission update

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

Permissions reference change log

02 February 2025

CloudShell available in BlueXP workload factory console

CloudShell is available from anywhere in the BlueXP workload factory console. CloudShell allows you to use the AWS and ONTAP credentials that you’ve provided in your BlueXP account and execute AWS CLI commands or ONTAP CLI commands in a shell-like environment.

Use CloudShell

Permissions update for Databases

The following permission is now available in *read* mode for Databases: `iam:SimulatePrincipalPolicy`.

Permissions reference change log

22 January 2025

BlueXP workload factory permissions

You can now view the permissions that BlueXP workload factory uses to execute various operations starting from the discovery of your storage environments to deploying AWS resources such as file systems in Storage or knowledge bases for GenAI workloads. You can view IAM policies and permissions for Storage, Databases, VMware, and GenAI workloads.

BlueXP workload factory permissions

5 January 2025

Support for service accounts in BlueXP workload factory

Service accounts are now supported in BlueXP workload factory. You can create service accounts to act as machine users that automate infrastructure operations.

Create and manage service accounts

11 November 2024

Workload factory integration in the BlueXP console

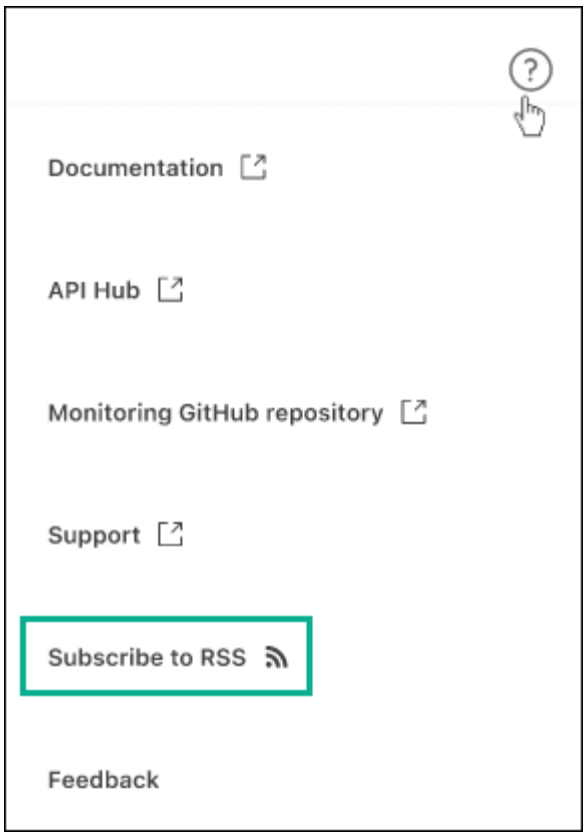
You now have the ability to use workload factory from the BlueXP console. The BlueXP console experience provides the same functionality as the workload factory console.

Learn how to access workload factory from the BlueXP console

1 September 2024

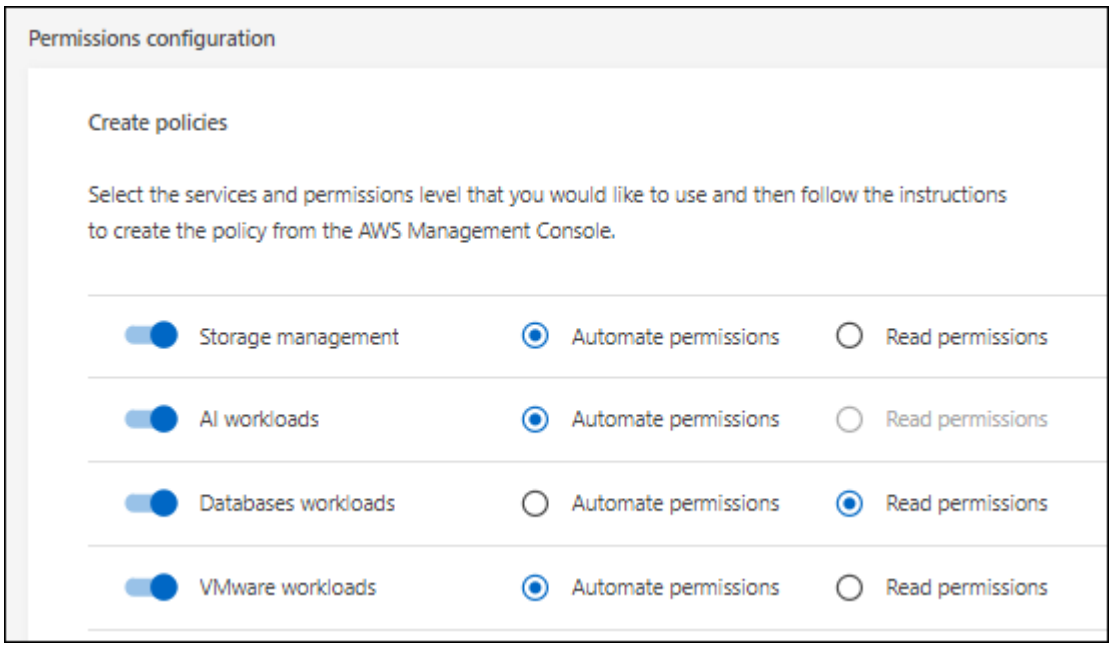
RSS subscription

RSS subscription is available from the workload factory console. Using an RSS feed is an easy way to consume and be aware of changes in BlueXP workload factory.



Support for a single permission policy per workload

When adding AWS credentials in workload factory, you can now select a single permission policy, either read or automate mode, for each workload and storage management.



Add AWS credentials to workload factory

4 August 2024

Terraform support

Terraform support is available for Amazon FSx for NetApp ONTAP file system deployment and storage VM creation. The setup and admin guide now has instructions for how to use Terraform from the Codebox.

Use Terraform from Codebox

7 July 2024

Initial release of BlueXP workload factory

BlueXP 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.

Get started

Learn the basics

Learn about BlueXP workload factory

BlueXP 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.

Database lifecycle management

Discover database workloads and analyze costs savings with Amazon FSx for NetApp ONTAP; leverage storage and application benefits when migrating SQL server databases to FSx for ONTAP storage; deploy SQL servers, databases, and database clones that implement vendor best practices; use an Infrastructure as Code co-pilot to automate operations; and continuously monitor and optimize SQL server estates to improve performance, availability, protection, and cost-efficiency.

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.

Savings 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.

Service accounts to promote automation

Use service accounts to automate BlueXP workload factory operations securely and reliably. Service accounts provide reliable, long-lasting automation without any user management restrictions and are more secure because they only provide API access.

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.

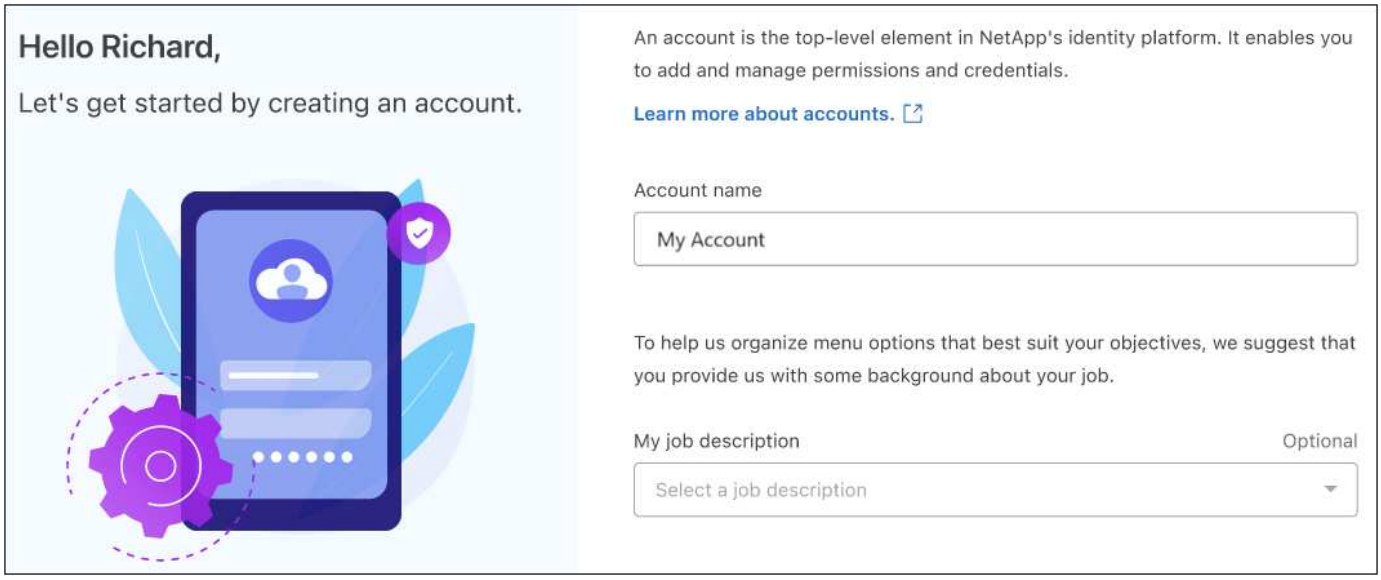
Software-as-a-service

Workload factory is accessible through the BlueXP workload factory web-based console and the BlueXP web-based console. These SaaS experiences enables you to automatically access the latest features as they're released and to easily switch between your Workload Factory accounts and links.

Learn more about the different console experiences.

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.

Service accounts

A service account acts as a "user" that can make authorized API calls to BlueXP workload factory for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. All account holders in Workload Factory are considered account admins. Account admins can create and delete multiple service accounts.

Learn how to manage service 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-only mode** enhances the experience of Basic mode by assisting the user in detecting various resources and tools, and consequently, helping to complete relevant wizards.
- **Read/Write 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 savings calculators so you can compare the costs of your storage environments or your database workloads 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.

- Learn how to explore savings for your storage environments
- Learn how to explore savings for your database workloads

https://raw.githubusercontent.com/NetAppDocs/workload-family/main/_include/learn-about-tools.adoc

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-only 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.

Read/Write 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.

Learn more about permissions for BlueXP workload factory.

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-only	No	Moderately complete IaC template	Yes	Yes
Read/Write	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-only	Read-only	Not required
Read/Write	Read-write credentials	Required

Learn more about links

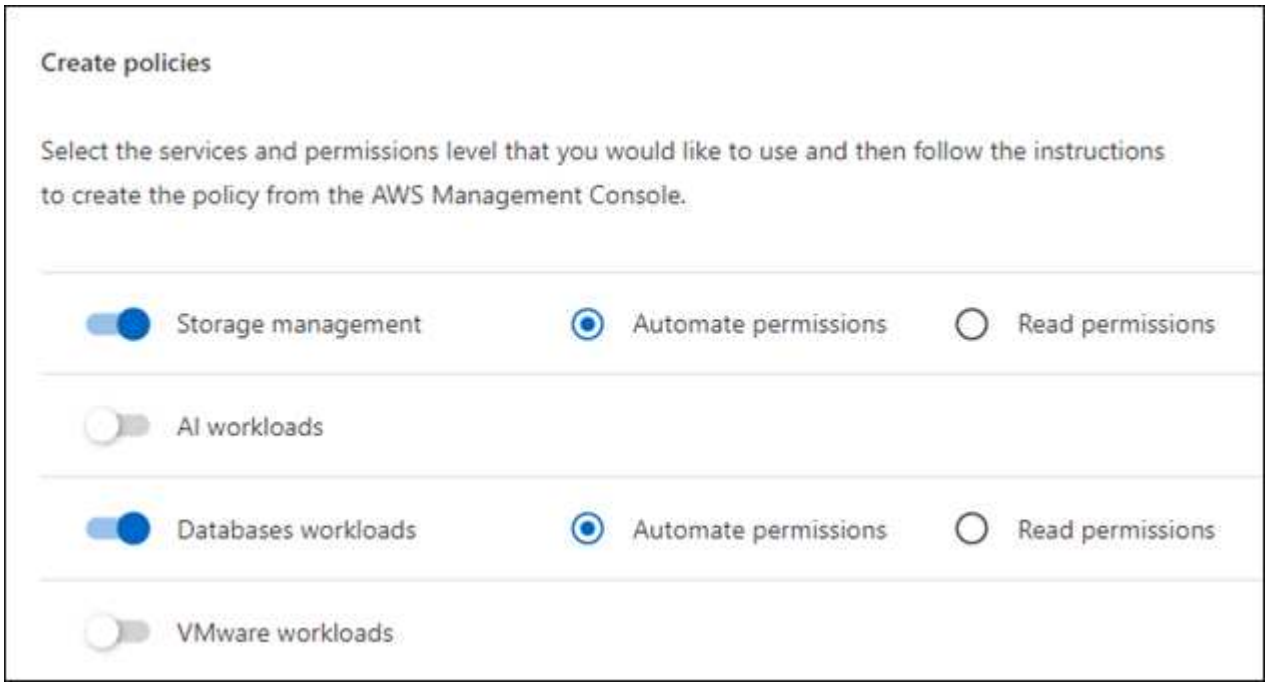
Operational mode examples

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 Read/Write 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 (Read/Write mode) for creating FSx for ONTAP file systems, deploying databases, and viewing other types of AWS storage used in the account.

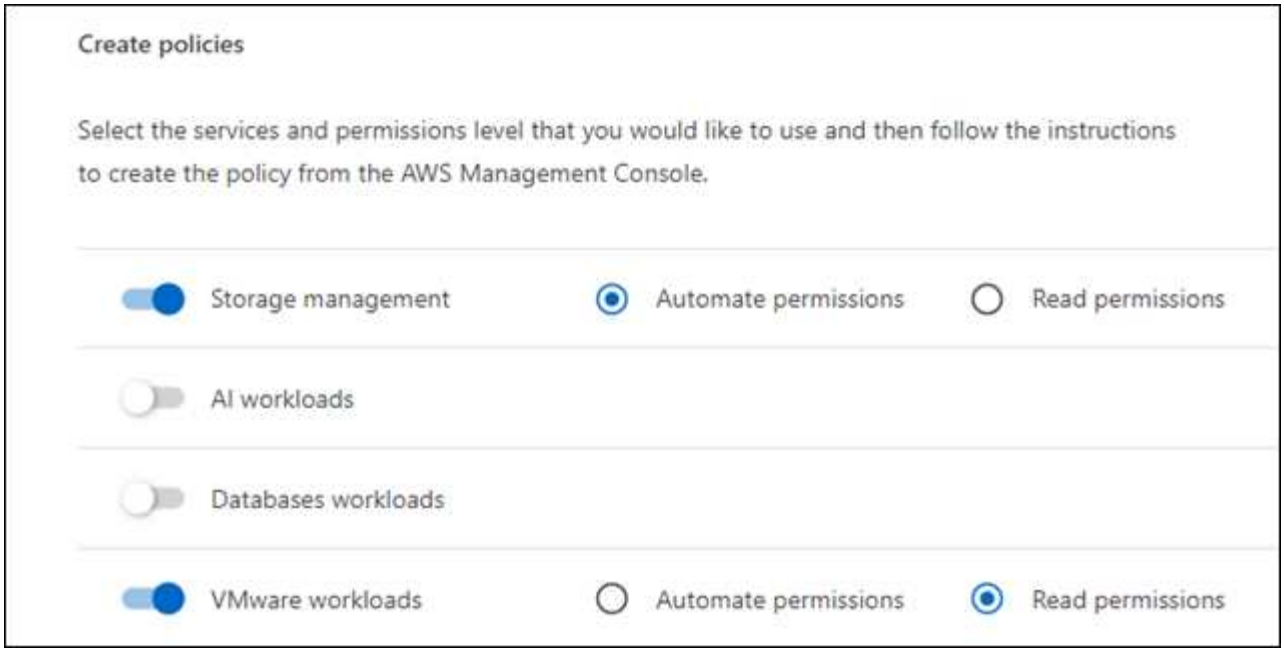


However, they will have no automation controls for creating and deploying VMware workloads (Basic mode) from workload factory. If they want to create VMware workloads, they'll need to copy the code from the Codebox, log in to their AWS account manually, and manually populate missing entries in the generated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

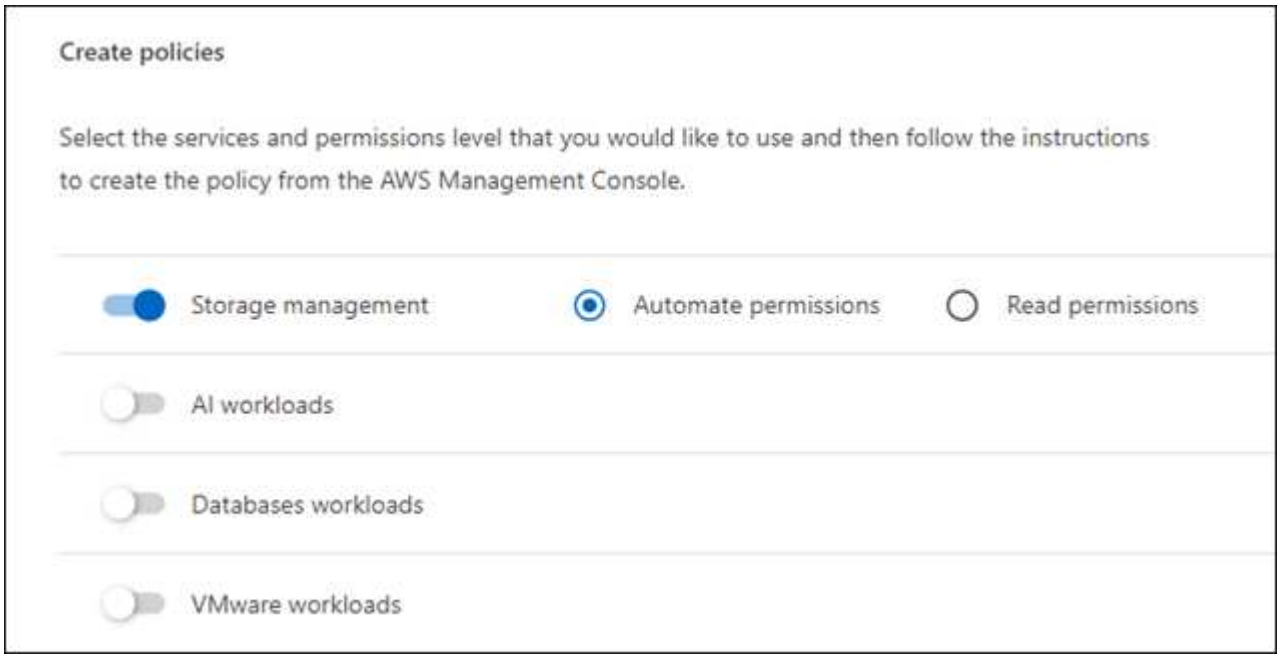
Example 2

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.

Console experiences

BlueXP workload factory is accessible via two web-based consoles. Learn how to access BlueXP workload factory using the BlueXP workload factory console and the BlueXP console.

You can use two consoles to access BlueXP workload factory.

- **BlueXP console**: Offers a hybrid experience where you can manage your working environments and workloads in the same place.
- **Workload factory console**: Offers a dedicated workload factory experience focused on workloads running on Amazon FSx for NetApp ONTAP.

Access workload factory in the BlueXP console

You can access workload factory from BlueXP. In addition to using BluXP Workload Factory for AWS storage and workload capabilities, you can also access other BlueXP platform services like Copy and Sync, Digital Wallet, and more.

Steps

1. Log in to the workload factory console
2. Navigate to the workload you'd like to use and select an option to get started.

Access workload factory in the Workload Factory console

You can access workload factory from the Workload Factory console.

Steps

1. Log in to the BlueXP console

2. Select **Workloads** from the left navigation.
3. Select **Home** to view all workloads or select one workload like **Storage** or **Databases**.
4. Select an option to get started in the workload.

Permissions for BlueXP workload factory

To use BlueXP workload factory features and services, you'll need to provide permissions so that workload factory can perform operations in your cloud environment.

Why use permissions

When you provide Read-only or Read/Write mode permissions, workload factory attaches a policy to the instance with permissions to manage resources and processes within that AWS account. This allows workload factory to execute various operations starting from discovery of your storage environments to deploying AWS resources such as file systems in storage management or knowledge bases for GenAI workloads.

For database workloads for example, when workload factory is granted with the required permissions, it scans all EC2 instances in a given account and region, and filters all Windows-based machines. If AWS Systems Manager (SSM) Agent is installed and running on the host and System Manager networking is configured properly, workload factory can access the Windows machine and verify whether SQL Server software is installed or not.

Permissions by workload

Each workload uses permissions to perform certain tasks in workload factory. Scroll to the workload you use to view the list of permissions, their purpose, where they are used, and which modes support them.

Permissions for Storage

The IAM policies available for Storage provide the permissions that workload factory needs to manage resources and processes within your public cloud environment based on the operational mode you operate in.

Select your operational mode to view the required IAM policies:

IAM policies for Storage

Read-only mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "ec2:Describe*",
        "kms:Describe*",
        "elasticfilesystem:Describe*",
        "kms:List*",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Read/Write mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "iam:CreateServiceLinkedRole",
        "kms:Describe*",
        "elasticfilesystem:Describe*",
        "kms:List*",
        "kms:CreateGrant",
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricData",
        "iam:SimulatePrincipalPolicy",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    }
  ]
}
```

The following table displays the permissions for Storage.

Table of permissions for Storage

Purpose	Action	Where used	Mode
Create an FSx for ONTAP file system	fsx:CreateFileSystem*	Deployment	Read/Write
Create a security group for an FSx for ONTAP file system	ec2:CreateSecurityGroup	Deployment	Read/Write
Add tags to a security group for an FSx for ONTAP file system	ec2:CreateTags	Deployment	Read/Write
Authorize security group egress and ingress for an FSx for ONTAP file system	ec2:AuthorizeSecurityGroupEgress	Deployment	Read/Write
	ec2:AuthorizeSecurityGroupIngress	Deployment	Read/Write
Granted role provides communication between FSx for ONTAP and other AWS services	iam:CreateServiceLinkedRole	Deployment	Read/Write
Get details to fill in the FSx for ONTAP file system deployment form	ec2:DescribeVpcs	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeSubnets	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeRegions	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeSecurityGroups	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeRouteTables	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeNetworkInterfaces	• Deployment • Explore savings	• Read-only • Read/Write
	ec2:DescribeVolumeStatus	• Deployment • Explore savings	• Read-only • Read/Write

Purpose	Action	Where used	Mode
Get KMS key details and use for FSx for ONTAP encryption	kms:CreateGrant	Deployment	Read/Write
	kms:Describe*	Deployment	• Read-only • Read/Write
	kms:List*	Deployment	• Read-only • Read/Write
Get volume details for EC2 instances	ec2:DescribeVolumes	• Inventory • Explore savings	• Read-only • Read/Write
Get details for EC2 instances	ec2:DescribeInstances	Explore savings	• Read-only-only • Read/Write
Describe Elastic File System in the savings calculator	elasticfilesystem:Describe*	Explore savings	Read-only
List tags for FSx for ONTAP resources	fsx:ListTagsForResource	Inventory	• Read-only • Read/Write
Manage security group egress and ingress for an FSx for ONTAP file system	ec2:RevokeSecurityGroupIngress	Management operations	Read/Write
	ec2:DeleteSecurityGroup	Management operations	Read/Write

Purpose	Action	Where used	Mode
Create, view, and manage FSx for ONTAP file system resources	fsx:CreateVolume*	Management operations	Read/Write
	fsx:TagResource*	Management operations	Read/Write
	fsx:CreateStorageVirtualMachine*	Management operations	Read/Write
	fsx:DeleteFileSystem*	Management operations	Read/Write
	fsx:DeleteStorageVirtualMachine*	Management operations	Read/Write
	fsx:DescribeFileSystems*	Inventory	• Read-only • Read/Write
	fsx:DescribeStorageVirtualMachines*	Inventory	• Read-only • Read/Write
	fsx:UpdateFileSystem*	Management operations	Read/Write
	fsx:UpdateStorageVirtualMachine*	Management operations	Read/Write
	fsx:DescribeVolumes*	Inventory	• Read-only • Read/Write
	fsx:UpdateVolume*	Management operations	Read/Write
	fsx:DeleteVolume*	Management operations	Read/Write
	fsx:UntagResource*	Management operations	Read/Write
	fsx:DescribeBackups*	Management operations	• Read-only • Read/Write
	fsx:CreateBackup*	Management operations	Read/Write
	fsx:CreateVolumeFromBackup*	Management operations	Read/Write
Report CloudWatch metrics	cloudwatch:PutMetricData	Management operations	Read/Write

Purpose	Action	Where used	Mode
Get file system and volume metrics	cloudwatch:GetMetricData	Management operations	• Read-only • Read/Write
	cloudwatch:GetMetricStatistics	Management operations	• Read-only • Read/Write

Permissions for Databases workloads

The IAM policies available for Databases workloads provide the permissions that workload factory needs to manage resources and processes within your public cloud environment based on the operational mode you operate in.

Select your operational mode to view the required IAM policies:

IAM policies for Databases workloads

Read-only mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CommonGroup",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics",
        "sns:ListTopics",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAddresses",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:DescribeKey",
        "cloudformation:ListStacks",
        "cloudformation:DescribeAccountLimits",
        "ds:DescribeDirectories",
        "fsx:DescribeVolumes",
        "fsx:DescribeBackups",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeFileSystems",
        "servicequotas:ListServiceQuotas",
        "ssm:GetParametersByPath",
        "ssm:GetCommandInvocation",
        "ssm:SendCommand",
        "ssm:GetConnectionStatus",
        "ssm:DescribePatchBaselines",
        "ssm:DescribeInstancePatchStates",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation",
        "fsx:ListTagsForResource"
```

```
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:DeleteParameters"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
    },
    {
      "Sid": "SSMResponseCloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Read/Write mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateAddress",
```

```
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVolume",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVolume",
        "ec2:DisassociateAddress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyInstancePlacement",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolume",
        "ec2:ModifyVolumeAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "WLMDB*"
        }
      }
    },
    {
      "Sid": "FSxNGroup",
```

```
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/aws:cloudformation:stack-name": "WLMDB*"
        }
      }
    },
    {
      "Sid": "CommonGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:GetMetricStatistics",
        "ds:DescribeDirectories",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:RunInstances",
        "ec2:ModifyVpcAttribute",
        "ec2messages:*",
        "fsx:CreateFileSystem",
        "fsx:UpdateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:UpdateVolume",
        "fsx:Describe*",
        "fsx:List*",
        "kms:CreateGrant",
        "kms:Describe*",
        "kms:List*",
        "kms:GenerateDataKey",
        "kms:Decrypt",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLog*",
        "logs:GetLog*",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "servicequotas:ListServiceQuotas",
        "sns:ListTopics",
        "sns:Publish",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:PutInventory",
        "ssm:SendCommand",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation",
        "ssmmessages:*",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:PutRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ArnGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:SignalResource"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/WLMDB*",
        "arn:aws:logs:*:*:log-group:WLMDB*"
      ]
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
```

```
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole",
        "iam:DeleteInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup1",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:DeleteParameters"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

The following table displays the permissions for database workloads.

Table of permissions for database workloads

Purpose	Action	Where used	Mode
Get metric statistics for FSx for ONTAP, EBS, and FSx for Windows File Server	cloudwatch:GetMetricStatistics	• Inventory • Explore savings	• Read-only • Read/Write
List and set triggers for events	sns:ListTopics	Deployment	• Read-only • Read/Write
Get details for EC2 instances	ec2:DescribeInstances	• Inventory • Explore savings	• Read-only • Read/Write
	ec2:DescribeKeyPairs	Deployment	• Read-only • Read/Write
	ec2:DescribeNetworkInterfaces	Deployment	• Read-only • Read/Write
	ec2:DescribeInstanceTypes	• Deployment • Explore savings	• Read-only • Read/Write
Get details to fill in the FSx for ONTAP deployment form	ec2:DescribeVpcs	• Deployment • Inventory	• Read-only • Read/Write
	ec2:DescribeSubnets	• Deployment • Inventory	• Read-only • Read/Write
	ec2:DescribeSecurityGroups	Deployment	• Read-only • Read/Write
	ec2:DescribeImages	Deployment	• Read-only • Read/Write
	ec2:DescribeRegions	Deployment	• Read-only • Read/Write
	ec2:DescribeRouteTables	• Deployment • Inventory	• Read-only • Read/Write

Purpose	Action	Where used	Mode
Get any existing VPC endpoints to determine if new endpoints need to be created before deployments	ec2:DescribeVpcEndpoints	• Deployment • Inventory	• Read-only • Read/Write
Create VPC endpoints if they don’t exist for required services irrespective of public network connectivity on EC2 instances	ec2:CreateVpcEndpoint	Deployment	Read/Write
Get instance types available in region for validation nodes (t2.micro/t3.micro)	ec2:DescribeInstanceTypeOfferings	Deployment	• Read-only • Read/Write
Get snapshot details of each attached EBS volumes for pricing and savings estimate	ec2:DescribeSnapshots	Explore savings	• Read-only • Read/Write
Get details of each attached EBS volumes for pricing and savings estimate	ec2:DescribeVolumes	• Inventory • Explore savings	• Read-only • Read/Write
Get KMS key details for FSx for ONTAP file system encryption	kms:ListAliases	Deployment	• Read-only • Read/Write
	kms:ListKeys	Deployment	• Read-only • Read/Write
	kms:DescribeKey	Deployment	• Read-only • Read/Write
Get list of CloudFormation stacks running in the environment to check quota limit	cloudformation:ListStacks	Deployment	• Read-only • Read/Write
Check account limits for resources before triggering deployment	cloudformation:DescribeAccountLimits	Deployment	• Read-only • Read/Write
Get list of AWS-managed Active Directories in the region	ds:DescribeDirectories	Deployment	• Read-only • Read/Write

Purpose	Action	Where used	Mode
Get lists and details of volumes, backups, SVMs, file systems in AZs, and tags for FSx for ONTAP file system	fsx:DescribeVolumes	• Inventory • Explore Savings	• Read-only • Read/Write
	fsx:DescribeBackups	• Inventory • Explore Savings	• Read-only • Read/Write
	fsx:DescribeStorageVirtualMachines	• Deployment • Manage operations • Inventory	• Read-only • Read/Write
	fsx:DescribeFileSystems	• Deployment • Manage operations • Inventory • Explore savings	• Read-only • Read/Write
	fsx:ListTagsForResource	Manage operations	• Read-only • Read/Write
Get service quota limits for CloudFormation and VPC	servicequotas:ListServiceQuotas	Deployment	• Read-only • Read/Write
Use SSM-based query to get the updated list of FSx for ONTAP supported regions	ssm:GetParametersByPath	Deployment	• Read-only • Read/Write
Poll for SSM response after sending command for manage operations post deployment	ssm:GetCommandInvocation	• Manage operations • Inventory • Explore savings • Optimization	• Read-only • Read/Write

Purpose	Action	Where used	Mode
Send commands over SSM to EC2 instances	ssm:SendCommand	• Manage operations • Inventory • Explore savings • Optimization	• Read-only • Read/Write
Get the SSM connectivity status on instances post deployment	ssm:GetConnectionStatus	• Manage operations • Inventory • Optimization	• Read-only • Read/Write
Fetch SSM association status for a group of managed EC2 instances (SQL nodes)	ssm:DescribeInstanceInformation	Inventory	Read
Get the list of available patch baselines for operating system patch assessment	ssm:DescribePatchBaselines	Optimization	• Read-only • Read/Write
Get the patching state on Windows EC2 instances for operating system patch assessment	ssm:DescribeInstancePatchStates	Optimization	• Read-only • Read/Write
List commands executed by AWS Patch Manager on EC2 instances for operating system patch management	ssm:ListCommands	Optimization	• Read-only • Read/Write
Check if account is enrolled in AWS Compute Optimizer	compute-optimizer:GetEnrollmentStatus	• Explore savings • Optimization	Read/Write
Update an existing recommendation preference in AWS Compute Optimizer to tailor suggestions for SQL server workloads	compute-optimizer:PutRecommendationPreferences	• Explore savings • Optimization	Read/Write

Purpose	Action	Where used	Mode
Get recommendation preferences that are in effect for a given resource from AWS Compute Optimizer	compute-optimizer:GetEffectiveRecommendationPreferences	• Explore savings • Optimization	Read/Write
Fetch recommendations that AWS Compute Optimizer generates for Amazon Elastic Compute Cloud (Amazon EC2) instances	compute-optimizer:GetEC2InstanceRecommendations	• Explore savings • Optimization	Read/Write
Check for instance association to auto-scaling groups	autoscaling:DescribeAutoScalingGroups	• Explore savings • Optimization	Read/Write
	autoscaling:DescribeAutoScalingInstances	• Explore savings • Optimization	Read/Write
Get, list, create, and delete SSM parameters for AD, FSx for ONTAP, and SQL user credentials used during deployment or managed in your AWS account	ssm:GetParameter [1]	• Deployment • Manage operations	• Read-only • Read/Write
	ssm:GetParameters [1]	Manage operations	• Read-only • Read/Write
	ssm:PutParameter [1]	• Deployment • Manage operations	• Read-only • Read/Write
	ssm:DeleteParameters [1]	Manage operations	• Read-only • Read/Write

Purpose	Action	Where used	Mode
Associate network resources to SQL nodes and validation nodes, and add additional secondary IPs to SQL nodes	ec2:AllocateAddress [1]	Deployment	Read/Write
	ec2:AllocateHosts [1]	Deployment	Read/Write
	ec2:AssignPrivateIpAddresses [1]	Deployment	Read/Write
	ec2:AssociateAddress [1]	Deployment	Read/Write
	ec2:AssociateRouteTable [1]	Deployment	Read/Write
	ec2:AssociateSubnetCidrBlock [1]	Deployment	Read/Write
	ec2:AssociateVpcCidrBlock [1]	Deployment	Read/Write
	ec2:AttachInternetGateway [1]	Deployment	Read/Write
	ec2:AttachNetworkInterface [1]	Deployment	Read/Write
Attach EBS volumes required to the SQL nodes for deployment	ec2:AttachVolume	Deployment	Read/Write
Attach security groups and modify rules for the provisioned nodes	ec2:AuthorizeSecurityGroupEgress	Deployment	Read/Write
	ec2:AuthorizeSecurityGroupIngress	Deployment	Read/Write
Create EBS volumes required to the SQL nodes for deployment	ec2:CreateVolume	Deployment	Read/Write
Remove the temporary validation nodes created of type t2.micro and for rollback or retry of failed EC2 SQL nodes	ec2:DeleteNetworkInterface	Deployment	Read/Write
	ec2:DeleteSecurityGroup	Deployment	Read/Write
	ec2:DeleteTags	Deployment	Read/Write
	ec2:DeleteVolume	Deployment	Read/Write
	ec2:DetachNetworkInterface	Deployment	Read/Write
	ec2:DetachVolume	Deployment	Read/Write
	ec2:DisassociateAddress	Deployment	Read/Write
	ec2:DisassociateIamInstanceProfile	Deployment	Read/Write
	ec2:DisassociateRouteTable	Deployment	Read/Write
	ec2:DisassociateSubnetCidrBlock	Deployment	Read/Write
	ec2:DisassociateVpcCidrBlock	Deployment	Read/Write

Purpose	Action	Where used	Mode
Modify attributes for created SQL instances. Only applicable to names that start with WLMDB.	ec2:ModifyInstanceAttribute	Deployment	Read/Write
	ec2:ModifyInstancePlacement	Deployment	Read/Write
	ec2:ModifyNetworkInterfaceAttribute	Deployment	Read/Write
	ec2:ModifySubnetAttribute	Deployment	Read/Write
	ec2:ModifyVolume	Deployment	Read/Write
	ec2:ModifyVolumeAttribute	Deployment	Read/Write
	ec2:ModifyVpcAttribute	Deployment	Read/Write
Disassociate and destroy validation instances	ec2:ReleaseAddress	Deployment	Read/Write
	ec2:ReplaceRoute	Deployment	Read/Write
	ec2:ReplaceRouteTableAssociation	Deployment	Read/Write
	ec2:RevokeSecurityGroupEgress	Deployment	Read/Write
	ec2:RevokeSecurityGroupIngress	Deployment	Read/Write
Start the deployed instances	ec2:StartInstances	Deployment	Read/Write
Stop the deployed instances	ec2:StopInstances	Deployment	Read/Write
Tag custom values for Amazon FSx for NetApp ONTAP resources created by WLMDB to get billing details during resource management	fsx:TagResource [1]	• Deployment • Manage operations	Read/Write
Create and validate CloudFormation template for deployment	cloudformation:CreateStack	Deployment	Read/Write
	cloudformation:DescribeStackEvents	Deployment	Read/Write
	cloudformation:DescribeStacks	Deployment	Read/Write
	cloudformation:ListStacks	Deployment	Read/Write
	cloudformation:ValidateTemplate	Deployment	Read/Write
Fetch metrics for compute optimization recommendation	cloudwatch:GetMetricStatistics	Explore savings	Read/Write
Fetch directories available in the region	ds:DescribeDirectories	Deployment	Read/Write
Add rules for the Security Group attached to provisioned EC2 instances	ec2:AuthorizeSecurityGroupEgress	Deployment	Read/Write
	ec2:AuthorizeSecurityGroupIngress	Deployment	Read/Write

Purpose	Action	Where used	Mode
Create nested stack templates for retry and rollback	ec2:CreateLaunchTemplate	Deployment	Read/Write
	ec2:CreateLaunchTemplateVersion	Deployment	Read/Write
Manage tags and network security on created instances	ec2:CreateNetworkInterface	Deployment	Read/Write
	ec2:CreateSecurityGroup	Deployment	Read/Write
	ec2:CreateTags	Deployment	Read/Write
Delete the Security Group created temporarily for validation nodes	ec2:DeleteSecurityGroup	Deployment	Read/Write
Get instance details for provisioning	ec2:Describe*	• Deployment • Inventory • Explore savings	Read/Write
	ec2:Get*	• Deployment • Inventory • Explore savings	Read/Write
Start the created instances	ec2:RunInstances	Deployment	Read/Write
Systems Manager uses AWS message delivery service endpoint for API operations	ec2messages:*	• Deployment *Inventory	Read/Write
Create FSx for ONTAP resources required for provisioning. For existing FSx for ONTAP systems, a new SVM is created to host SQL volumes.	fsx:CreateFileSystem	Deployment	Read/Write
	fsx:CreateStorageVirtualMachine	Deployment	Read/Write
	fsx:CreateVolume	• Deployment • Manage operations	Read/Write
Get FSx for ONTAP details	fsx:Describe*	• Deployment • Inventory • Manage operations • Explore savings	Read/Write
	fsx:List*	• Deployment • Inventory	Read/Write

Purpose	Action	Where used	Mode
Resize FSx for ONTAP file system to remediate file system headroom	fsx:UpdateFilesystem	Optimization	Read/Write
Resize volumes to remediate log and TempDB drive sizes	fsx:UpdateVolume	Optimization	Read/Write
Get KMS key details and use for FSx for ONTAP encryption	kms:CreateGrant	Deployment	Read/Write
	kms:Describe*	Deployment	Read/Write
	kms:List*	Deployment	Read/Write
	kms:GenerateDataKey	Deployment	Read/Write
Create CloudWatch logs for validation and provisioning scripts running on EC2 instances	logs:CreateLogGroup	Deployment	Read/Write
	logs:CreateLogStream	Deployment	Read/Write
	logs:DescribeLog*	Deployment	Read/Write
	logs:GetLog*	Deployment	Read/Write
	logs:ListLogDeliveries	Deployment	Read/Write
	logs:PutLogEvents	• Deployment • Manage operations	Read/Write
	logs:TagResource	Deployment	Read/Write
Workload factory switches to Amazon CloudWatch logs for the SQL instance upon encountering SSM output truncation	logs:GetLogEvents	• Storage assessment (Optimization) • Inventory	• Read-only • Read/Write
Allow workload factory to get current log groups and check that retention is set for log groups created by workload factory	logs:DescribeLogGroups	• Storage assessment (Optimization) • Inventory	Read-only
Allow workload factory to set a one-day retention policy for log groups created by workload factory to avoid unnecessary accumulation of log streams for SSM command outputs	logs:PutRetentionPolicy	• Storage assessment (Optimization) • Inventory	• Read-only • Read/Write
Create secrets in a user account for the credentials provided for SQL, domain, and FSx for ONTAP	servicequotas:ListServiceQuotas	Deployment	Read/Write

Purpose	Action	Where used	Mode
List customer SNS topics and publish to WLMDB backend SNS as well as customer SNS if selected	sns:ListTopics	Deployment	Read/Write
	sns:Publish	Deployment	Read/Write
Required SSM permissions to run the discovery script on provisioned SQL instances and to fetch latest list of FSx for ONTAP supported AWS regions.	ssm:Describe*	Deployment	Read/Write
	ssm:Get*	• Deployment • Manage operations	Read/Write
	ssm:List*	Deployment	Read/Write
	ssm:PutComplianceItems	Deployment	Read/Write
	ssm:PutConfigurePackageResult	Deployment	Read/Write
	ssm:PutInventory	Deployment	Read/Write
	ssm:SendCommand	• Deployment • Inventory • Manage operations	Read/Write
	ssm:UpdateAssociationStatus	Deployment	Read/Write
	ssm:UpdateInstanceAssociationStatus	Deployment	Read/Write
	ssm:UpdateInstanceInformation	Deployment	Read/Write
	ssmmessages:*	• Deployment • Inventory • Manage operations	Read/Write

Purpose	Action	Where used	Mode
Save credentials for FSx for ONTAP, Active Directory, and SQL user (only for SQL user authentication)	ssm:GetParameter [1]	• Deployment • Manage operations • Inventory	Read/Write
	ssm:GetParameters [1]	• Deployment • Inventory	Read/Write
	ssm:PutParameter [1]	• Deployment • Manage operations	Read/Write
	ssm:DeleteParameters [1]	• Deployment • Manage operations	Read/Write
Signal CloudFormation stack on success or failure.	cloudformation:SignalResource [1]	Deployment	Read/Write
Add EC2 role created by template to the instance profile of EC2 to allow scripts on EC2 to access the required resources for deployment.	iam:AddRoleToInstanceProfile	Deployment	Read/Write
Create instance profile for EC2 and attach the created EC2 role.	iam:CreateInstanceProfile	Deployment	Read/Write
Create EC2 role through template with permissions listed below	iam:CreateRole	Deployment	Read/Write
Create role linked to EC2 service	iam:CreateServiceLinkedRole [2]	Deployment	Read/Write
Delete instance profile created during deployment specifically for the validation nodes	iam:DeleteInstanceProfile	Deployment	Read/Write
Get the role and policy details to determine any gaps in permission and validate for deployment	iam:GetPolicy	Deployment	Read/Write
	iam:GetPolicyVersion	Deployment	Read/Write
	iam:GetRole	Deployment	Read/Write
	iam:GetRolePolicy	Deployment	Read/Write
	iam:GetUser	Deployment	Read/Write
Pass the role created to EC2 instance	iam:PassRole [3]	Deployment	Read/Write
Add policy with required permissions to the EC2 role created	iam:PutRolePolicy	Deployment	Read/Write

Purpose	Action	Where used	Mode
Detach role from the provisioned EC2 instance profile	iam:RemoveRoleFromInstanceProfile	Deployment	Read/Write
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	• Read-only • Read/Write

1. Permission is restricted to resources starting with WLMDB.
2. "iam:CreateServiceLinkedRole" limited by "iam:AWSServiceName": "ec2.amazonaws.com"*
3. "iam:PassRole" limited by "iam:PassedToService": "ec2.amazonaws.com"*

Permissions for GenAI workloads

The IAM policies for VMware workloads provide the permissions that workload factory for VMware needs to manage resources and processes within your public cloud environment based on the operational mode you operate in.

GenAI IAM policies are only available in Read/Write mode:

IAM policies for GenAI workloads

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "FSXNGroup",
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FSXNGroup2",
      "Effect": "Allow",
      "Action": [
        "fsx:UntagResource",
```

```
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
    },
    {
      "Sid": "SSMMessages",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMCommandDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
      ]
    },
    {
      "Sid": "SSMCommandInstance",
      "Effect": "Allow",
```

```
      "Action": [
        "ssm:SendCommand",
        "ssm:GetConnectionStatus"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
        }
      }
    },
    {
      "Sid": "KMS",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchAiEngine",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
    },
    {
      "Sid": "CloudWatchAiEngineLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
    },
    {
      "Sid": "BedrockGroup",
      "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchBedrock",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
    },
    {
      "Sid": "BedrockLoggingAttachRole",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    },
    {
      "Sid": "BedrockLoggingIamOperations",
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:ListApplications"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

The following table provides details about the permissions for GenAI workloads.

Table of permissions for GenAI workloads

Purpose	Action	Where used	Mode
Create AI engine cloudformation stack during deploy and rebuild operations	cloudformation:CreateStack	Deployment	Read/Write
Create the AI engine cloudformation stack	cloudformation:DescribeStacks	Deployment	Read/Write
List regions for the AI engine deployment wizard	ec2:DescribeRegions	Deployment	Read/Write
Display AI engine tags	ec2:DescribeTags	Deployment	Read/Write
List VPC endpoints before AI engine stack creation	ec2:CreateVpcEndpoint	Deployment	Read/Write
Create an AI engine security group during the AI engine stack creation during deploy and rebuild operations	ec2:CreateSecurityGroup	Deployment	Read/Write
Tag resources created by AI engine stack creation during deploy and rebuild operations	ec2:CreateTags	Deployment	Read/Write
Publish encrypted events to the WLMAI backend from the AI engine stack	kms:GenerateDataKey	Deployment	Read/Write
	kms:Decrypt	Deployment	Read/Write
Publish events and custom resources to the WLMAI backend from the ai-engine stack	sns:Publish	Deployment	Read/Write
List VPCs during AI engine deployment wizard	ec2:DescribeVpcs	Deployment	Read/Write
List subnets on the ai-engine deployment wizard	ec2:DescribeSubnets	Deployment	Read/Write
Get route tables during AI engine deployment and rebuild	ec2:DescribeRouteTables	Deployment	Read/Write
List key-pairs during AI engine deployment wizard	ec2:DescribeKeyPairs	Deployment	Read/Write
List security groups during AI engine stack creation (to find security groups on the private endpoints)	ec2:DescribeSecurityGroups	Deployment	Read/Write
Get VPC endpoints to determine if any should be created during the AI engine deployment	ec2:DescribeVpcEndpoints	Deployment	Read/Write
List the Amazon Q Business applications	qbusiness:ListApplications	Deployment	Read/Write

Purpose	Action	Where used	Mode
List instances to find out the AI engine state	ec2:DescribeInstances	Troubleshooting	Read/Write
List images during the AI engine stack creation during deploy and rebuild operations	ec2:DescribeImages	Deployment	Read/Write
Create and update AI instance and private endpoint security group during the AI instance stack creation during deploy and rebuild operations	ec2:RevokeSecurityGroupEgress	Deployment	Read/Write
	ec2:RevokeSecurityGroupIngress	Deployment	Read/Write
Run AI engine during cloudformation stack creation during deploy and rebuild operations	ec2:RunInstances	Deployment	Read/Write
Attach security group and modify rules for the AI engine during stack creation during deploy and rebuild operations	ec2:AuthorizeSecurityGroupEgress	Deployment	Read/Write
	ec2:AuthorizeSecurityGroupIngress	Deployment	Read/Write
Query Amazon Bedrock / Amazon CloudWatch logging status during AI engine deployment	bedrock:GetModelInvocationLoggingConfiguration	Deployment	Read/Write
Initiate chat request to one of the foundation models	bedrock:InvokeModelWithResponseStream	Deployment	Read/Write
Begin chat/embedding request for foundation models	bedrock:InvokeModel	Deployment	Read/Write
Show the available foundation models in a region	bedrock:ListFoundationModels	Deployment	Read/Write
Get information about a foundation model	bedrock:GetFoundationModel	Deployment	Read/Write
Verify access to the foundation model	bedrock:GetFoundationModelAvailability	Deployment	Read/Write
Verify need to create Amazon CloudWatch log group during deploy and rebuild operations	logs:DescribeLogGroups	Deployment	Read/Write
Get regions that support FSx and Amazon Bedrock during the AI engine wizard	ssm:GetParametersByPath	Deployment	Read/Write
Get the latest Amazon Linux image for the AI engine deployment during deploy and rebuild operations	ssm:GetParameters	Deployment	Read/Write
Get the SSM response from the command sent to the AI engine	ssm:GetCommandInvocation	Deployment	Read/Write

Purpose	Action	Where used	Mode
Check the SSM connection to the AI engine	ssm:SendCommand	Deployment	Read/Write
	ssm:GetConnectionStatus	Deployment	Read/Write
Create AI engine instance profile during stack creation during deploy and rebuild operations	iam:CreateRole	Deployment	Read/Write
	iam:CreateInstanceProfile	Deployment	Read/Write
	iam:AddRoleToInstanceProfile	Deployment	Read/Write
	iam:PutRolePolicy	Deployment	Read/Write
	iam:GetRolePolicy	Deployment	Read/Write
	iam:GetRole	Deployment	Read/Write
	iam:TagRole	Deployment	Read/Write
	iam:PassRole	Deployment	Read/Write
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	Read/Write
List FSx for ONTAP file systems during the "Create knowledgebase" wizard	fsx:DescribeVolumes	Knowledge base creation	Read/Write
List FSx for ONTAP file system volumes during the "Create knowledgebase" wizard	fsx:DescribeFileSystems	Knowledge base creation	Read/Write
Manage knowledge bases on the AI engine during rebuild operations	fsx:ListTagsForResource	Troubleshooting	Read/Write
List FSx for ONTAP file system storage virtual machines during the "Create knowledgebase" wizard	fsx:DescribeStorageVirtualMachines	Deployment	Read/Write
Move the knowledgebase to a new instance	fsx:UntagResource	Troubleshooting	Read/Write
Manage knowledgebase on the AI engine during rebuild	fsx:TagResource	Troubleshooting	Read/Write
Save SSM secrets (ECR token, CIFS credentials, tenancy service accounts keys) in a secure way	ssm:GetParameter	Deployment	Read/Write
	ssm:PutParameter	Deployment	Read/Write
Send the AI engine logs to Amazon CloudWatch log group during deploy and rebuild operations	logs:CreateLogGroup	Deployment	Read/Write
	logs:PutRetentionPolicy	Deployment	Read/Write
Send the AI engine logs to Amazon CloudWatch log group	logs:TagResource	Troubleshooting	Read/Write

Purpose	Action	Where used	Mode
Get SSM response from Amazon CloudWatch (when the response is too long)	logs:DescribeLogStreams	Troubleshooting	Read/Write
Get the SSM response from Amazon CloudWatch	logs:GetLogEvents	Troubleshooting	Read/Write
Create an Amazon CloudWatch log group for Amazon Bedrock logs during the stack creation during deploy and rebuild operations	logs:CreateLogGroup	Deployment	Read/Write
	logs:PutRetentionPolicy	Deployment	Read/Write
	logs:TagResource	Deployment	Read/Write
Send bedrock logs to Amazon CloudWatch	bedrock:PutModelInvocationLoggingConfiguration	Troubleshooting	Read/Write
Create the role that enables sending Amazon Bedrock logs to Amazon CloudWatch	iam:AttachRolePolicy	Troubleshooting	Read/Write
Create the role that enables sending Amazon Bedrock logs to Amazon CloudWatch	iam:PassRole	Troubleshooting	Read/Write
Create the role that enables sending Amazon Bedrock logs to Amazon CloudWatch	iam:createPolicy	Troubleshooting	Read/Write
List inference profiles for the model	bedrock:ListInferenceProfiles	Troubleshooting	Read/Write

Permissions for VMware workloads

The IAM policies for VMware workloads provide the permissions that workload factory for VMware needs to manage resources and processes within your public cloud environment based on the operational mode you operate in.

Select your operational mode to view the required IAM policies:

IAM policies for VMware workloads

Read-only mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ssm:GetParametersByPath",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Read/Write mode

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath",
        "ssm:GetParameters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
```

```
        "Resource": "*"
      }
    ]
}
```

The following table provides details about the permissions for VMware workloads.

Table of permissions for VMware workloads

Purpose	Action	Where used	Mode
Attach security groups and modify rules for the provisioned nodes	ec2:AuthorizeSecurityGroupIngress	Deployment	Read/Write
Create EBS volumes	ec2:CreateVolume	Deployment	Read/Write
Tag custom values for FSx for NetApp ONTAP resources created by VMware workloads	fsx:TagResource	Deployment	Read/Write
Create and validate the CloudFormation template	cloudformation:CreateStack	Deployment	Read/Write
Manage tags and network security on created instances	ec2:CreateSecurityGroup	Deployment	Read/Write
Start the created instances	ec2:RunInstances	Deployment	Read/Write
Get EC2 instance details	ec2:DescribeInstances	Deployment	Read/Write
List images during the stack creation during deploy and rebuild operations	ec2:DescribeImages	Deployment	Read/Write
Get the VPCs in the selected environment to complete deployment form	ec2:DescribeVpcs	• Deployment • Inventory	• Read-only • Read/Write
Get the subnets in selected environment to complete deployment form	ec2:DescribeSubnets	• Deployment • Inventory	• Read-only • Read/Write
Get the security groups in selected environment to complete deployment form	ec2:DescribeSecurityGroups	Deployment	• Read-only • Read/Write
Get the availability zones in selected environment	ec2:DescribeAvailabilityZones	• Deployment • Inventory	• Read-only • Read/Write
Get the regions with Amazon FSx for NetApp ONTAP support	ec2:DescribeRegions	Deployment	• Read-only • Read/Write
Get KMS keys' aliases to be used for Amazon FSx for NetApp ONTAP encryption	kms:ListAliases	Deployment	• Read-only • Read/Write
Get KMS keys to be used for Amazon FSx for NetApp ONTAP encryption	kms:ListKeys	Deployment	• Read-only • Read/Write
Get KMS keys expiry details to be used for Amazon FSx for NetApp ONTAP encryption	kms:DescribeKey	Deployment	• Read-only • Read/Write

Purpose	Action	Where used	Mode
SSM based query is used to get the updated list of Amazon FSx for NetApp ONTAP supported regions	ssm:GetParametersByPath	Deployment	• Read-only • Read/Write
Create Amazon FSx for NetApp ONTAP resources required for provisioning	fsx:CreateFileSystem	Deployment	Read/Write
	fsx:CreateStorageVirtualMachine	Deployment	Read/Write
	fsx:CreateVolume	• Deployment • Management operations	Read/Write
Get Amazon FSx for NetApp ONTAP details	fsx:Describe*	• Deployment • Inventory • Management operations • Explore savings	Read/Write
	fsx:List*	• Deployment • Inventory	Read/Write
Get KMS key details and use for Amazon FSx for NetApp ONTAP encryption	kms:CreateGrant	Deployment	Read/Write
	kms:Describe*	Deployment	Read/Write
	kms:List*	Deployment	Read/Write
	kms:Decrypt	Deployment	Read/Write
	kms:GenerateDataKey	Deployment	Read/Write
List customer SNS topics and publish to WLMVMC backend SNS as well as customer SNS if selected	sns:Publish	Deployment	Read/Write
Used to fetch latest list of Amazon FSx for NetApp ONTAP supported AWS regions	ssm:Get*	• Deployment • Management operations	Read/Write
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	Read/Write

Purpose	Action	Where used	Mode
SSM Parameter store is used to save credentials of Amazon FSx for NetApp ONTAP	ssm:GetParameter	• Deployment • Management operations • Inventory	Read/Write
	ssm:PutParameters	• Deployment • Inventory	Read/Write
	ssm:PutParameter	• Deployment • Management operations	Read/Write
	ssm:DeleteParameters	• Deployment • Management operations	Read/Write

Change log

As permissions are added and removed, we'll note them in the sections below.

4 May 2025

The following permission is now available in *Read/Write* mode for GenAI: `qbusiness:ListApplications`.

The following permissions are now available in *Read-only* mode for Databases:

- `logs:GetLogEvents`
- `logs:DescribeLogGroups`

The following permission is now available in *Read/Write* mode for Databases: `logs:PutRetentionPolicy`.

2 April 2025

The following permission is now available in *Read-only* mode for Databases: `ssm:DescribeInstanceInformation`.

30 March 2025

GenAI workload permissions update

The following permissions are now available in *Read/Write mode* for GenAI:

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:createPolicy`
- `bedrock:ListInferenceProfiles`

The following permission has been removed from *Read/Write mode* for GenAI: `Bedrock:GetFoundationModel`.

iam:SimulatePrincipalPolicy permission update

The `iam:SimulatePrincipalPolicy` permission is part of all workload permission policies if you enable the automatic permissions check when adding additional AWS account credentials or adding a new workload capability from the workload factory console. The permission simulates workload operations and checks if you have the required AWS account permissions before deploying resources from workload factory. Enabling this check reduces the time and effort that you might need to clean up resources from failed operations and to add in missing permissions.

2 March 2025

The following permission is now available in *Read/Write* mode for GenAI: `bedrock:GetFoundationModel`.

3 February 2025

The following permission is now available in *Read-only* mode for Databases: `iam:SimulatePrincipalPolicy`.

Quick start for BlueXP 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-only* mode or *Read/Write* 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 BlueXP workload factory

BlueXP 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:

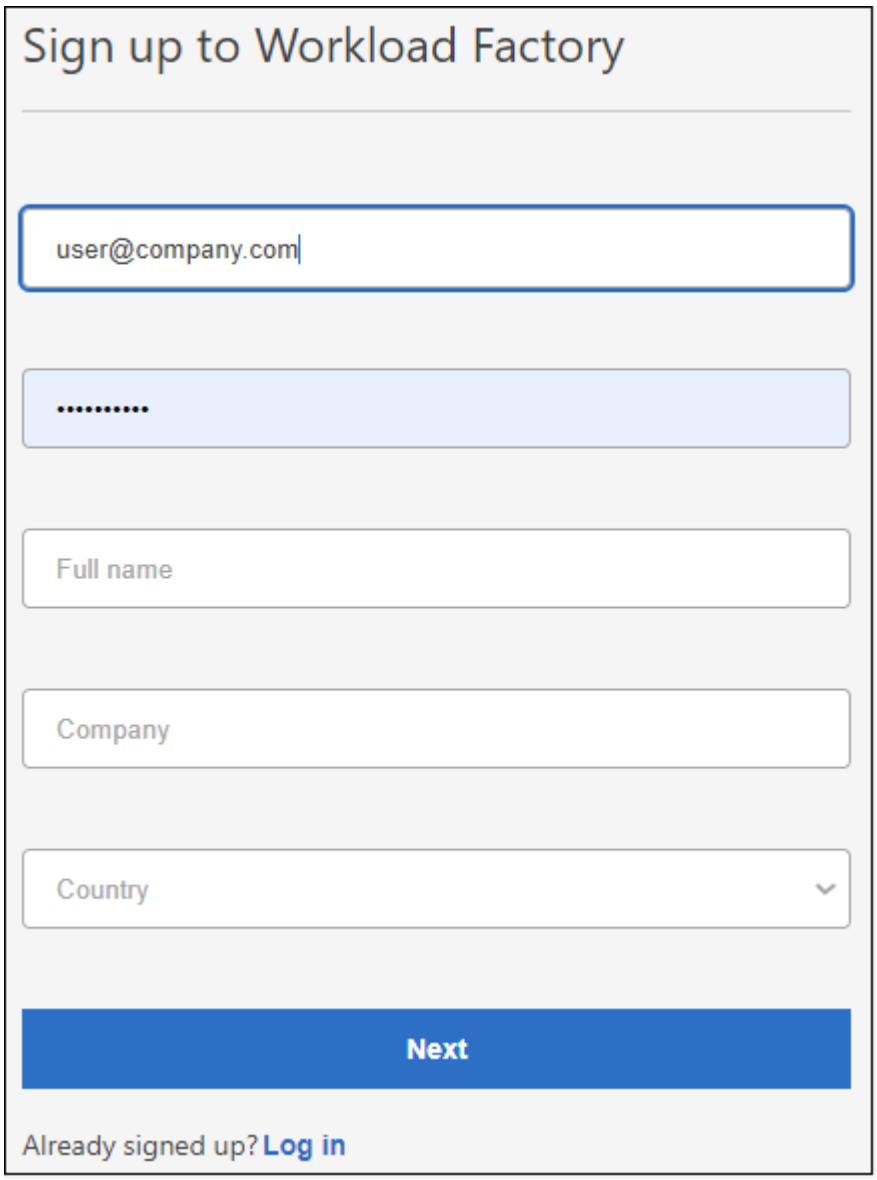
- Your existing NetApp Support Site (NSS) credentials
- A NetApp cloud login by specifying your email address and a password

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.

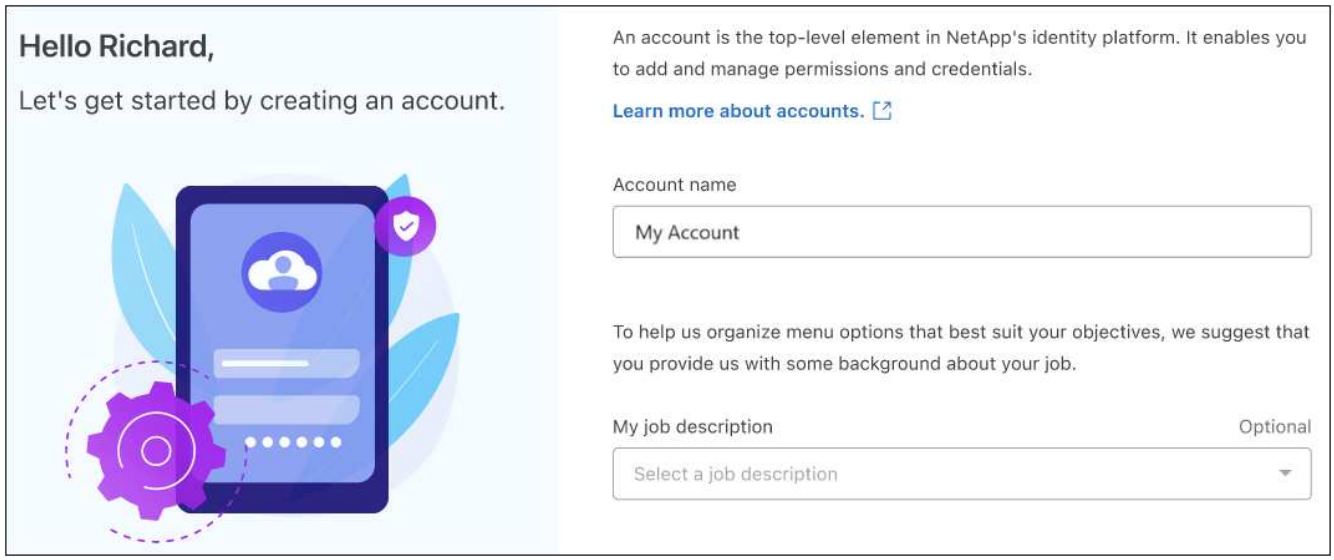
5. Enter the detailed information for your company and select **Sign up**.
6. Check your inbox for an email from NetApp that includes instructions to verify your email address.

   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-only* mode and *Read/Write* 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.

You can add AWS credentials to an account either from the workload factory console or from the BlueXP console.

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.

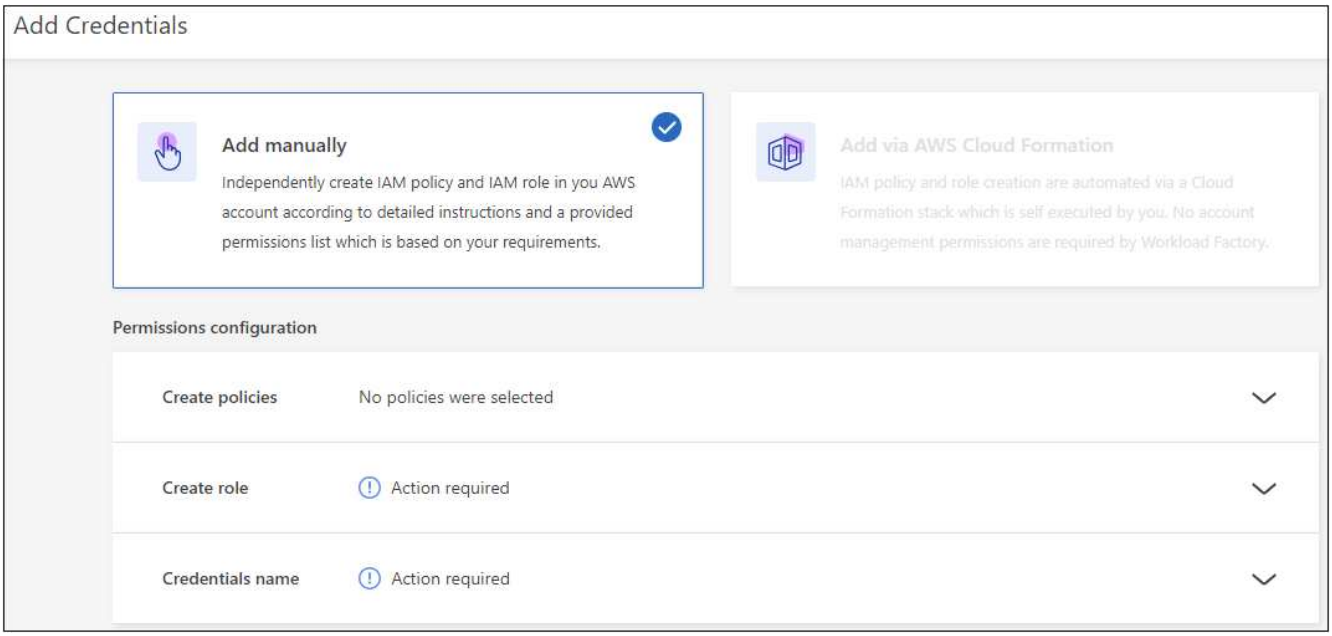
Before you begin

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

Steps

1. Log in to the workload factory console.
2. Select the **Account** icon, and select **Credentials**.

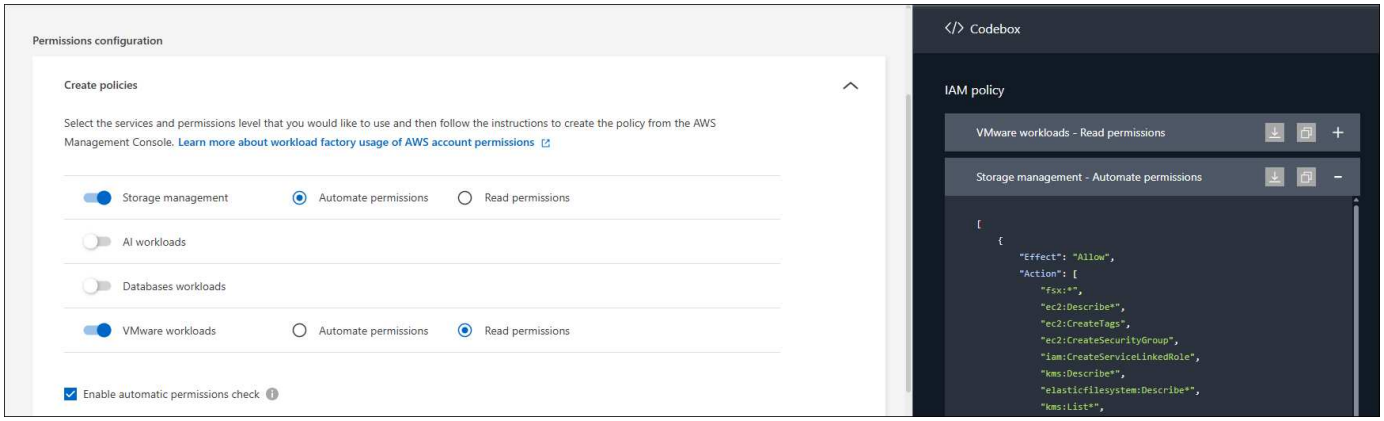
3. On the Credentials page, select **Add credentials**.
4. On the Add credentials page, select **Add manually** and then use the following steps to complete each section under *Permissions configuration*.



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

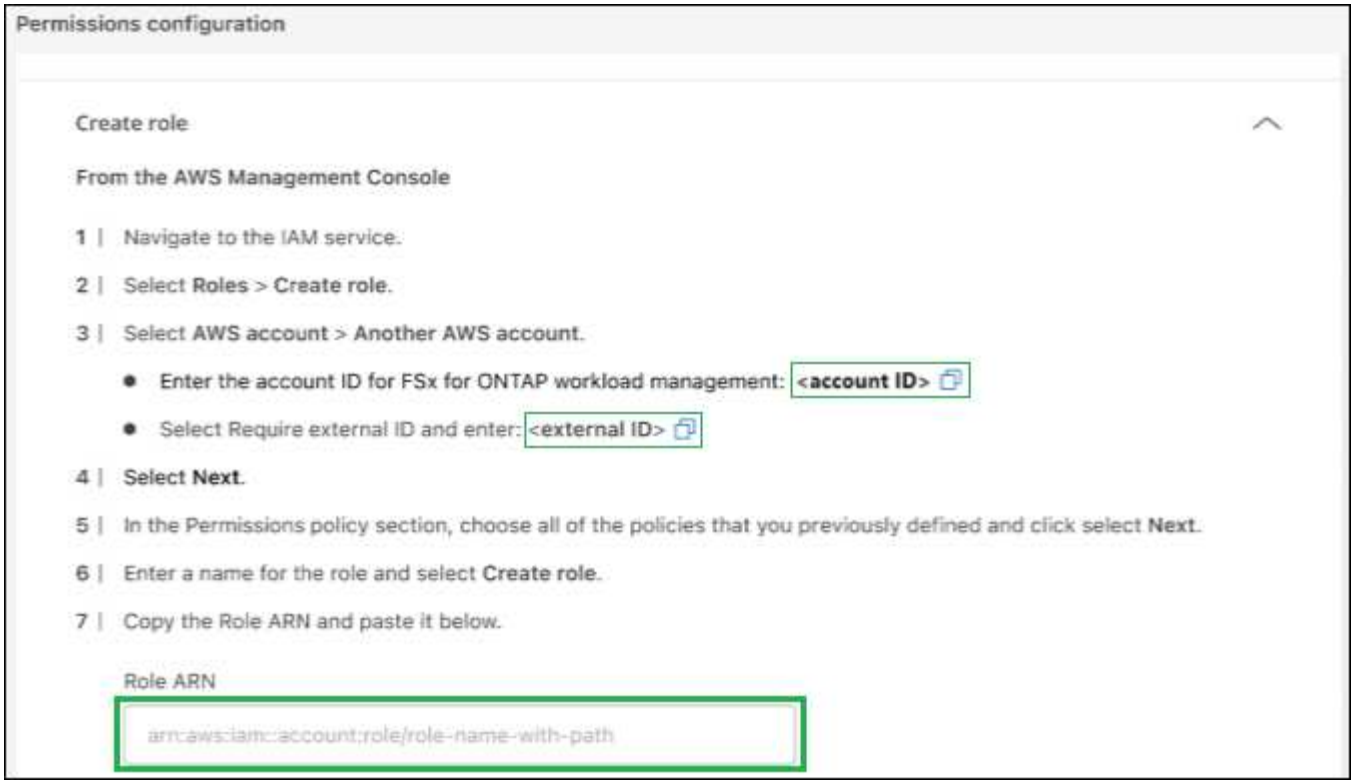
1. From the **Create policies** section, enable each of the workload capabilities that you want to include in these credentials.

   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 (Read-only, Read/Write, and so on), select the type of permissions that will be available with these credentials.
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 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 the **Credentials** page in 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 the **Credentials page** in 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.

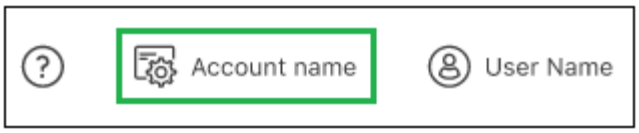
Before you begin

- 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:

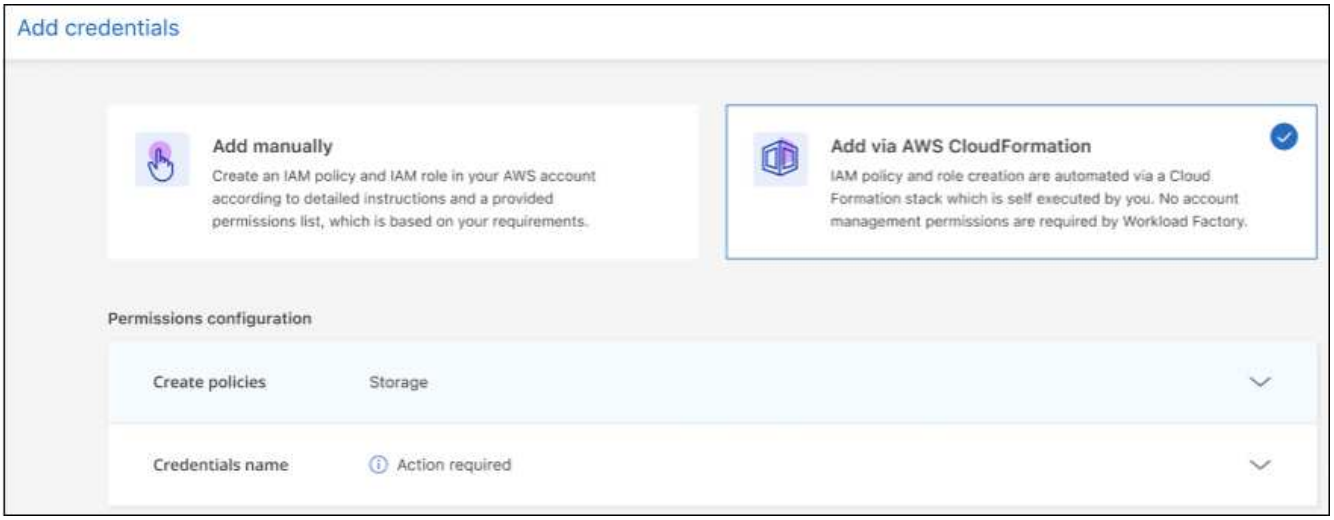
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "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. Log in to the workload factory console.
2. Select the **Account** icon, and select **Credentials**.



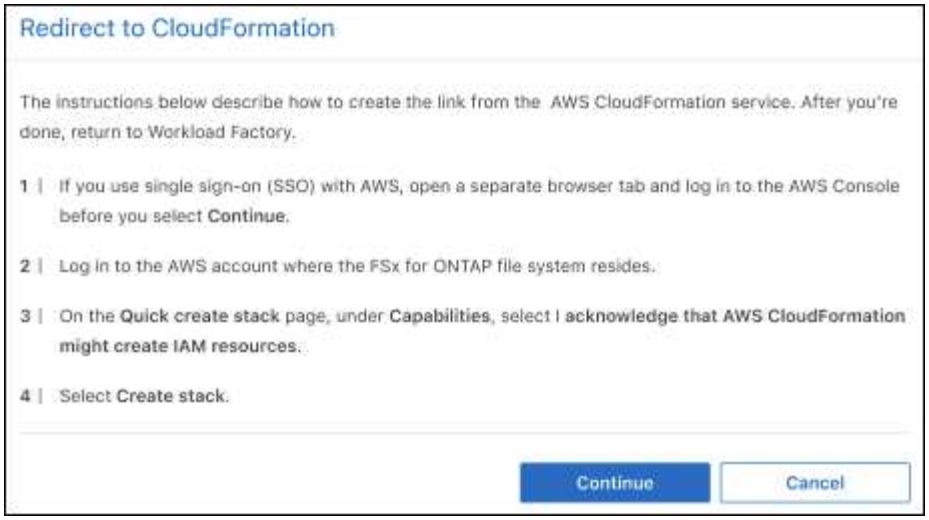
3. On the Credentials page, select **Add credentials**.
4. Select **Add via AWS CloudFormation**.



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 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 with BlueXP workload factory

Now that you've logged in and set up BlueXP 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.

Administer workload factory

Log in to BlueXP workload factory

After you sign up to BlueXP workload factory, you can log in at any time from the web-based console to start managing your workloads and FSx for ONTAP file systems.

About this task

You can log in to the workload factory web-based console using one of the following options:

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

Steps

1. Open a web browser and go to the workload factory console.
2. On the **Log in** page, enter the email address that's associated with your login.
3. Depending on the authentication method associated with your login, you'll be prompted to enter your credentials:
   - NetApp cloud credentials: Enter your password
   - Federated user: Enter your federated identity credentials
   - NetApp Support Site account: Enter your NetApp Support Site credentials
4. Select **Log in**.

   If you have successfully logged in in the past, you'll see the workload factory home page and you'll be using the default account.

   If this is the first time that you've logged in, you'll be directed to the **Account** page.

   - If you are a member of a single account, select **Continue**.
   - If you are a member of multiple accounts, select the account and select **Continue**.

Result

You're now logged in and can start using workload factory to manage FSx for ONTAP file systems and your workloads.

Manage service accounts

Create service accounts to act as machine users that automate infrastructure operations. You can revoke or change access to service accounts at any time.

About this task

Service accounts are a multi-tenancy functionality provided by BlueXP. Account admins create service accounts, control access, and delete service accounts. You can manage service accounts in the BlueXP console or in the BlueXP workload factory console.

Unlike managing service accounts in BlueXP where you can recreate a client secret, workload factory supports only creation and deletion of service accounts. If you want to recreate a client secret for a specific service

account in the BlueXP workload factory console, you'll need to delete the service account, and then create a new one.

Service accounts use a client ID and a secret for authentication rather than a password. Client IDs and secrets are fixed until the account admin decides to change them. To use a service account, you'll need the client ID and secret to generate the access token or you won't gain access. Keep in mind that access tokens are short-lived and can only be used for several hours.

Before you begin

Decide if you want to create a service account in the BlueXP console or in the BlueXP workload factory console. There are slight differences. The following instructions describe how to manage service accounts in the BlueXP workload factory console.

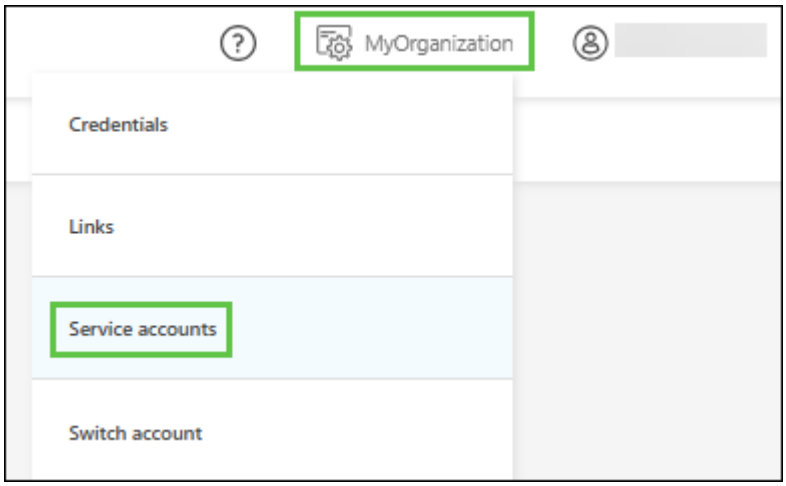
To manage service accounts in BlueXP, learn about BlueXP identity and access management and learn how to add BlueXP IAM members and manage their permissions.

Create a service account

When you create a service account, BlueXP workload factory enables you to copy or download a client ID and client secret for the service account. This key pair is used for authentication with BlueXP workload factory.

Steps

1. In the workload factory console, select the **Account** icon, and select **Service accounts**.



2. On the **Service accounts** page, select **Create service account**.
3. In the Create service account dialog, enter a name for the service account in the **Service account name** field.

   The **role** is preselected as **account admin**.

4. Select **Continue**.
5. Copy or download the client ID and client secret.

   The client secret is visible only once and is not stored anywhere by workload factory. Copy or download the secret and store it safely.

6. Optionally, you can get an access token for Auth0 management API by executing a client credentials exchange. The curl example shows how can you take the client ID and secret and use an API to generate the access token which are time-limited. The token provides several hours of access to the BlueXP

workload factory APIs.

7. Select **Close**.

The new service account is created and listed on the Service accounts page.

Delete a service account

Delete a service account if you no longer need to use it.

Steps

1. In the Workload Factory console, select the **Account** icon, and select **Service accounts**.
2. On the **Service accounts** page, select the three-dot menu and then select **Delete**.
3. In the Delete service account dialog, enter **delete** in the text box.
4. Select **Delete** to confirm deletion.

The service account is deleted.

Automate tasks using Codebox

Learn about codebox automation

Codebox is an Infrastructure as Code (IaC) co-pilot that helps developers and DevOps generate the code needed to execute any operation supported by workload factory. Codebox is aligned with the workload factory operation modes (Basic, Read-only, and Read/Write) and it sets a clear path for execution readiness as well as providing an automation catalog for quick future reuse.

Codebox capabilities

Codebox provides two key IaC capabilities:

- *Codebox Viewer* shows the IaC that is generated by a specific job flow operation by matching entries and selections from the graphical wizard or from the conversational chat interface. While Codebox Viewer supports color coding for easy navigation and analysis, it does not allow editing—only copying or saving code to the Automation Catalog.
- *Codebox Automation Catalog* shows all saved IaC jobs, allowing you to easily reference them for future use. Automation catalog jobs are saved as templates and shown in context of the resources that apply to them.

Additionally, when setting up workload factory credentials, Codebox dynamically displays the AWS permissions that are needed to create IAM policies. The permissions are provided for each workload factory capability that you plan to use (databases, AI, FSx for ONTAP, and so on), and they are customized based on whether the users of the policy will get Read-only permissions or full Read/Write permissions. You just copy the permissions from Codebox and then paste them in the AWS Management Console so that workload factory has the correct permissions to manage your workloads.

Supported code formats

The supported code formats include:

- Workload factory REST APIs
- AWS CLI
- AWS CloudFormation

Learn how to use Codebox.

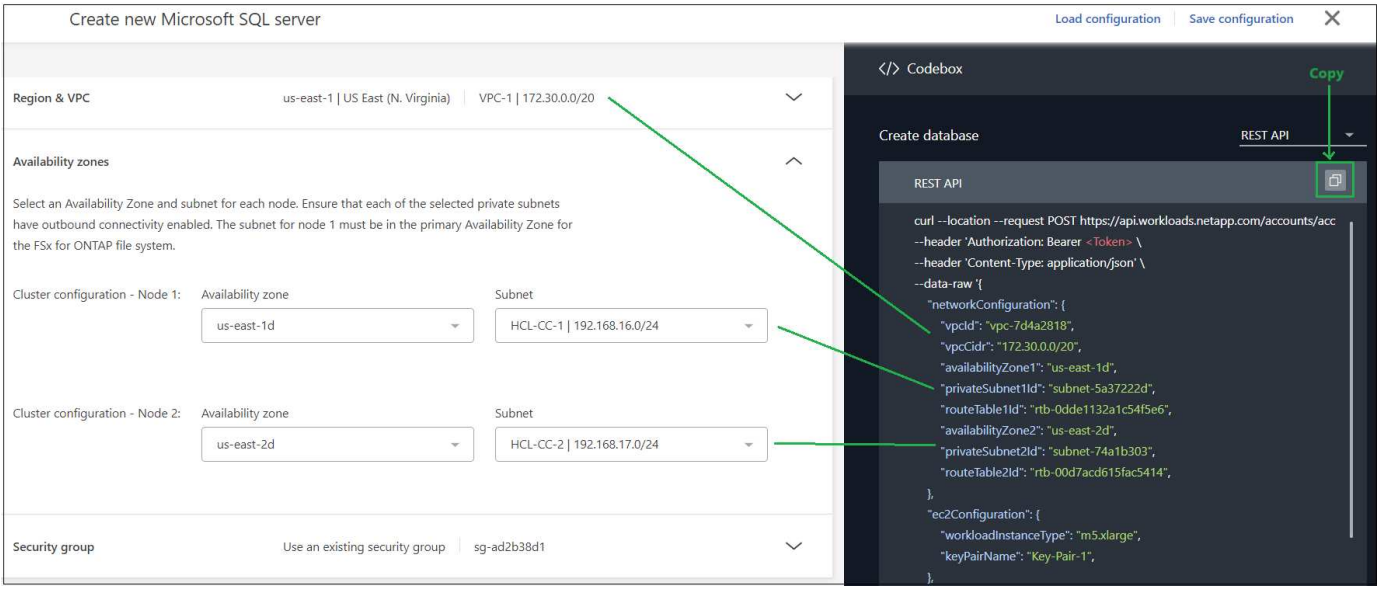
Use Codebox for automation in BlueXP workload factory

You can use Codebox to generate the code needed to execute any operation supported by BlueXP workload factory. You can generate code that can be consumed and run using workload factory REST APIs, the AWS CLI, and AWS CloudFormation.

Codebox is aligned with the workload factory operation modes (Basic, Read-only, and Read/Write) by populating the appropriate data in the code based on the AWS permissions provided in the workload factory account for each user. The code can be used like a template where you can fill in missing information (for example, credentials) or customize certain data before running the code.

How to use Codebox

As you enter values in the workload factory UI wizards, you can see the data update in Codebox as you complete each field. When you complete the wizard, but before you select the **Create** button at the bottom of the page, select to copy in Codebox to capture the code required to build your configuration. For example, this screenshot from creating a new Microsoft SQL Server shows the wizard entries for VPC and availability zones and the equivalent entries in Codebox for a REST API implementation.



With some code formats you can also select the Download button to save the code in a file that you can bring to another system. If required, you can edit the code after it has been downloaded so that you can adapt it to other AWS accounts.

Use CloudFormation code from Codebox

You can copy the CloudFormation code generated from Codebox and then launch the Amazon Web Services CloudFormation stack in your AWS account. CloudFormation will perform the actions that you defined in the workload factory UI.

The steps to use the CLoudFormation code might be different depending on whether you are deploying an FSx for ONTAP file system, creating account credentials, or performing other workload factory actions.

Note that the code within a CloudFormation-generated YAML file expires after 7 days for security reasons.

Before you begin

- You'll need to have credentials to log in to your AWS account.
- You'll need to have the following user permissions to use 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. After you have used the UI to define the operation that you want to perform, copy the code in the Codebox.
2. Select **Redirect to CloudFormation** and the Redirect to CloudFormation page is displayed.
3. Open another browser window and log in to the AWS Management Console.
4. Select **Continue** from the Redirect to CloudFormation page.

5. Log in to the AWS account where the code should be run.
6. On the Quick create stack page, under Capabilities, select **I acknowledge that AWS CloudFormation might …**.
7. Select **Create stack**.
8. Monitor the progress from AWS or from workload factory.

Use REST API code from Codebox

You can use the workload factory REST APIs generated from Codebox to deploy and manage your FSx for ONTAP file systems and other AWS resources.

You can run the APIs from any host that supports curl and that has internet connectivity.

Note that the authentication tokens are hidden in Codebox, but they are populated when you copy and paste the API call.

Steps

1. After you have used the UI to define the operation that you want to perform, copy the API code in the Codebox.
2. Paste the code and run it on your host system.

Use AWS CLI code from Codebox

You can use the Amazon Web Services CLI generated from Codebox to deploy and manage your FSx for ONTAP file systems and other AWS resources.

Steps

1. After you have used the UI to define the operation that you want to perform, copy the AWS CLI in the Codebox.
2. Open another browser window and log in to the AWS Management Console.
3. Paste the code and run it.

Use Terraform from Codebox

You can use Terraform to deploy and manage your FSx for ONTAP file systems and other AWS resources.

Before you begin

- You'll need a system where Terraform is installed (Windows/Mac/Linux).
- You'll need to have credentials to log in to your AWS account.

Steps

1. After you have used the user interface to define the operation that you want to perform, download the Terraform code from the Codebox.
2. Copy the downloaded script archive to the system where Terraform is installed.
3. Extract the zip file and follow the steps in the README.md file.

Use CloudShell in BlueXP workload factory

Open CloudShell to execute AWS or ONTAP CLI commands from anywhere in the BlueXP workload factory user interface.

About this task

CloudShell allows you to execute AWS CLI commands or ONTAP CLI commands in a shell-like environment from within the BlueXP workload factory user interface. It simulates terminal sessions in the browser, providing terminal features and proxying messages through workload factory's backend. It allows you to use the AWS credentials and ONTAP credentials that you have provided in your BlueXP account.

CloudShell features include:

- Multiple CloudShell sessions: deploy multiple CloudShell sessions at one time to issue several sequences of commands in parallel,
- Multiple views: split CloudShell tab sessions so you can view two or more tabs horizontally or vertically at the same time
- Session renaming: rename sessions as needed
- Last session content persistence: re-open the last session if you close it by mistake
- Settings preferences: change the font size and output type
- AI-generated error responses for ONTAP CLI commands
- Autocomplete support: start typing a command and use the **Tab** key to view available options

CloudShell commands

Within the CloudShell GUI interface, you can enter `help` to view available CloudShell commands. After you issue the `help` command, the following reference appears.

Description

NetApp CloudShell is a GUI interface built into BlueXP workload factory enables you to execute AWS CLI commands or ONTAP CLI commands in a shell-like environment. It simulates terminal sessions in the browser, providing terminal features and proxying messages through the backend in workload factory. It enables you to use the AWS credentials and ONTAP credentials that you have provided in your BlueXP Account.

Available commands

- `clear`
- `help`
- `[--fsx <fsxId>] <ontap-command> [parameters]`
- `aws <aws-command> <aws-sub-command> [parameters]`

Context

Each terminal session runs in a specific context: credentials, region, and optionally FSx for ONTAP file system.

All AWS commands execute in the provided context. AWS commands will only succeed if the provided credentials have permissions in the specified region.

You can specify ONTAP commands with an optional `fsxId`. If you provide an `fsxId` with an individual ONTAP command, then this ID overrides the ID in the context. If the terminal session doesn't have an FSx for ONTAP file system ID context, then you must provide `fsxId` with each ONTAP command.

To update different context specifics, do the following:
* To change credentials: "using credentials <credentialId>"
* To change region: "using region <regionCode>"
* To change FSx for ONTAP file system: "using fsx <fileSystemId>"

Showing Items

- To show available credentials: "show credentials"
- To show available regions: "show regions"
- To show command history: "show history"

Variables

The following are examples of setting and using variables. If a variable value contains spaces, you should set it inside quotes.

- To set a variable: $<variable> = <value>
- To use a variable: $<variable>
- Example setting a variable: $svm1 = svm123
- Example using a variable: --fsx FileSystem-1 volumes show --vserver $svm1
- Example setting a variable with string value $comment1 = "A comment with spaces"

Operators

Shell operators such as pipe `|`, background execution `&`, and redirection `>` aren't supported. Command execution fails if you include these operators.

Before you begin

CloudShell works in the context of your AWS credentials. To use CloudShell, you must provide at least one AWS credential.

CloudShell is available for you to execute any AWS or ONTAP CLI command. However, if you want to work within the context of an FSx for ONTAP file system, make sure you issue the following command: `using fsx <file-system-name>`.

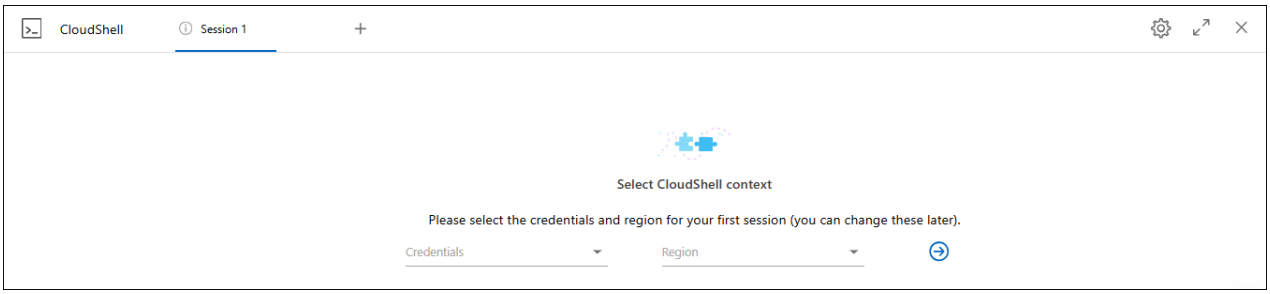
Deploy CloudShell

You can deploy CloudShell from anywhere in the BlueXP workload factory console. You can also deploy CloudShell from Storage from within an FSx for ONTAP file system.

Deploy from workload factory console

Steps

1. Log in using one of the console experiences.
2. Open CloudShell  from the top navigation bar.
3. In the CloudShell window, select credentials and region for the CloudShell session and then select the arrow to continue.



4. Enter `help` to view available CloudShell commands and instructions or refer to the following CLI reference documents for available commands:
   - AWS CLI reference: For commands related to FSx for ONTAP, select **fsx**.
   - ONTAP CLI reference
5. Issue commands within the CloudShell session.

   If an error occurs after issuing an ONTAP CLI command, select the light bulb icon to get a brief AI-generated error response with a description of the failure, the cause of the failure, and a detailed resolution. Select **Read more** for more details.

Deploy from Storage

Steps

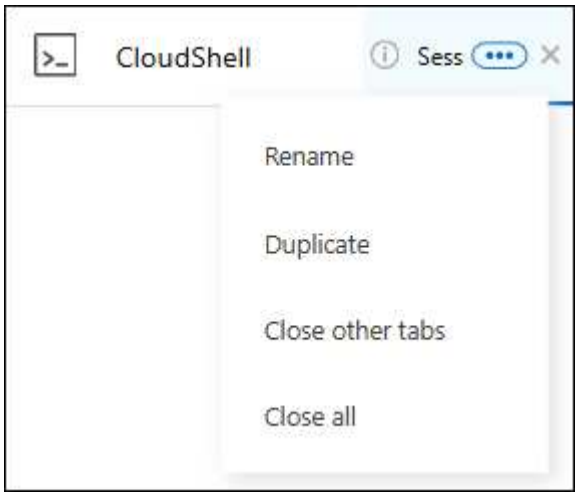
1. Log in using one of the console experiences.
2. In **Storage**, select **Go to storage inventory**.
3. In the **FSx for ONTAP** tab, select the three-dot menu of the file system and then select **Open CloudShell**.

   A CloudShell session opens in the context of the selected file system.

4. Enter `help` to view available CloudShell commands and instructions or refer to the following CLI reference documents for available commands:
   - AWS CLI reference: For commands related to FSx for ONTAP, select **fsx**.
   - ONTAP CLI reference
5. Issue commands within the CloudShell session.

   If an error occurs after issuing an ONTAP CLI command, select the light bulb icon to get a brief AI-generated error response with a description of the failure, the cause of the failure, and a detailed resolution. Select **Read more** for more details.

The CloudShell tasks shown in this screenshot can be completed by selecting the three-dot menu of an open CloudShell session tab. The instructions for each of these tasks follows.



Rename a CloudShell session tab

You can rename a CloudShell session tab to help you identify the session.

Steps

1. Select the three-dot menu of the CloudShell session tab.
2. Select **Rename**.
3. Enter a new name for the session tab and then click outside the tab name to set the new name.

Result

The new name appears in the CloudShell session tab.

Duplicate CloudShell session tab

You can duplicate a CloudShell session tab to create a new session with the same name, credentials, and region. The code from the original tab isn't duplicated in the duplicated tab.

Steps

1. Select the three-dot menu of the CloudShell session tab.
2. Select **Duplicate**.

Result

The new tab appears with the same name as the original tab.

Close CloudShell session tabs

You can close CloudShell tabs one at a time, close other tabs you're not working on, or close all tabs at once.

Steps

1. Select the three-dot menu of the CloudShell session tab.
2. Select one of the following:
   - Select "X" in the CloudShell tab window to close one tab at a time.

- Select **Close other tabs** to close all other tabs that are open except the one you're working on.
- Select **Close all tabs** to close all tabs.

Result

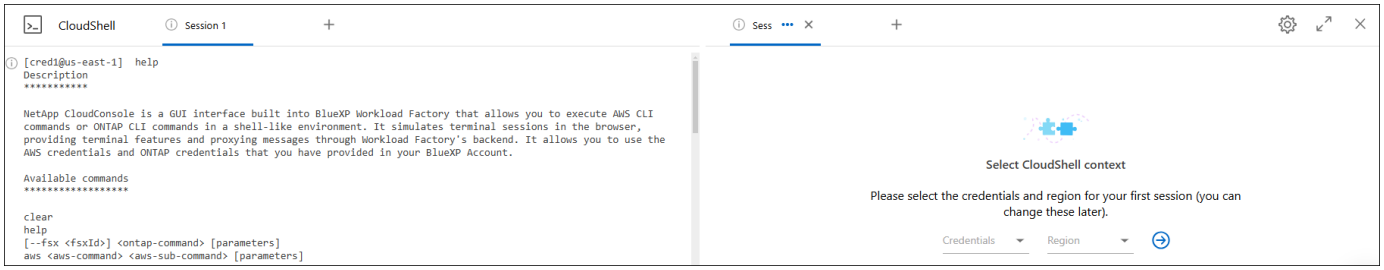
The selected CloudShell session tabs close.

Split CloudShell session tabs

You can split CloudShell session tabs to view two or more tabs at the same time.

Step

Drag and drop CloudShell session tabs to the top, bottom, left, or right of the CloudShell window to split the view.



Re-open your last CloudShell session

If by accident you close your CloudShell session, you can re-open it.

Step

Select the CloudShell icon  from the top navigation bar.

Result

The latest CloudShell sessions open.

Update settings for a CloudShell session

You can update font and output type settings for CloudShell sessions.

Steps

1. Deploy a CloudShell session.
2. In the CloudShell tab, select the settings icon.

   The settings dialog appears.

3. Update font size and output type as needed.

   Enriched output applies to JSON objects and table formatting. All other output appears as plain text.

4. Select **Apply**.

Result

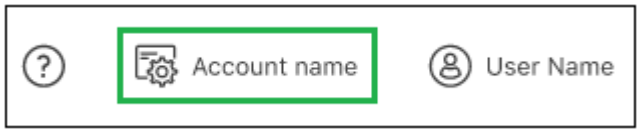
The CloudShell settings are updated.

Remove credentials from BlueXP workload factory

If you no longer need a set of credentials, you can delete them from workload factory. You can only delete credentials that aren't associated with an FSx for ONTAP file system.

Steps

1. Log in using one of the console experiences.
2. Navigate to the **Credentials** page.
   a. In the workload factory console, select the **Account** icon, and select **Credentials**.



   b. In the BlueXP console, select the **Settings** icon, and select **Credentials**.
3. On the **Credentials** page, select the action menu for a set of credentials and then select **Remove**.
4. Select **Remove** to confirm.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP workload factory and its storage solutions and services. You must register for support from the BlueXP console, which is a separate web-based console from workload factory.

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 workload factory documentation for that product.

Amazon FSx for ONTAP

Support registration overview

Registering your account ID support subscription (your 20 digit 960xxxxxxxx serial number located on the Support Resources page in BlueXP) serves as your single support subscription ID. Each BlueXP account-level support subscription must be registered.

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

Register your account for NetApp support

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

Existing customer with an NSS account

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

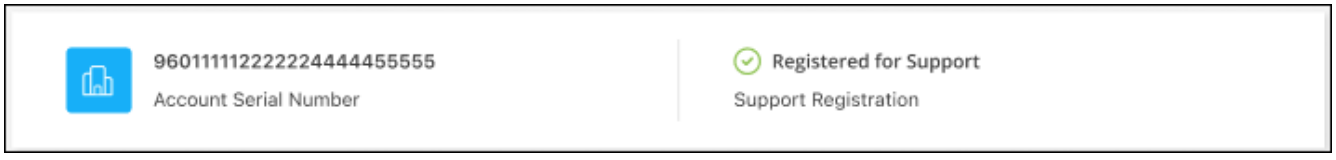
Steps

1. In the upper right of the workload factory console, select **Help > Support**.

   Selecting this option opens the BlueXP console a new browser tab and loads the Support dashboard.

2. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
3. Select **User Credentials**.
4. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
5. To confirm that the registration process was successful, select the Help icon, and select **Support**.

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



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

Existing customer but no NSS account

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

Steps

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

Brand new to NetApp

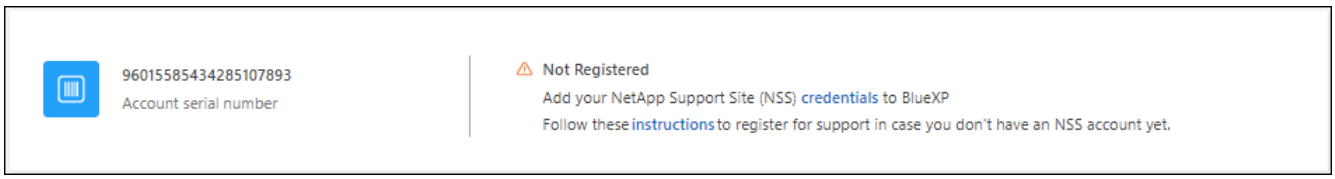
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the workload factory console, select **Help > Support**.

   Selecting this option opens the BlueXP console a new browser tab and loads the Support dashboard.

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



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

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

7. Confirm the action from within the email.

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

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.

b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

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

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

Get help

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

Get support for FSx for ONTAP

For technical support related to FSx for ONTAP, its infrastructure, or any solution using the service, refer to "Getting help" in the workload factory documentation for that product.

Amazon FSx for ONTAP

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

Use self-support options

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

- Documentation

  The workload factory documentation that you're currently viewing.

- Knowledge base

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

- Communities

  Join the workload factory 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 register for support. associate your NetApp Support Site credentials with your workload factory login. Learn how to register for support.

Steps

1. In the upper right of the workload factory console, select **Help > Support**.

   Selecting this option opens the BlueXP console a new browser tab and loads the Support dashboard.

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.

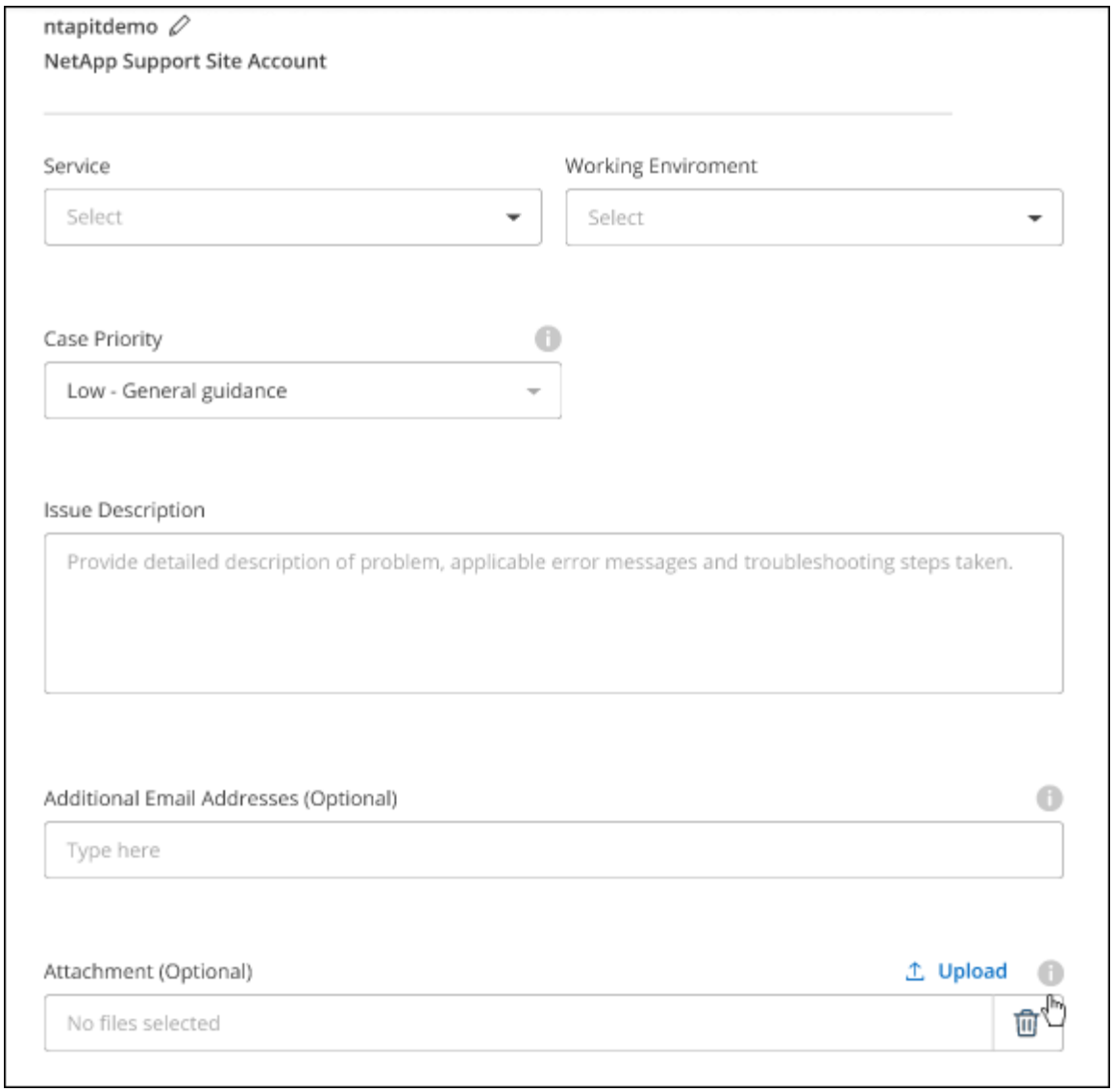
   b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

      - **Service**: Select **Workload Factory**.
      - **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.



After you finish

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

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

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

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

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

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

Manage your support cases (Preview)

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

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

Note the following:

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

  The results in the table reflect the cases related to the view that you selected.
- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

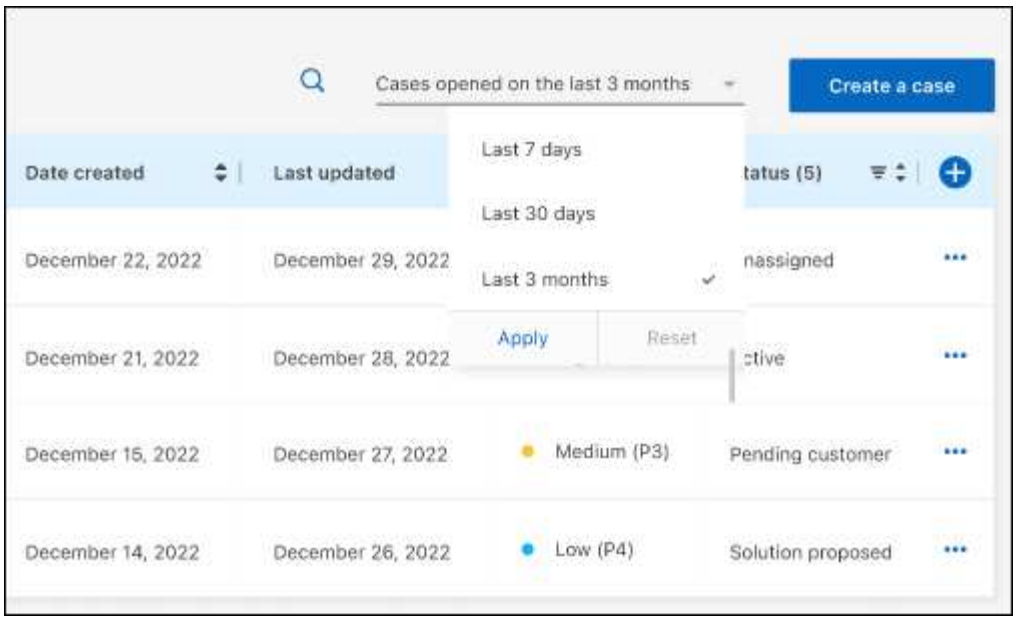
  View the steps below for more details.
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

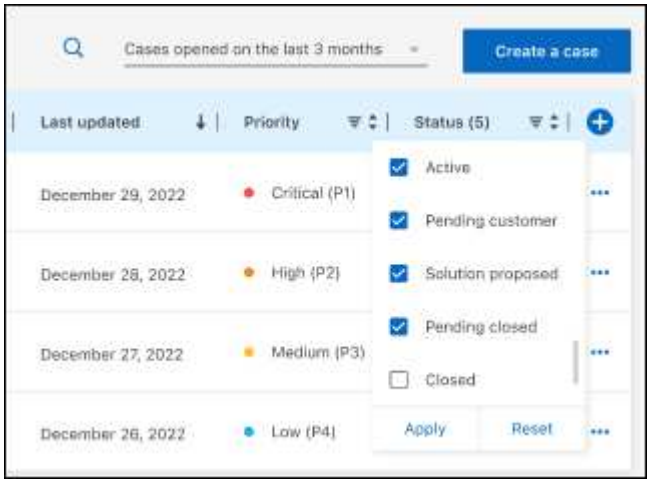
1. In the upper right of the workload factory console, select **Help > Support**.

   Selecting this option opens the BlueXP console a new browser tab and loads the Support dashboard.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

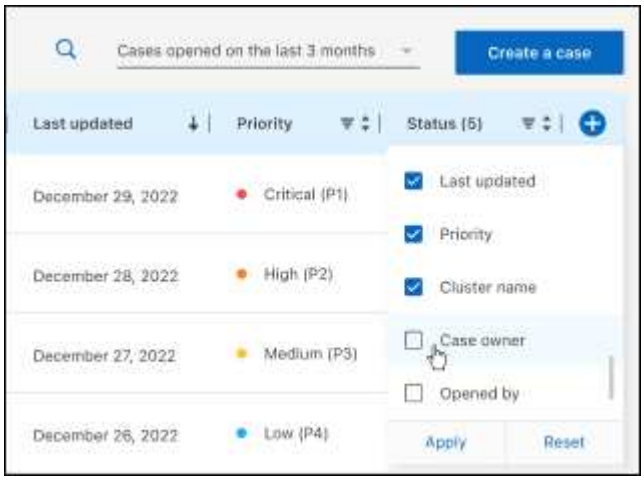
   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.
3. Optionally modify the information that displays in the table:
   - Under **Organization's cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.



- 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.

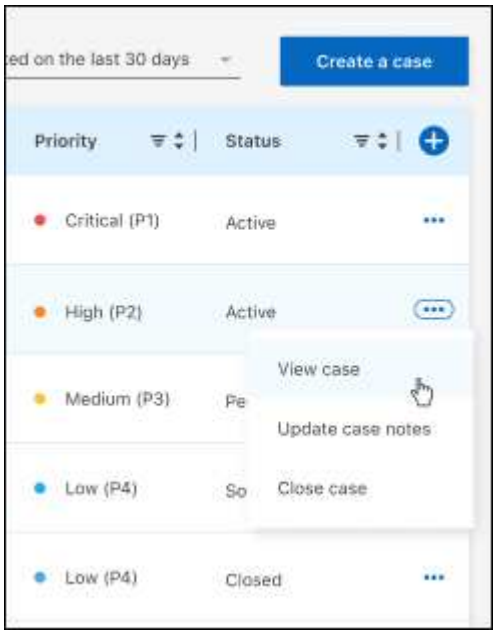


4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **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 for BlueXP workload factory

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.

BlueXP workload factory