



NetApp Workload Factory setup and administration documentation

Setup and administration

NetApp
February 02, 2026

Table of Contents

NetApp Workload Factory setup and administration documentation	1
Release notes	2
What's new with NetApp Workload Factory administration features	2
01 February 2026	2
04 January 2026	3
27 November 2025	3
06 October 2025	3
05 October 2025	3
09 September 2025	3
29 June 2025	4
04 May 2025	4
30 March 2025	4
02 February 2025	5
22 January 2025	5
5 January 2025	5
11 November 2024	5
1 September 2024	5
4 August 2024	7
7 July 2024	7
Get started	8
Learn the basics	8
Learn about NetApp Workload Factory	8
Console experiences	12
Permissions for NetApp Workload Factory	13
Quick start for NetApp Workload Factory	64
Sign up to NetApp Workload Factory	64
Sign up to Workload Factory	65
Invite others to join an account in Workload Factory	67
Add AWS credentials to Workload Factory	67
Overview	67
AWS credentials	68
Add credentials to an account manually	68
Add credentials to an account using CloudFormation	71
Optimize workloads with NetApp Workload Factory	74
Administer Workload Factory	75
Log in to NetApp Workload Factory	75
Manage service accounts	75
Create a service account	76
Delete a service account	77
Build and operate well-architected workloads	77
How it works	77
Why it matters	78
Get started with Workload Factory to detect and correct misconfigurations	78

Best practices and recommendations for storage workloads	78
Best practices and recommendations for database workloads	80
Best practices and recommendations for EVS workloads	84
Related information	85
Configure NetApp Workload Factory notifications	85
Notification types and messages	85
Configure Workload Factory notifications	87
Subscribe to the Amazon SNS topic	88
Filter notifications	88
Automate tasks using Codebox	90
Learn about codebox automation	90
Use Codebox for automation in NetApp Workload Factory	91
Use CloudShell in NetApp Workload Factory	94
About this task	94
CloudShell commands	95
Before you begin	96
Deploy CloudShell	96
Rename a CloudShell session tab	98
Duplicate CloudShell session tab	98
Close CloudShell session tabs	99
Split CloudShell session tabs	99
Update settings for a CloudShell session	99
Remove credentials from NetApp Workload Factory	100
Knowledge and support	101
Register for support	101
Support registration overview	101
Register your account for NetApp support	101
Get help	103
Get support for FSx for ONTAP	103
Use self-support options	103
Create a case with NetApp support	103
Manage your support cases (Preview)	106
Legal notices for NetApp Workload Factory	109
Copyright	109
Trademarks	109
Patents	109
Privacy policy	109
Open source	109

NetApp Workload Factory setup and administration documentation

Release notes

What's new with NetApp Workload Factory administration features

Learn what's new with Workload Factory administration features: cloud provider credentials, Codebox enhancements, and more.

01 February 2026

Well-architected updates

NetApp Workload Factory includes the well-architected assessment for Elastic VMware Service (EVS) workloads, and adds new configurations for Storage and Database workloads.

- **VMware workloads**

NetApp Workload Factory provides best practices and recommendations for operating well-architected Amazon Elastic VMware Service (EVS) workloads.

[Implement well-architected EVS configurations](#)

- **Storage workloads**

Several new configurations have been added to well-architected feature in the Storage workload so that you have more insight into storage performance and costs.

- Storage VM logical reporting
- Optimize cache volume size
- Orphaned block devices

[Implement well-architected file system configurations for Storage workloads](#)

- **Database workloads**

Workload Factory for Databases includes new storage configuration for Oracle for enabling and setting up Direct NFS (dNFS) to improve I/O performance and decrease the load on the host and the storage system.

- dNFS enablement
- dNFS consistent IP resolution
- dNFS configuration file
- dNFS nosharecache

[Implement well-architected database workloads](#)

New permissions for Storage

New permissions have been added to the Storage workload for enhancements to managing S3 access points.

[Permissions reference change log](#)

04 January 2026

Ask me AI assistant home page integration

The Workload Factory console home page embeds the Ask me AI assistant, enabling you to ask questions about your own storage estate, get personalized insights directly from your environment, and refer to previous conversations. You can interact with Ask me to understand your workloads, troubleshoot issues, and learn more about Workload Factory — all without leaving the console.

27 November 2025

Permissions update for Storage

The FSx for ONTAP EMS events analyzer uses the following Amazon Bedrock permissions in the *operations and remediation* permission policy to fetch events data for the Storage workload.

- bedrock:ListInferenceProfiles
- bedrock:GetInferenceProfile
- bedrock:InvokeModelWithResponseStream
- bedrock:InvokeModel

[Permissions reference change log](#)

06 October 2025

BlueXP workload factory now NetApp Workload Factory

BlueXP has been renamed and redesigned to better reflect the role it has in managing your data infrastructure. As a result, BlueXP workload factory has been renamed to NetApp Workload Factory.

Ask Me integration with MCP

Ask Me, Workload Factory's AI assistant, is integrated with the Model Context Protocol (MCP). Using MCP, Ask Me securely interfaces with external environments and queries API tools to deliver responses tailored to your specific storage environment.

05 October 2025

New notification for Storage

The NetApp Workload Factory notification service includes the notification for well-architected issues for Storage.

[Notifications for NetApp Workload Factory](#)

09 September 2025

New notification for Storage

The BlueXP workload factory notification service includes the notification for automatic capacity management for Storage.

29 June 2025

Permissions update for Databases

The following permission is now available in *read-only* mode for Databases: `cloudwatch:GetMetricData`.

[Permissions reference change log](#)

BlueXP workload factory notification service support

The BlueXP workload factory notification service enables workload factory to send notifications to the BlueXP alerts service or to an Amazon SNS topic. Notifications sent to BlueXP alerts appear in the BlueXP alerts panel. When workload factory publishes notifications to an Amazon SNS topic, subscribers to the topic (such as people or other applications) receive the notifications at the endpoints configured for the topic (such as email or SMS messages).

[Configure BlueXP workload factory notifications](#)

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

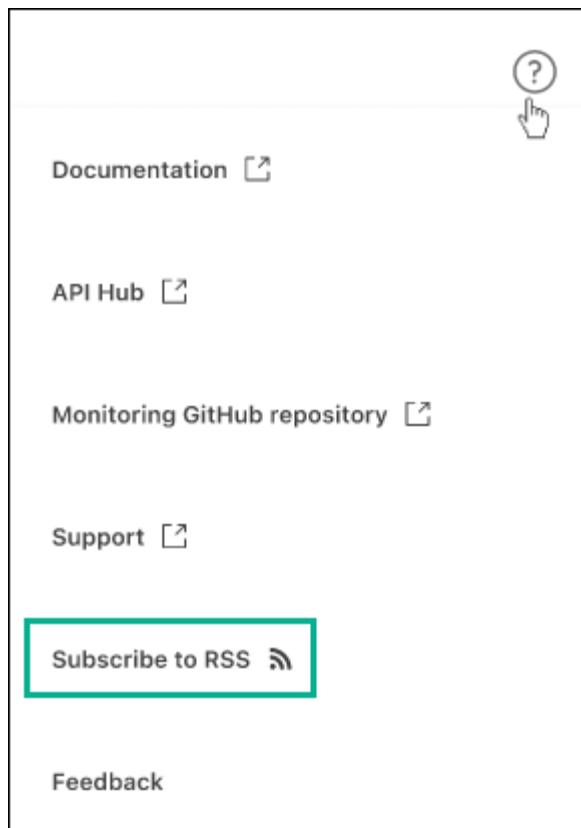
You now have the ability to use workload factory from the [BlueXP console](#). The BlueXP console experience provides the same functionality as the workload factory console.

[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.

The screenshot shows the 'Permissions configuration' section. It has a heading 'Create policies' and a sub-instruction: 'Select the services and permissions level that you would like to use and then follow the instructions to create the policy from the AWS Management Console.' Below this are four rows of workload and permission settings:

Workload	Storage management	Automate permissions	Read permissions
AI workloads	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Databases workloads	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>
VMware workloads	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>

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 NetApp Workload Factory

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

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

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

Features

The Workload Factory platform provides the following major capabilities.

Flexible and low cost storage

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

Migrate on-premises vSphere environments to VMware Cloud on AWS

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

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 organization's 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 NetApp 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.

Ask Me AI assistant

Ask the AI assistant questions about managing and operating FSx for ONTAP file systems. Using the Model Context Protocol (MCP), Ask Me securely interfaces with external environments and queries API tools to deliver responses tailored to your specific storage environment.

Supported cloud providers

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

Security

Security for NetApp Workload Factory is a top priority for NetApp. All workloads in Workload Factory run atop Amazon FSx for NetApp ONTAP. In addition to all [AWS security features](#), NetApp Workload Factory has received [SOC2 Type 1 compliance](#), [SOC2 Type 2 compliance](#), and [HIPAA compliance](#).

Amazon FSx for NetApp ONTAP for NetApp Workload Factory is an [AWS solution for deploying enterprise apps](#) that was created with well-architected best practices in mind.

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 [NetApp Workload Factory console](#) and the [NetApp 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.

Hello Richard,

Let's get started by creating an account.

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

[Learn more about accounts.](#)



Account name

My Account

To help us organize menu options that best suit your objectives, we suggest that you provide us with some background about your job.

My job description

Optional

Select a job description

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 the NetApp Console, then you'll already belong to an account because Workload Factory leverages NetApp accounts.

Service accounts

A service account acts as a "user" that can make authorized API calls to NetApp 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](#)

Permissions

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

[Learn more about Workload Factory permission policies](#)

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-only*, and *read/write*) 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, database, or VMware workloads on FSx for ONTAP file systems against other Amazon services. 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](#)
- [Learn how to explore savings for your VMware workloads](#)

Well-architected workloads

Workload Factory helps you maintain and operate reliable, secure, efficient, and cost-effective storage and database configurations that align with the AWS Well-Architected Framework. Workload Factory scans FSx for ONTAP file systems, SQL Server, and Oracle database deployments daily to provide insights into potential misconfigurations and recommends either manual or automated actions for fixing issues.

[Learn more about well-architected workloads](#)

Tools to use NetApp Workload Factory

You can use NetApp Workload Factory with the following tools:

- **Workload Factory console:** The Workload Factory console provides a visual, holistic view of your applications and projects.
- **NetApp Console:** The NetApp Console provides a hybrid interface experience so that you can use Workload Factory along with other NetApp data services.
- **Ask me:** Use the Ask me AI assistant to ask questions and learn more about Workload Factory without leaving the Workload Factory console. Access Ask me from the Workload Factory help menu.
- **CloudShell CLI:** Workload Factory includes a CloudShell CLI to manage and operate AWS and NetApp environments across accounts from a single, browser-based CLI. Access CloudShell from the top bar of the Workload Factory console.
- **REST API:** Use the Workload Factory REST APIs to deploy and manage your FSx for ONTAP file systems and other AWS resources.
- **CloudFormation:** Use AWS CloudFormation code to perform the actions you defined in the Workload Factory console to model, provision, and manage AWS and third-party resources from the CloudFormation

stack in your AWS account.

- **Terraform NetApp Workload Factory provider:** Use Terraform to build and manage infrastructure workflows generated in the Workload Factory console.

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](#)

Console experiences

NetApp Workload Factory is accessible via two web-based consoles. Learn how to access Workload Factory using the Workload Factory console and the NetApp Console.

- **NetApp Console:** Offers a hybrid experience where you can manage your FSx for ONTAP file systems and workloads running on Amazon FSx for NetApp ONTAP 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 NetApp Console

You can access Workload Factory from the NetApp Console. In addition to using Workload Factory for AWS storage and workload capabilities, you can also access other data services like NetApp Copy and Sync and more.

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads** and then **Overview**.

Access Workload Factory in the Workload Factory console

You can access Workload Factory from the Workload Factory console.

Step

1. Log in to the [Workload Factory console](#).

Permissions for NetApp Workload Factory

To use NetApp 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 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. Permissions are bundled into set permission policies. Scroll to the workload you use to learn about the permission policies, copyable JSON for the permission policies, and a table that lists all permissions, their purpose, where they are used, and which permission policies 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.

Storage has the following permission policies to choose from:

- **View, planning, and analysis:** View FSx for ONTAP file systems, learn about system health, get the well-architected analysis for your systems, and explore savings.
- **Operations and remediation:** Perform operational tasks like adjust file system capacity and fix issues for your file system configurations.
- **File system creation and deletion:** Create and delete FSx for ONTAP file systems and storage VMs.

View the required IAM policies:

IAM policies for Storage

View, planning, and analysis

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "fsx:DescribeFileSystems",  
        "fsx:DescribeStorageVirtualMachines",  
        "fsx:DescribeVolumes",  
        "fsx>ListTagsForResource",  
        "fsx:DescribeBackups",  
        "fsx:DescribeSharedVpcConfiguration",  
        "cloudwatch:GetMetricData",  
        "cloudwatch:GetMetricStatistics",  
        "ec2:DescribeInstances",  
        "ec2:DescribeVolumes",  
        "elasticfilesystem:DescribeFileSystems",  
        "ce:GetCostAndUsage",  
        "ce:GetTags",  
      ],  
      "Resource": "*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam:SimulatePrincipalPolicy"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Operations and remediation

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "fsx>CreateVolume",  
        "fsx>DeleteVolume",  
        "fsx:UpdateFileSystem",  
      ]  
    }  
  ]  
}
```

```
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume",
        "fsx>CreateBackup",
        "fsx>CreateVolumeFromBackup",
        "fsx>DeleteBackup",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx>CreateAndAttachS3AccessPoint",
        "fsx:DetachAndDeleteS3AccessPoint",
        "s3>CreateAccessPoint",
        "s3>DeleteAccessPoint",
        "s3:GetObjectTagging",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock>ListInferenceProfiles",
        "bedrock:GetInferenceProfile",
        "s3tables CreateTableBucket",
        "s3tables>ListTables",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables CreateTable",
        "s3tables:GetNamespace",
        "s3tables:PutTableData",
        "s3tables>CreateNamespace",
        "s3tables:GetTableData",
        "s3tables>ListNamespaces",
        "s3tables>ListTableBuckets",
        "s3tables:GetTableBucket",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables>ListTagsForResource",
        "s3tables:TagResource",
        "s3:GetObjectTagging",
        "s3>ListBucket"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource": "*"
}
]
```

File system creation and deletion

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "fsx>CreateFileSystem",  
        "fsx>CreateStorageVirtualMachine",  
        "fsx>DeleteFileSystem",  
        "fsx>DeleteStorageVirtualMachine",  
        "fsx>TagResource",  
        "fsx>UntagResource",  
        "kms>CreateGrant",  
        "iam>CreateServiceLinkedRole",  
        "ec2>CreateSecurityGroup",  
        "ec2>CreateTags",  
        "ec2>DescribeVpcs",  
        "ec2>DescribeSubnets",  
        "ec2>DescribeSecurityGroups",  
        "ec2>DescribeRouteTables",  
        "ec2>DescribeNetworkInterfaces",  
        "ec2>DescribeVolumeStatus",  
        "kms>DescribeKey",  
        "kms>ListKeys",  
        "kms>ListAliases"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2>AuthorizeSecurityGroupEgress",  
        "ec2>AuthorizeSecurityGroupIngress",  
        "ec2>RevokeSecurityGroupEgress",  
        "ec2>RevokeSecurityGroupIngress",  
        "ec2>DeleteSecurityGroup"  
      ],  
      "Resource": "*",  
      "Condition": {  
        "StringLike": {  
          "ec2>ResourceTag/AppCreator": "NetappFSxWF"  
        }  
      }  
    },  
  ],  
}
```

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

The following table displays the permissions for Storage.

Table of permissions for Storage

Purpose	Action	Where used	Permission policy
Create an FSx for ONTAP file system	fsx>CreateFileSystem	Deployment	File system creation and deletion
Create a security group for an FSx for ONTAP file system	ec2>CreateSecurityGroup	Deployment	File system creation and deletion
Add tags to a security group for an FSx for ONTAP file system	ec2>CreateTags	Deployment	File system creation and deletion
Authorize security group egress and ingress for an FSx for ONTAP file system	ec2:AuthorizeSecurityGroupEgress	Deployment	File system creation and deletion
	ec2:AuthorizeSecurityGroupIngress	Deployment	File system creation and deletion
Granted role provides communication between FSx for ONTAP and other AWS services	iam>CreateServiceLinkedRole	Deployment	File system creation and deletion

Purpose	Action	Where used	Permission policy
Get details to fill in the FSx for ONTAP file system deployment form	ec2:DescribeVpcs	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
	ec2:DescribeSubnets	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
	ec2:DescribeSecurityGroups	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
	ec2:DescribeRouteTables	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
	ec2:DescribeNetworkInterfaces	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
	ec2:DescribeVolumeStatus	<ul style="list-style-type: none"> Deployment Explore savings 	File system creation and deletion
Get KMS key details and use for FSx for ONTAP encryption	kms:CreateGrant	Deployment	File system creation and deletion
	kms:DescribeKey	Deployment	File system creation and deletion
	kms>ListKeys	Deployment	File system creation and deletion
	kms>ListAliases	Deployment	File system creation and deletion
Get volume details for EC2 instances	ec2:DescribeVolumes	<ul style="list-style-type: none"> Inventory Explore savings 	View, planning, and analysis
Get details for EC2 instances	ec2:DescribeInstances	Explore savings	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Describe Elastic File System in the savings calculator	Elasticfilesystem:DescribeFileSystems	Explore savings	View, planning, and analysis
List tags for FSx for ONTAP resources	fsx>ListTagsForResource	Inventory	View, planning, and analysis
Manage security group egress and ingress for an FSx for ONTAP file system	ec2:RevokeSecurityGroupIngress	Management operations	File system creation and deletion
	ec2: RevokeSecurityGroupEgress	Management operations	File system creation and deletion
	ec2:DeleteSecurityGroup	Management operations	File system creation and deletion

Purpose	Action	Where used	Permission policy
Create, view, and manage FSx for ONTAP file system resources	fsx:CreateVolume	Management operations	Operations and remediation
	fsx:TagResource	Management operations	Operations and remediation
	fsx>CreateStorageVirtualMachine	Management operations	File system creation and deletion
	fsx>DeleteFileSystem	Management operations	File system creation and deletion
	fsx>DeleteStorageVirtualMachine	Management operations	View, planning, and analysis
	fsx:DescribeFileSystems	Inventory	View, planning, and analysis
	fsx:DescribeStorageVirtualMachines	Inventory	View, planning, and analysis
	fsx:DescribeSharedVpcConfiguration	Inventory	View, planning, and analysis
	fsx:UpdateFileSystem	Management operations	Operations and remediation
	fsx:UpdateStorageVirtualMachine	Management operations	Operations and remediation
	fsx:DescribeVolumes	Inventory	View, planning, and analysis
	fsx:UpdateVolume	Management operations	Operations and remediation
	fsx>DeleteVolume	Management operations	Operations and remediation
	fsx:UntagResource	Management operations	Operations and remediation
	fsx:DescribeBackups	Management operations	View, planning, and analysis
	fsx>CreateBackup	Management operations	Operations and remediation
	fsx>CreateVolumeFromBackup	Management operations	Operations and remediation
	fsx>DeleteBackup	Management operations	Operations and remediation

Purpose	Action	Where used	Permission policy
Get file system and volume metrics	cloudwatch:GetMetricData	Management operations	View, planning, and analysis
	cloudwatch:GetMetricStatistics	Management operations	View, planning, and analysis
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	All
Provide AI-based insights for FSx for ONTAP EMS events	bedrock>ListInferenceProfiles	FSx for ONTAP EMS analysis	Operations and remediation
	bedrock:GetInferenceProfile	FSx for ONTAP EMS analysis	Operations and remediation
	bedrock:InvokeModelWithResponseStream	FSx for ONTAP EMS analysis	Operations and remediation
	bedrock:InvokeModel	FSx for ONTAP EMS analysis	Operations and remediation
Get cost and usage data for FSx for ONTAP file systems from AWS Cost Explorer	ce:GetCostAndUsage	Cost and usage analysis	View, planning, and analysis
	ce:GetTags	Cost and usage analysis	View, planning, and analysis
Create an S3 access point and attaches it to an FSx for ONTAP file system	fsx>CreateAndAttachS3AccessPoint	S3 access point management	Operations and remediation
Detach an S3 access point from an FSx for ONTAP file system and delete it	fsx:DetachAndDeleteS3AccessPoint	S3 access point management	Operations and remediation
Create an S3 access point for simplified bucket access management	s3>CreateAccessPoint	S3 access point management	Operations and remediation
Delete an S3 access point	s3>DeleteAccessPoint	S3 access point management	Operations and remediation
Add tags to an S3 access point	s3:TagResource	S3 access point management	Operations and remediation
List and view tags on an S3 access point	s3>ListTagsForResource	S3 access point management	Operations and remediation
Remove tags from an S3 access point	s3:UntagResource	S3 access point management	Operations and remediation
Discover objects in an S3 access point bucket	s3>ListBucket	S3 bucket operations	Operations and remediation

Purpose	Action	Where used	Permission policy
List, create, and describe S3 table buckets	s3tables>ListTableBuckets s3tables>CreateTableBucket s3tables>GetTableBucket	S3 table bucket management	Operations and remediation
List, create, and retrieve S3 tables	s3tables>ListTables s3tables>CreateTable s3tables>GetTable	S3 table operations	Operations and remediation
Read table metadata location	s3tables>GetTableMetadataLocation	S3 table metadata operations	Operations and remediation
Update table metadata location	s3tables>UpdateTableMetadataLocation	S3 table metadata operations	Operations and remediation
List, create, and retrieve table namespaces	s3tables>ListNamespaces s3tables>CreateNamespace s3tables>GetNamespace	S3 namespace operations	Operations and remediation
Read table data (select, scan)	s3tables>GetTableData	S3 table data operations	Operations and remediation
Write table data (insert)	s3tables>PutTableData	S3 table data operations	Operations and remediation
List tags on an inventory table (get FSx for ONTAP, storage VM, volume IDs)	s3tables>ListTagsForResource	S3 table tag operations	Operations and remediation
Tag an inventory table for Workload Factory lookup	s3tables>TagResource	S3 table tag operations	Operations and remediation
Retrieve object tagging via access point	s3GetObjectTagging	S3 object operations	Operations and remediation

Permissions for Database workloads

The IAM policies available for Database workloads provide the permissions that Workload Factory needs to manage resources and processes within your public cloud environment.

Databases has the following permission policies to choose from:

- **View, planning, and analysis:** View the inventory of database resources, learn about the health of your resources, review the well-architected analysis for your database configurations, and explore savings, get error log analysis, and explores savings.
- **Operations and remediation:** Perform operational tasks for your database resources and fix issues for database configurations and the underlying FSx for ONTAP file system storage.
- **Database host creation:** Deploy database hosts and the underlying FSx for ONTAP file system storage according to best practices.

Select your operational mode to view the required IAM policies:

IAM policies for Database workloads

View, planning, and analysis

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "CommonGroup",  
      "Effect": "Allow",  
      "Action": [  
        "cloudwatch:GetMetricStatistics",  
        "cloudwatch:GetMetricData",  
        "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",
        "bedrock>GetFoundationModelAvailability",
        "bedrock>ListInferenceProfiles"
    ],
    "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/*"
}
]
}

```

Operations and remediation

```

[

{
  "Sid": "FSxRemediation",
  "Effect": "Allow",
  "Action": [
    "fsx:UpdateFileSystem",
    "fsx:UpdateVolume"
  ],
  "Resource": "*"
},

{
  "Sid": "EC2Remediation",
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:StopInstances"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/aws:cloudformation:stack-name": "WLMDB*"
    }
  }
}
]

```

Database host creation

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2TagGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:CreateAddress",
        "ec2:CreateHosts"
      ],
      "Resource": "*"
    }
  ]
}

```

```

        "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:ModifyInstancePlacement",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolume",
        "ec2:ModifyVolumeAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
    ],
    "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": "CreationGroup",
    "Effect": "Allow",
    "Action": [
        "cloudformation>CreateStack",
        "cloudformation>DescribeStackEvents",
        "cloudformation>DescribeStacks",
        "cloudformation>ValidateTemplate",
        "ec2>CreateLaunchTemplate",
        "ec2>CreateLaunchTemplateVersion",
        "ec2>CreateNetworkInterface",
        "ec2>CreateSecurityGroup",
        "ec2>CreateTags",
        "ec2>CreateVpcEndpoint",
        "ec2>RunInstances",
        "ec2>DescribeTags",
        "ec2>DescribeLaunchTemplates",
        "ec2>ModifyVpcAttribute",
        "fsx>CreateFileSystem",
        "fsx>CreateStorageVirtualMachine",
        "fsx>CreateVolume",
        "fsx>DescribeFileSystemAliases",
        "kms>CreateGrant",
        "kms>DescribeCustomKeyStores",
        "kms>GenerateDataKey",
        "kms>Decrypt",
        "logs>CreateLogGroup",
        "logs>CreateLogStream",
        "logs>GetLogGroupFields",
        "logs>GetLogRecord",
        "logs>ListLogDeliveries",
        "logs>PutLogEvents",
        "logs>TagResource",
        "sns>Publish",
        "ssm>PutComplianceItems",
        "ssm>PutConfigurePackageResult",
        "ssm>PutInventory",
        "ssm>UpdateAssociationStatus",
        "ssm>UpdateInstanceState",
        "ssm>UpdateInstanceInformation",
        "ssmmessages>CreateControlChannel",
        "ssmmessages>CreateDataChannel",
        "ssmmessages>OpenControlChannel",
        "ssmmessages>PutData"
    ]
}
```

```

        "ssmmessages:OpenDataChannel",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:PutRecommendationPreferences",
        "compute-
optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser"
    ],
    "Resource": "*"
},
{
    "Sid": "ArnGroup",
    "Effect": "Allow",
    "Action": [
        "cloudformation:SignalResource"
    ],
    "Resource": [
        "arn:aws:cloudformation:*:*:stack/WLMDB*",
        "arn:aws:logs:*:*:log-group:WLMDB*"
    ]
},
{
    "Sid": "IAMGroup1",
    "Effect": "Allow",
    "Action": [
        "iam:AddRoleToInstanceProfile",
        "iam>CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/WLMDB*"
    ]
},
{
    "Sid": "IAMGroup2",
    "Effect": "Allow",
    "Action": "iam>CreateServiceLinkedRole",

```

```

    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/WLMDB*"
    ],
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "IAMGroup3",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/WLMDB*"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "IAMGroup4",
    "Effect": "Allow",
    "Action": "iam:CreateRole",
    "Resource": "arn:aws:iam::*:role/WLMDB*"
}
]
}

```

The following table displays the permissions for database workloads.

Table of permissions for database workloads

Purpose	Action	Where used	Permission policy
Get metric statistics for FSx for ONTAP, EBS, and FSx for Windows File Server and for compute optimization recommendation	cloudwatch:GetMetricStatistics	<ul style="list-style-type: none"> Inventory Explore savings 	View, planning, and analysis
Gather performance metrics saved to Amazon CloudWatch from registered SQL nodes. Data generates in performance trend charts on the manage instance screen for registered SQL instances.	cloudwatch:GetMetricData	Inventory	View, planning, and analysis
Get details for EC2 instances	ec2:DescribeInstances	<ul style="list-style-type: none"> Inventory Explore savings 	View, planning, and analysis
	ec2:DescribeKeyPairs	Deployment	View, planning, and analysis
	ec2:DescribeNetworkInterfaces	Deployment	View, planning, and analysis
	ec2:DescribeInstanceTypes	<ul style="list-style-type: none"> Deployment Explore savings 	View, planning, and analysis
Get details to fill in the FSx for ONTAP deployment form	ec2:DescribeVpcs	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
	ec2:DescribeSubnets	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
	ec2:DescribeSecurityGroups	Deployment	View, planning, and analysis
	ec2:DescribeImages	Deployment	View, planning, and analysis
	ec2:DescribeRegions	Deployment	View, planning, and analysis
	ec2:DescribeRouteTables	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Get any existing VPC endpoints to determine if new endpoints need to be created before deployments	ec2:DescribeVpcEndpoints	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
Create VPC endpoints if they don't exist for required services irrespective of public network connectivity on EC2 instances	ec2:CreateVpcEndpoint	Deployment	Database host creation
Get instance types available in region for validation nodes (t2.micro/t3.micro)	ec2:DescribeInstanceTypeOfferings	Deployment	View, planning, and analysis
Get snapshot details of each attached EBS volumes for pricing and savings estimate	ec2:DescribeSnapshots	Explore savings	View, planning, and analysis
Get details of each attached EBS volumes for pricing and savings estimate	ec2:DescribeVolumes	<ul style="list-style-type: none"> Inventory Explore savings 	View, planning, and analysis
Get KMS key details for FSx for ONTAP file system encryption	kms>ListAliases	Deployment	View, planning, and analysis
	kms>ListKeys	Deployment	View, planning, and analysis
	kms>DescribeKey	Deployment	View, planning, and analysis
Get list of CloudFormation stacks running in the environment to check quota limit	cloudformation>ListStacks	Deployment	View, planning, and analysis
Check account limits for resources before triggering deployment	cloudformation>DescribeAccountLimits	Deployment	View, planning, and analysis
Get list of AWS-managed Active Directories in the region	ds>DescribeDirectories	Deployment	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Get lists and details of volumes, backups, SVMs, file systems in AZs, and tags for FSx for ONTAP file system	fsx:DescribeVolumes	<ul style="list-style-type: none"> • Inventory • Explore Savings 	View, planning, and analysis
	fsx:DescribeBackups	<ul style="list-style-type: none"> • Inventory • Explore Savings 	View, planning, and analysis
	fsx:DescribeStorageVirtualMachines	<ul style="list-style-type: none"> • Deployment • Management operations • Inventory 	View, planning, and analysis
	fsx:DescribeFileSystems	<ul style="list-style-type: none"> • Deployment • Management operations • Inventory • Explore savings 	View, planning, and analysis
	fsx>ListTagsForResource	Management operations	View, planning, and analysis
Get service quota limits for CloudFormation and VPC / Create secrets in a user account for the credentials provided for SQL, domain, and FSx for ONTAP	servicequotas>ListServiceQuotas	Deployment	View, planning, and analysis
Use SSM-based query to get the updated list of FSx for ONTAP supported regions	ssm>GetParametersByPath	Deployment	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Poll for SSM response after sending command for management operations post deployment	ssm:GetCommandInvocation	<ul style="list-style-type: none"> Management operations Inventory Explore savings Optimization 	View, planning, and analysis
Send commands over SSM to EC2 instances for discovery and management	ssm:SendCommand	<ul style="list-style-type: none"> Management operations Inventory Explore savings Optimization 	View, planning, and analysis
Get the SSM connectivity status on instances post deployment	ssm:GetConnectionStatus	<ul style="list-style-type: none"> Management operations Inventory Optimization 	View, planning, and analysis
Fetch SSM association status for a group of managed EC2 instances (SQL nodes)	ssm:DescribeInstanceInformation	Inventory	View, planning, and analysis
Get the list of available patch baselines for operating system patch assessment	ssm:DescribePatchBaselines	Optimization	View, planning, and analysis
Get the patching state on Windows EC2 instances for operating system patch assessment	ssm:DescribeInstancePatchStates	Optimization	View, planning, and analysis

Purpose	Action	Where used	Permission policy
List commands executed by AWS Patch Manager on EC2 instances for operating system patch management	ssm>ListCommands	Optimization	View, planning, and analysis
Check if account is enrolled in AWS Compute Optimizer	compute-optimizer:GetEnrollmentStatus	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation
Update an existing recommendation preference in AWS Compute Optimizer to tailor suggestions for SQL server workloads	compute-optimizer:PutRecommendationPreferences	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation
Get recommendation preferences that are in effect for a given resource from AWS Compute Optimizer	compute-optimizer:GetEffectiveRecommendationPreferences	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation
Fetch recommendations that AWS Compute Optimizer generates for Amazon Elastic Compute Cloud (Amazon EC2) instances	compute-optimizer:GetEC2InstanceRecommendations	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation
Check for instance association to auto-scaling groups	autoscaling:DescribeAutoScalingGroups	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation
	autoscaling:DescribeAutoScalingInstances	<ul style="list-style-type: none"> Explore savings Optimization 	Database host creation

Purpose	Action	Where used	Permission policy
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	<ul style="list-style-type: none"> Deployment Management operations Inventory 	View, planning, and analysis
	ssm:GetParameters ¹	<ul style="list-style-type: none"> Deployment Management operations Inventory 	View, planning, and analysis
	ssm:PutParameter ¹	<ul style="list-style-type: none"> Deployment Management operations 	View, planning, and analysis
	ssm:DeleteParameters ¹	<ul style="list-style-type: none"> Deployment Management operations 	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Associate network resources to SQL nodes and validation nodes, and add additional secondary IPs to SQL nodes	ec2:AllocateAddress ¹	Deployment	Database host creation
	ec2:AllocateHosts ¹	Deployment	Database host creation
	ec2:AssignPrivateIpAddresses ¹	Deployment	Database host creation
	ec2:AssociateAddress ¹	Deployment	Database host creation
	ec2:AssociateRouteTable ¹	Deployment	Database host creation
	ec2:AssociateSubnetCidrBlock ¹	Deployment	Database host creation
	ec2:AssociateVpcCidrBlock ¹	Deployment	Database host creation
	ec2:AttachInternetGateway ¹	Deployment	Database host creation
	ec2:AttachNetworkInterface ¹	Deployment	Database host creation
Attach EBS volumes required to the SQL nodes for deployment	ec2:AttachVolume	Deployment	Database host creation
Attach security groups and modify rules to provisioned EC2 instances	ec2:AuthorizeSecurityGroupEgress	Deployment	Database host creation
	ec2:AuthorizeSecurityGroupIngress	Deployment	Database host creation
Create EBS volumes required to the SQL nodes for deployment	ec2>CreateVolume	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
Remove the temporary validation nodes created of type t2.micro and for rollback or retry of failed EC2 SQL nodes	ec2:DeleteNetworkInterface	Deployment	Database host creation
	ec2:DeleteSecurityGroup	Deployment	Database host creation
	ec2:DeleteTags	Deployment	Database host creation
	ec2:DeleteVolume	Deployment	Database host creation
	ec2:DetachNetworkInterface	Deployment	Database host creation
	ec2:DetachVolume	Deployment	Database host creation
	ec2:DisassociateAddress	Deployment	Database host creation
	ec2:DisassociateIamInstanceProfile	Deployment	Database host creation
	ec2:DisassociateRouteTable	Deployment	Database host creation
	ec2:DisassociateSubnetCidrBlock	Deployment	Database host creation
	ec2:DisassociateVpcCidrBlock	Deployment	Database host creation
Modify attributes for created SQL instances. Only applicable to names that start with WLMDB.	ec2:ModifyInstanceAttribute	Deployment	Operations and remediation
	ec2:ModifyInstancePlacement	Deployment	Database host creation
	ec2:ModifyNetworkInterfaceAttribute	Deployment	Database host creation
	ec2:ModifySubnetAttribute	Deployment	Database host creation
	ec2:ModifyVolume	Deployment	Database host creation
	ec2:ModifyVolumeAttribute	Deployment	Database host creation
	ec2:ModifyVpcAttribute	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
Disassociate and destroy validation instances	ec2:ReleaseAddress	Deployment	Database host creation
	ec2:ReplaceRoute	Deployment	Database host creation
	ec2:ReplaceRouteTableAssociation	Deployment	Database host creation
	ec2:RevokeSecurityGroupEgress	Deployment	Database host creation
	ec2:RevokeSecurityGroupIngress	Deployment	Database host creation
Start the deployed instances	ec2:StartInstances	Deployment	Operations and remediation
Stop the deployed instances	ec2:StopInstances	Deployment	Operations and remediation
Tag custom values for Amazon FSx for NetApp ONTAP resources created by WLMDB to get billing details during resource management	fsx:TagResource ¹	<ul style="list-style-type: none"> Deployment Management operations 	Database host creation
Create and validate CloudFormation template for deployment	cloudformation>CreateStack	Deployment	Database host creation
	cloudformation>DescribeStackEvents	Deployment	Database host creation
	cloudformation>DescribeStacks	Deployment	Database host creation
	cloudformation>ListStacks	Deployment	View, planning, and analysis
	cloudformation>ValidateTemplate	Deployment	Database host creation
Create nested stack templates for retry and rollback	ec2>CreateLaunchTemplate	Deployment	Database host creation
	ec2>CreateLaunchTemplateVersion	Deployment	Database host creation
Manage tags and network security on created instances	ec2>CreateNetworkInterface	Deployment	Database host creation
	ec2>CreateSecurityGroup	Deployment	Database host creation
	ec2>CreateTags	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
Get instance details for provisioning	ec2:DescribeAddresses	Deployment	View, planning, and analysis
	ec2:DescribeLaunchTemplates	Deployment	View, planning, and analysis
Start the created instances	ec2:RunInstances	Deployment	Database host creation
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	Database host creation
	fsx>CreateStorageVirtualMachine	Deployment	Database host creation
	fsx>CreateVolume	<ul style="list-style-type: none"> Deployment Management operations 	Database host creation
Get FSx for ONTAP details	fsx:DescribeFileSystemAliases	Deployment	Database host creation
Resize FSx for ONTAP file system to remediate file system headroom	fsx:UpdateFilesystem	Optimization	Operations and remediation
Resize volumes to remediate log and TempDB drive sizes	fsx:UpdateVolume	Optimization	Operations and remediation
Get KMS key details and use for FSx for ONTAP encryption	kms>CreateGrant	Deployment	Database host creation
	kms:DescribeCustomKeyStores	Deployment	Database host creation
	kms:GenerateDataKey	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
Create CloudWatch logs for validation and provisioning scripts running on EC2 instances	logs:CreateLogGroup	Deployment	Database host creation
	logs:CreateLogStream	Deployment	Database host creation
	logs:GetLogGroupFields	Deployment	Database host creation
	logs:GetLogRecord	Deployment	Database host creation
	logs>ListLogDeliveries	Deployment	Database host creation
	logs:PutLogEvents	<ul style="list-style-type: none"> Deployment Management operations 	Database host creation
	logs:TagResource	Deployment	Database host creation
Workload Factory switches to Amazon CloudWatch logs for the SQL instance upon encountering SSM output truncation	logs:GetLogEvents	<ul style="list-style-type: none"> Storage assessment (Optimization) Inventory 	View, planning, and analysis
Allow Workload Factory to get current log groups and check that retention is set for log groups created by Workload Factory	logs:DescribeLogGroups	<ul style="list-style-type: none"> Storage assessment (Optimization) Inventory 	View, planning, and analysis
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	<ul style="list-style-type: none"> Storage assessment (Optimization) Inventory 	View, planning, and analysis
List customer SNS topics and publish to WLMDB backend SNS as well as customer SNS if selected	sns>ListTopics	Deployment	View, planning, and analysis
	sns:Publish	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
	ssm:PutComplianceItems	Deployment	Database host creation
	ssm:PutConfigurePackageResult	Deployment	Database host creation
	ssm:PutInventory	Deployment	Database host creation
	ssm:UpdateAssociationStatus	Deployment	Database host creation
	ssm:UpdateInstanceAssociationStatus	Deployment	Database host creation
	ssm:UpdateInstanceInformation	Deployment	Database host creation
	ssmmessages:CreateControlChannel	Deployment	Database host creation
	ssmmessages:CreateDataChannel	Deployment	Database host creation
	ssmmessages:OpenControlChannel	Deployment	Database host creation
	ssmmessages:OpenDataChannel	Deployment	Database host creation
Signal CloudFormation stack on success or failure.	cloudformation:SignalResource ¹	Deployment	Database host creation
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	Database host creation
Create instance profile for EC2 and attach the created EC2 role.	iam:CreateInstanceProfile	Deployment	Database host creation
Create EC2 role through template with permissions listed below	iam:CreateRole	Deployment	Database host creation
Create role linked to EC2 service	iam:CreateServiceLinkedRole ²	Deployment	Database host creation
Delete instance profile created during deployment specifically for the validation nodes	iam:DeleteInstanceProfile	Deployment	Database host creation

Purpose	Action	Where used	Permission policy
Get the role and policy details to determine any gaps in permission and validate for deployment	iam:GetPolicy	Deployment	Database host creation
	iam:GetPolicyVersion	Deployment	Database host creation
	iam:GetRole	Deployment	Database host creation
	iam:GetRolePolicy	Deployment	Database host creation
	iam:GetUser	Deployment	Database host creation
Pass the role created to EC2 instance	iam:PassRole ³	Deployment	Database host creation
Add policy with required permissions to the EC2 role created	iam:PutRolePolicy	Deployment	Database host creation
Detach role from the provisioned EC2 instance profile	iam:RemoveRoleFromInstanceProfile	Deployment	Database host creation
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	All
Get the foundation models available for error log analysis	bedrock:GetFoundationModelAvailability	Error log analysis	View, planning, and analysis
List interface profiles available in Amazon Bedrock for error log analysis	bedrock>ListInferenceProfiles	Error log analysis	View, planning, and analysis

1. Permission is restricted to resources starting with WLMDB.
2. "iam:CreateServiceLinkedRole" limited by "iam:AWSPropertyName": "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 with *read/write* permissions:

- **Read/Write:** executes and automates operations in AWS on your behalf along with the assigned credentials that have the needed and validated permissions for execution.

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: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:ListTagsForResource"
  ],
  "Resource": "*"
}

```

```
    "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"
  ],
  "Resource": [
    "arn:aws:ssm:*:instance/*"
  ]
}
```

```
"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:ListRolePolicies",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    }
]
```

```

    "Effect": "Allow",
    "Action": [
        "iam:CreatePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "QBusiness",
    "Effect": "Allow",
    "Action": [
        "qbusiness>ListApplications"
    ],
    "Resource": "*"
},
{
    "Sid": "S3",
    "Effect": "Allow",
    "Action": [
        "s3>ListAllMyBuckets"
    ],
    "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	Permission policy
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 S3 buckets	s3>ListAllMyBuckets	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

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

Purpose	Action	Where used	Permission policy
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
List inference profiles for the model	bedrock>ListInferenceProfiles	Troubleshooting	Read/Write

Permissions for VMware workloads

VMware workloads has the following permission policies to choose from:

- **View, planning, and analysis:** View the inventory of EVS virtualization environments, get the well-architected analysis for your systems, and explore savings.
- **Datastore deployment and connectivity:** Deploy recommended VM layouts to Amazon EVS, Amazon EC2, or VMware Cloud on AWS vSphere clusters and use customized Amazon FSx for NetApp ONTAP file systems as external datastores.

Select the permission policy to view the required IAM policies:

IAM policies for VMware workloads

View, planning, and analysis

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:DescribeRegions",  
        "ec2:DescribeAvailabilityZones",  
        "ec2:DescribeVpcs",  
        "ec2:DescribeSecurityGroups",  
        "ec2:DescribeSubnets",  
        "ec2:DescribeDhcpOptions",  
        "kms:DescribeKey",  
        "kms>ListKeys",  
        "kms>ListAliases",  
        "secretsmanager>ListSecrets",  
        "evs>ListEnvironments",  
        "evs:GetEnvironment",  
        "evs>ListEnvironmentVlans"  
      ],  
      "Resource": "*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "iam:SimulatePrincipalPolicy"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Datastore deployment and connectivity

```
{  
  "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>GenerateDataKey",
            "kms>Decrypt",
            "kms>CreateGrant"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2>RunInstances",
            "ec2>DescribeInstances",
            "ec2>CreateSecurityGroup",
            "ec2>AuthorizeSecurityGroupIngress",
            "ec2>DescribeImages"
        ],
        "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	Permission policy
Attach security groups and modify rules for the provisioned nodes	ec2:AuthorizeSecurityGroupIngress	Deployment	Datastore deployment and connectivity
Create EBS volumes	fsx>CreateVolume	Deployment	Datastore deployment and connectivity
Tag custom values for FSx for NetApp ONTAP resources created by VMware workloads	fsx:TagResource	Deployment	Datastore deployment and connectivity
Create and validate the CloudFormation template	cloudformation>CreateStack	Deployment	Datastore deployment and connectivity
Manage tags and network security on created instances	ec2>CreateSecurityGroup	Deployment	Datastore deployment and connectivity
Start the created instances	ec2:RunInstances	Deployment	Datastore deployment and connectivity
Get EC2 instance details	ec2:DescribeInstances	Inventory	Datastore deployment and connectivity
List images during the stack creation during deploy and rebuild operations	ec2:DescribeImages	Inventory	Datastore deployment and connectivity
View configuration details of DHCP options sets associated with VPCs	ec2:DescribeDhcpOptions	Inventory	View, planning, and analysis
Get the VPCs in the selected environment to complete deployment form	ec2:DescribeVpcs	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
Get the subnets in selected environment to complete deployment form	ec2:DescribeSubnets	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
Get the security groups in selected environment to complete deployment form	ec2:DescribeSecurityGroups	Deployment	View, planning, and analysis
Get the availability zones in selected environment	ec2:DescribeAvailabilityZones	<ul style="list-style-type: none"> Deployment Inventory 	View, planning, and analysis
Get the regions with Amazon FSx for NetApp ONTAP support	ec2:DescribeRegions	Deployment	View, planning, and analysis

Purpose	Action	Where used	Permission policy
Get KMS keys' aliases to be used for Amazon FSx for NetApp ONTAP encryption	kms>ListAliases	Deployment	View, planning, and analysis
Get KMS keys to be used for Amazon FSx for NetApp ONTAP encryption	kms>ListKeys	Deployment	View, planning, and analysis
Get KMS keys expiry details to be used for Amazon FSx for NetApp ONTAP encryption	kms>DescribeKey	Deployment	View, planning, and analysis
List secrets in AWS Secrets Manager	secretsmanager>ListSecrets	Inventory	View, planning, and analysis
Get a list of environments from Amazon EVS	evs>ListEnvironments	Inventory	View, planning, and analysis
Get detailed information about a specific Amazon EVS environment	evs>GetEnvironment	Inventory	View, planning, and analysis
List Vlans associated with an Amazon EVS environment	evs>ListEnvironmentVlans	Inventory	View, planning, and analysis
Create Amazon FSx for NetApp ONTAP resources required for provisioning	fsx>CreateFileSystem	Deployment	Datastore deployment and connectivity
	fsx>CreateStorageVirtualMachine	Deployment	Datastore deployment and connectivity
	fsx>CreateVolume	<ul style="list-style-type: none"> Deployment Management operations 	Datastore deployment and connectivity
Get Amazon FSx for NetApp ONTAP details	fsx>Describe*	<ul style="list-style-type: none"> Deployment Inventory Management operations Explore savings 	Datastore deployment and connectivity

Purpose	Action	Where used	Permission policy
Get KMS key details and use for Amazon FSx for NetApp ONTAP encryption	kms:CreateGrant	Deployment	Datastore deployment and connectivity
	kms:Describe*	Deployment	View, planning, and analysis
	kms>List*	Deployment	View, planning, and analysis
	kms:Decrypt	Deployment	Datastore deployment and connectivity
	kms:GenerateDataKey	Deployment	Datastore deployment and connectivity
List customer SNS topics and publish to WLMVMC backend SNS as well as customer SNS if selected	sns:Publish	Deployment	Datastore deployment and connectivity
Simulate workload operations to validate available permissions and compare with required AWS account permissions	iam:SimulatePrincipalPolicy	Deployment	<ul style="list-style-type: none"> • Datastore deployment and connectivity • View, planning, and analysis

Change log

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

1 February 2025

The following permissions were added to the Storage workload:

- s3:TagResource
- s3>ListTagsForResource
- s3:UntagResource
- s3tables>CreateTableBucket
- s3tables>ListTables
- s3tables:GetTable
- s3tables:GetTableMetadataLocation

- s3tables:CreateTable
- s3tables:GetNamespace
- s3tables:PutTableData
- s3tables>CreateNamespace
- s3tables:GetTableData
- s3tables>ListNamespaces
- s3tables>ListTableBuckets
- s3tables:GetTableBucket
- s3tables:UpdateTableMetadataLocation
- s3tables>ListTagsForResource
- s3tables:TagResource
- s3:GetObjectTagging
- s3>ListBucket

04 December 2025

The following permissions were added to the Storage workload:

- fsx>CreateAndAttachS3AccessPoint
- fsx:DetachAndDeleteS3AccessPoint
- s3>CreateAccessPoint
- s3>DeleteAccessPoint

27 November 2025

The following permissions were added to the Storage workload:

- bedrock>ListInferenceProfiles
- bedrock:GetInferenceProfile
- bedrock:InvokeModelWithResponseStream
- bedrock:InvokeModel

2 November 2025

The permission policies "read-only" and "read/write" have been replaced in Storage, Database workloads, and VMware workloads to provide more granularity and flexibility in assigning permissions.

5 October 2025

The following permissions were removed from GenAI and are now handled by the GenAI engine:

- bedrock:GetMappingInvocationLoggingConfiguration

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

29 June 2025

The following permission is now available in *read-only* mode for Databases: `cloudwatch:GetMetricData`.

3 June 2025

The following permission is now available in *read/write* mode for GenAI: `s3>ListAllMyBuckets`.

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 NetApp Workload Factory

Get started with NetApp 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.

NetApp 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](#).

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 without adding credentials to access your AWS account. Adding AWS credentials to Workload Factory 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

After 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.

[Optimize your workloads with FSx for ONTAP.](#)

Sign up to NetApp Workload Factory

NetApp 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.

You can also invite others to join your Workload Factory account so they can access and use Workload Factory.

Sign up to Workload Factory

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**.

Sign up to Workload Factory

user@company.com

.....

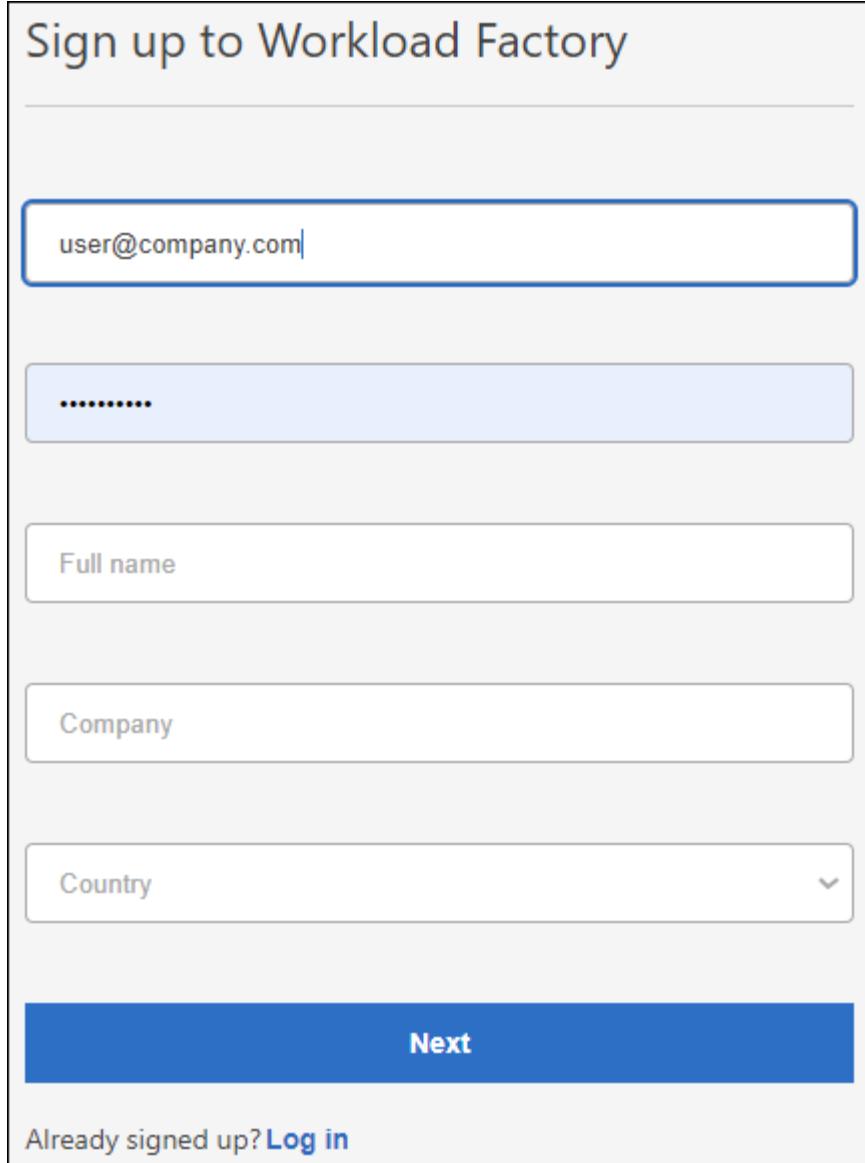
Full name

Company

Country

Next

Already signed up? [Log in](#)



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.

Hello Richard,

Let's get started by creating an account.



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

[Learn more about accounts.](#)

Account name

To help us organize menu options that best suit your objectives, we suggest that you provide us with some background about your job.

My job description

Optional

Select a job description

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.

Invite others to join an account in Workload Factory

As an Account Admin, you can invite others to join your Workload Factory account so they can access and use Workload Factory. Account management is possible only from the NetApp Console.

Refer to NetApp Console documentation to [learn how to add members \(user accounts\)](#), to your Workload Factory account.

Result

The invited user will receive an email with instructions to join your Workload Factory account.

Add AWS credentials to Workload Factory

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

Overview

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.

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 permissions 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.

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 NetApp 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. From the menu, select **Administration** and then **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*.

The screenshot shows the 'Add Credentials' page. At the top, there are two options: 'Add manually' (selected) and 'Add via AWS Cloud Formation'. The 'Permissions configuration' section contains three dropdowns: 'Create policies' (No policies were selected), 'Create role' (Action required), and 'Credentials name' (Action required).

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 policies, 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.

Permissions configuration

Create role

From the AWS Management Console

- 1 | Navigate to the IAM service.
- 2 | Select **Roles > Create role**.
- 3 | Select **AWS account > Another AWS account**.
 - Enter the account ID for FSx for ONTAP workload management: `<account ID>` 
 - Select **Require external ID** and enter: `<external ID>` 
- 4 | Select **Next**.
- 5 | In the Permissions policy section, choose all of the policies that you previously defined and click **select Next**.
- 6 | Enter a name for the role and select **Create role**.
- 7 | Copy the Role ARN and paste it below.

Role ARN

`arn:aws:iam::account:role/role-name-with-path`

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 Add Credentials page in Workload Factory, expand the **Create role** section under **Permission configuration**, 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 Add Credentials page in Workload Factory, expand **Credentials name** under **Permission configuration**.
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. From the menu, select **Administration** and then **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.

Optimize workloads with NetApp Workload Factory

After you've logged in and set up NetApp 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 template FSx for ONTAP deployments based on best practices, and access advanced management capabilities.

- [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.

- [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.

- [VMware workloads](#)

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

- [EDA workloads](#)

Optimize FSx for ONTAP across multiple file system to boost performance and reduce operational costs through automated storage parameter management.

Administer Workload Factory

Log in to NetApp Workload Factory

After you sign up to NetApp 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 NetApp. Account admins create service accounts, control access, and delete service accounts. You can manage service accounts in the NetApp Console or in the NetApp Workload Factory console.

Unlike managing service accounts in the NetApp Console 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 NetApp 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 NetApp console or in the Workload Factory console. There are slight differences. The following instructions describe how to manage service accounts in the Workload Factory console.

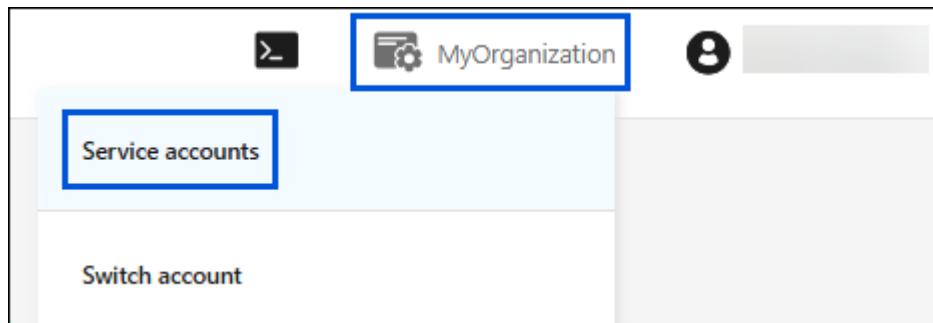
To manage service accounts in the NetApp Console, [learn how identity and access management works](#) and [learn how to add IAM members and manage their permissions](#).

Create a service account

When you create a service account, 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 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 you can 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 NetApp Workload Factory APIs.
7. Select **Close**.

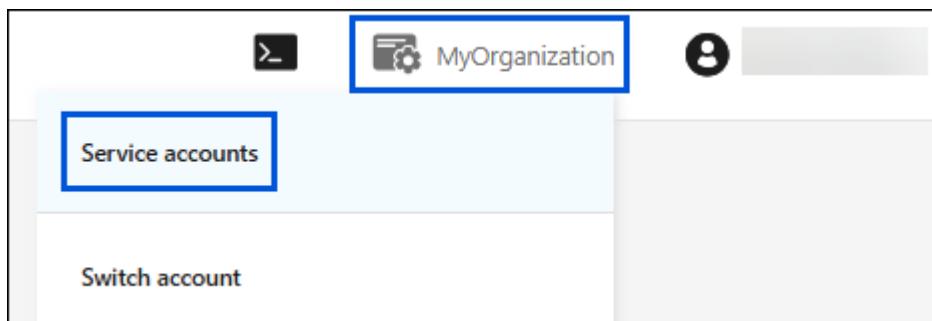
The new service account is created and listed on the Service accounts page.

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 actions menu and then select **Delete**.
3. In the Delete service account dialog, enter **delete** in the text box.
4. Select **Delete** to confirm deletion.

Build and operate well-architected workloads

Workload Factory, the NetApp management suite for Amazon FSx for NetApp ONTAP, helps you maintain and operate reliable, secure, efficient, and cost-effective storage and database configurations that align with the AWS Well-Architected Framework. Workload Factory provides daily analysis of your storage and database workloads, recommendations, and automatic fixes to promote healthy workload operations. By automating this process, Workload Factory minimizes human error and ensures consistency in workload management.

How it works

Workload Factory analyzes Amazon FSx for NetApp ONTAP file systems, Microsoft SQL Server, and Oracle database deployments daily. The analysis provides well-architected status, insights, and recommendations. You can automatically fix configuration issues to meet best practices and operate efficiently.

After the daily analysis completes, configurations appear as "optimized" or "not optimized" in the Well-architected dashboard for the deployment. You'll find the total optimization score, configuration issues by category, and a list of configuration issues and recommendations. You can review the recommendations for configuration issues. Some issues can be fixed automatically by Workload Factory, while others require manual intervention. In this case, Workload Factory provides detailed instructions to help you implement the recommended changes.

You can dismiss the analysis of configurations that do not apply to your environments. This avoids unnecessary alerts and inaccurate optimization results. When you dismiss a specific configuration analysis, Workload Factory does not include the configuration in the total optimization score.

Why it matters

Workload Factory applies best practices to large storage or database environments by combining ongoing assessment with recommendation insights and remediation. Automated fixes reduce human error, ensure uniform management, and maintain performance and reliability. Fixes applied in the Workload Factory console reduce human error and ensure uniform management. Automation ensures configurations are applied correctly and maintained, preserving performance and reliability across your workload infrastructures.

Get started with Workload Factory to detect and correct misconfigurations

To get started with Workload Factory, sign up, add credentials, and establish connectivity to manage AWS resources and optimize workloads using Amazon FSx for NetApp ONTAP.

[Quick start](#)

Best practices and recommendations for storage workloads

Workload Factory assesses storage configurations to provide an in-depth view of ONTAP configuration best practices and for compliance with the AWS Well-Architected Framework. The assessment also recommends improvements and fixes.

The well-architected analysis categorizes configurations in the following pillars of the framework: *reliability*, *security*, *operational excellence*, *cost optimization*, and *performance efficiency*.

Reliability

Reliability ensures that workloads perform their intended functions correctly and consistently, even when there are disruptions.

- **Schedule FSx for ONTAP backups**

FSx for ONTAP: Backing up your volumes helps support data retention and compliance needs. Use FSx for ONTAP backup to set up automated backups and retention for your data.

- **Schedule local snapshots**

Schedule local snapshots for efficient backup and quick restores. Snapshots are instant, point-in-time images of your volumes.

- **Cross-region replication**

Cross-region replication ensures that your data is replicated to another AWS region, providing enhanced data durability and availability. Workload Factory recommends setting up cross-region replication to help with disaster recovery and compliance.

- **Set up data replication**

To extend data reliability, data can be replicated to an FSx for ONTAP file system in the same region or in another region. Set up data replication to support migration, disaster recovery, and long-term retention across file systems.

- **Increase SSD capacity threshold**

The SSD storage tier capacity should not exceed 80% utilization on an ongoing basis. This might impact data reads and writes to your capacity pool storage tier and impact the throughput capacity of your file

system. Running out of capacity might result in data volumes becoming read-only, and services trying to write new data might fail.

- **Match labels to ensure data reliability**

The snapshot policy labels of the source volume and the replication policy labels must match to ensure data reliability.

- **Increase file capacity threshold**

The file capacity threshold should be raised to avoid hitting the volume capacity limit. Low file capacity (inodes) prevents writing additional data to the volume. Workload Factory recommends staying below 80% utilization of the available file capacity on an ongoing basis. Available file capacity is required to create new files in the volume.

Security

Security emphasizes protecting data, systems, and assets through risk assessments and mitigation strategies.

- **Enable ARP/AI**

NetApp Autonomous Ransomware Protection with AI (ARP/AI) helps protect your volumes from ransomware threats. Workload Factory recommends enabling ARP/AI for all volumes.

- **Unauthorized access to volumes**

Volumes serving application data using iSCSI should not allow NAS access in parallel. Workload Factory recommends that volumes accessed via the iSCSI protocol should be restricted to any additional protocols.

Operational excellence

Operational excellence focuses on delivering the most optimal architecture and business value.

- **Enable automatic capacity management**

Automatic capacity management should be enabled to regularly ensure that the SSD tier doesn't exceed the threshold.

- **Volume capacity utilization threshold**

Workload Factory recommends that volume capacity doesn't exceed 80% utilization on an ongoing basis. This might impact data reads and writes to your application. Volume capacity increases can be manual or automatic using the volume autogrow feature.

- **Volume utilization nearing full**

When a volume is nearing full capacity, Workload Factory recommends taking action to increase the volume capacity to avoid potential application disruptions.

- **Cache relationship write mode**

For optimal performance, Workload Factory recommends the cache relationship write mode that best suits your workload. Write-around mode provides better performance for read-heavy workloads with small files, whereas write-back mode provides better performance for write-heavy workloads with large files.

- **Optimize cache volume size**

Workload Factory recommends enabling volume autosize and scrubbing on cache volumes to maintain optimal size and focus the cache on hot data for peak efficiency.

- **Storage VM logical reporting**

Workload Factory recommends that the default reporting setting is set to logical for a storage VM to provide better visibility into storage usage at the volume level.

Cost optimization

Cost optimization helps you get the most value for your business while keeping costs low.

- **Optimize TCO by tiering cold data**

Cold data tiering should be enabled to reduce SSD storage tier utilization. Applying a tiering policy to every volume is recommended. FSx for ONTAP scans the data continuously to detect cold data and move it to the capacity storage pool tier without disruption.

- **Enable storage efficiencies**

Storage efficiencies should be enabled - compaction, compression, and deduplication - to optimize storage utilization and reduce the SSD tier cost.

- **Unnecessary snapshot and backup deletion**

Snapshots and backups that are no longer needed should be deleted to reduce costs.

- **Orphaned block devices**

After a block device isn't used for seven days, Workload Factory recommends archiving block device data or deleting the unused block device to reduce costs.

Best practices and recommendations for database workloads

Workload Factory provides a set of best practices and recommendations for operating well-architected database workloads. The well-architected analysis assesses Microsoft SQL Server and Oracle Database configurations and settings related to storage sizing, storage layout, storage configuration, compute, application (SQL Server), and resiliency.

Storage sizing

- **Storage tier**

For best storage performance, create FSx for ONTAP volumes on the primary SSD tier. Using the capacity pool tier might make performance slower and increase latency.

- **File system headroom**

To optimize storage performance, set the file system capacity to 1.35 times the total size of your volumes.

File system headroom percentages are as follows:

- Under-provisioned: < 35%
- Optimized: 35-100%
- Over-provisioned: > 100%

- **Log drive size**

Ensure accurate sizing and regular monitoring of the SQL Server log drive to prevent issues such as transaction rollbacks, database unavailability, data corruption, and performance degradation caused by a full log drive.

Log drive size percentages are as follows:

- Under-provisioned: < 20%
- Optimized: 20-30%
- Over-provisioned: > 30%

- **TempDB drive size**

Ensure accurate sizing and regular monitoring of the SQL Server TempDB to optimize performance and maintain overall stability. Properly configured TempDB prevents performance issues and instability. Insufficient space or high contention can lead to query slowdowns, application timeouts, and system crashes.

TempDB drive size percentages are as follows:

- Under-provisioned: < 10%
- Optimized: 10-20%
- Over-provisioned: > 20%

Storage layout

- **Data files (.mdf) placement**

Separate data and log files onto different drives to improve performance, enable independent backup schedules, and improve restore functionality. For smaller databases, separate data and log LUN paths into different volumes. This separation is required for more than one large database (> 500 GiB).

- **Log files (.ldf) placement**

Separate data and log files onto different drives to improve performance, enable independent backup schedules, and improve restore functionality. For smaller databases, separate data and log LUN paths into different volumes. This separation is required for more than one large database (> 500 GiB).

- **TempDB placement**

Isolate TempDB I/O and avoid I/O contention from other databases by placing TempDB on its own dedicated drive. This optimization improves overall SQL Server performance and stability. Failure to do so can result in significant I/O bottlenecks, slower query performance, and potential system instability.

Storage configuration

- **ONTAP configuration**

Entity	Setting	Recommendation
Volume	<ul style="list-style-type: none"> Thin provisioning (-space-guarantee = none) Autosize on Autosize-mode = grow Fractional reserve = 0% Snapshot copy reserve = 0% Snapshot autodelete (volume/oldest first) Space-mgmt-try-first = volume_grow 	To optimize storage efficiency and cost-effectiveness, configure thin provisioning, autosize, and space management options for your FSx for ONTAP volumes. Without thin provisioning, storage is allocated upfront, leading to inefficient use and higher costs due to over-provisioning; static allocation results in paying for unused capacity, increasing expenses; lack of dynamic allocation hampers scalability and flexibility, impacting performance; and without space reclamation, deleted data occupies space, reducing efficiency.
Volume	<ul style="list-style-type: none"> Tiering-policy = snapshot-only Tiering-minimum-cooling-days = 7 	For optimal database performance and cost efficiency, Workload Factory recommends moving only snapshots to the capacity tier. This strategy ensures high performance while reducing costs. It is especially recommended to tier snapshots that are older than 7 days.
LUN	OS type = windows_2008	ONTAP LUN OS type value should match the operating system partitioning scheme to achieve I/O alignment. Incorrect configuration might result in suboptimal performance.
LUN	Space reservation enabled	When space reservation is enabled, ONTAP reserves enough space in the volume so that writes to those LUNs do not fail because of a lack of disk space.
LUN	Space allocation enabled	This option ensures that FSx for ONTAP notifies the EC2 host when the volume is full and cannot accept writes. This setting also allows FSx for ONTAP to automatically reclaim space when SQL Server on the EC2 host deletes data. If disabled, write failures are possible and space might be inefficiently utilized.

- Windows storage configuration

Entity	Setting	Recommendation
Microsoft Multipath I/O (MPIO)	<ul style="list-style-type: none"> • Status = Enabled • Policy = Round Robin • Number of sessions = 5 	To ensure optimal uptime and data access consistency for Microsoft SQL Server databases on EC2 with underlying LUNs provisioned in FSx for ONTAP, Workload Factory recommends enabling and configuring Multipath I/O (MPIO). MPIO provides multiple paths to FSx for ONTAP, enhancing both resiliency and performance. This best practice protects against potential data loss or downtime by maintaining data access even if a component fails.
Allocation unit size	NTFS allocation unit size = 64K	Set NTFS allocation unit size to 64K to better use disk space, reduce fragmentation, and improve file read/write performance. Failure to configure this properly might lead to inefficient disk usage and degraded performance.

Compute

- **Compute rightsizing**

To ensure optimal performance and cost efficiency for your SQL Server EC2 instance, we recommend rightsizing based on your workload demands. If your current instance is under-provisioned, upgrading will enhance CPU, memory, and I/O capacity. If it is over-provisioned, downgrading will maintain performance while reducing costs.

- **Operating system patch**

Workload Factory recommends applying the latest patches to ensure security, protect SQL Server databases from vulnerabilities, and improve system reliability.

- **Network adapter settings**

Accurate configuration of receive side scaling (RSS) is essential for optimal network performance in Microsoft SQL Server instances. RSS distributes network processing across multiple processors, preventing bottlenecks and enhancing system performance. Workload Factory recommends the following RSS settings:

- Disable TCP Offloading Features: Ensure all TCP offloading features are disabled.
- Number of Receive Queues: Set to 8 if vCPUs > 8. Set to the number of vCPUs if vCPUs ≤ 8.
- RSS Profile: Set to NUMAStatic.
- Base Processor Number: Set to 2.

Following these settings will improve the performance and reliability of your Microsoft SQL Server instances. We suggest that you test the recommended settings to determine performance improvements before making changes to your production environment.

Application (SQL Server)

- **License**

The SQL Server license assessment and recommendation are provided at the host level.

Not optimized: A license is considered "not optimized" when Workload Factory detects that your database infrastructure doesn't use any of the commercial software license features you're paying for. An unoptimized license might result in unnecessary costs.

Optimized: A license is considered "optimized" when the commercial software license for your databases meets your performance requirements.

- **Microsoft SQL Server patch**

Workload Factory recommends applying the latest patches to ensure security, protect SQL Server databases from vulnerabilities, and improve system reliability.

- **MAXDOP**

Set the Maximum Degree of Parallelism (MAXDOP) to optimize query performance by balancing parallel processing. Accurate MAXDOP configuration enhances performance and efficiency. Setting MAXDOP to 4, 8, or 16 generally provides the best results in most use cases. We recommend that you test your workload and monitor for any parallelism-related wait types such as CXPACKET.

Reliability

- **Schedule FSx for ONTAP backups**

Backing up your Microsoft SQL Server volumes is crucial for supporting your data retention and compliance requirements. Use FSx for ONTAP backup to set up automatic backups and retention for your SQL Server data.

- **Schedule local snapshots**

Schedule local snapshots for efficient backup and quick restores. Snapshots are instant, point-in-time images of your volumes.

- **Cross-region replication**

Cross-region replication ensures that your data is replicated to another AWS region, providing enhanced data durability and availability. Workload Factory recommends setting up cross-region replication to help with disaster recovery and compliance.

Best practices and recommendations for EVS workloads

Workload Factory provides best practices and recommendations for operating well-architected Amazon Elastic VMware Service (EVS) workloads. The well-architected analysis assesses EVS configurations to help ensure your VMware environments are optimized for reliability, security, operational excellence, cost optimization, and performance efficiency. From the well-architected status tab in VMware, you'll find insights and recommendations to help implement well-architected best practices for your EVS environments.

The well-architected analysis categorizes configurations in the following pillars of the framework: *reliability* and *security*.

Reliability

Reliability ensures that workloads perform their intended functions correctly and consistently, even when there are disruptions.

- **EVS environment resiliency**

Ensure that your EVS cluster nodes are properly distributed across partition placement groups. All nodes should be members of a single partition placement group configured with four or more partitions. Proper partition placement ensures that your EVS cluster nodes are distributed across multiple fault-isolated hardware partitions within an AWS availability zone. Misalignment can result in significant loss of processing power or downtime if a partition fails.

Security

Security emphasizes protecting data, systems, and assets through risk assessments and mitigation strategies.

- **Cluster node management**

Ensure that your EVS cluster nodes have appropriate EC2 stop and termination protection configured. EVS ESXi nodes should be managed exclusively using vCenter or other VMware-level management tools. Without proper EC2-level protections, nodes could be accidentally stopped or terminated from the EC2 console, which can lead to virtual machine data unavailability or data loss.

Related information

- [Implement well-architected FSx for ONTAP file systems](#)
- [Implement well-architected database workloads](#)
- [Implement well-architected EVS configurations](#)

Configure NetApp Workload Factory notifications

You can configure the NetApp Workload Factory notification service to send notifications as alerts in the NetApp Console or to an Amazon SNS topic. Notifications sent as alerts appear in NetApp Console when you have a Console agent or link deployed. When Workload Factory publishes notifications to an Amazon SNS topic, subscribers to the topic (such as people or other applications) receive the notifications at the endpoints configured for the topic (such as email or SMS messages).

Notification types and messages

Workload Factory sends notifications for the following events:

Event	Description	Notification type	Severity	Workload	Resource type
Some database instances in your account are not well-architected	All Microsoft SQL Server instances in your account have been analyzed for well-architected issues. The description for this event gives the number of well-architected instances and unoptimized instances. Review well-architected status findings and recommendations in the Databases inventory from the Workload Factory console.	Well-architected	Recommendation	Databases	Microsoft SQL Server instance
Microsoft SQL Server/PostgreSQL server deployment succeeded	The deployment of the Microsoft SQL Server or PostgreSQL host succeeded. For more information, go to job monitoring.	Deployment	Success	Databases	FSx for ONTAP, DB host
Microsoft SQL Server/PostgreSQL server deployment failed	The deployment of the Microsoft SQL Server or PostgreSQL host failed. For more information, go to job monitoring.	Deployment	Error	Databases	FSx for ONTAP, DB host
Failed replication relationship creation	A SnapMirror replication relationship creation has failed. For more information, go to Tracker.	Replication	Critical	General storage	FSx for ONTAP
FSx for ONTAP creation failure	An FSx for ONTAP file system creation process has failed. For more information, go to Tracker.	FSx for ONTAP file system action	Critical	General storage	FSx for ONTAP
Automatic SSD capacity or inodes increase success	During a recent automatic capacity management update, the FSx for ONTAP file system either increased SSD capacity or volume inodes successfully. For more information, go to Tracker.	Capacity management	Success	General storage	FSx for ONTAP file
Automatic SSD capacity or inodes increase failure	During a recent automatic capacity management update, the FSx for ONTAP file system failed to increase SSD capacity or volume inodes. For more information, go to Tracker.	Capacity management	Critical	General storage	FSx for ONTAP file systems
FSx for ONTAP issue detected	All FSx for ONTAP file systems have been analyzed for well-architected issues. The scan detected one or more issues. For more information, review the well-architected analysis from the Storage dashboard in the Workload Factory console.	Well-architected analysis	Recommendation	General storage	FSx for ONTAP file systems

Event	Description	Notification type	Severity	Workload	Resource type
Automatic capacity management event for FSx for ONTAP	The SSD performance tier for the FSx for ONTAP file system reached the warning threshold capacity/percentage total.	Capacity management	Warning	General storage	FSx for ONTAP file systems
Automatic inodes management event for FSx for ONTAP	The inode count for the FSx for ONTAP volume reached the warning threshold count/percentage total.	Capacity management	Warning	General storage	FSx for ONTAP file systems

Configure Workload Factory notifications

Configure Workload Factory notifications using the NetApp Console or the Workload Factory console. If you use the NetApp Console, you can configure Workload Factory to send notifications as alerts in the NetApp Console or to an Amazon SNS topic. You can configure notifications from the **Notifications settings** in the NetApp Console.

Before you begin

- You need to configure Amazon SNS and create Amazon SNS topics using either the Amazon SNS console or the AWS CLI.
- Note that Workload Factory supports the **Standard** topic type. This type of topic does not ensure that notifications are sent to subscribers in the order in which they were received, so consider this if you have critical or emergency notifications.

Configure notifications from NetApp Console

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads, Administration**, and then **Notifications setup**.
3. On the Notifications setup page, do the following:
 - a. Optional: Select **Enable NetApp Console notifications** to configure Workload Factory to send notifications in the NetApp Console.
 - b. Select **Enable SNS notifications**.
 - c. Follow the instructions to configure Amazon SNS from the Amazon SNS console.

After you create the topic, copy the topic ARN and enter it in the **SNS topic ARN** field on the **Notifications setup** page.

4. After you verify the configuration by sending a test notification, select **Apply**.

Result

Workload Factory is configured to send notifications to the Amazon SNS topic that you specified.

Configure notifications from Workload Factory console

Steps

1. Log in to the [Workload Factory console](#).
2. From the Workload Factory console menu, select **Workloads, Administration**, and then **Notifications setup**.
3. Select **Enable SNS notifications**.
4. Follow the instructions to configure Amazon SNS from the Amazon SNS console.
5. After you verify the configuration by sending a test notification, select **Apply**.

Result

Workload Factory is configured to send notifications to the Amazon SNS topic that you specified.

Subscribe to the Amazon SNS topic

After you configure Workload Factory to send notifications to a topic, follow the [Instructions](#) in the Amazon SNS documentation to subscribe to the topic so that you can receive notifications from Workload Factory.

Filter notifications

You can reduce unnecessary notification traffic and target specific notification types for specific users by applying filters to the notifications. You can do this using an Amazon SNS policy for SNS notifications, and using the notifications settings in the NetApp Console.

Filter Amazon SNS notifications

When you subscribe to an Amazon SNS topic, you receive all notifications published to that topic by default. If you want to receive only specific notifications from the topic, you can use a filter policy to control which notifications you receive. Filter policies cause Amazon SNS to deliver only the notifications that match the filter policy to the subscriber.

You can filter Amazon SNS notifications by the following criteria:

Description	Filter policy field name	Possible values
Resource type	resourceType	<ul style="list-style-type: none">• DB• Microsoft SQL Server host• PostgreSQL Server host
Workload	workload	WLMDB
Priority	priority	<ul style="list-style-type: none">• Success• Info• Recommendation• Warning• Error• Critical
Notification type	notificationType	<ul style="list-style-type: none">• Deployment• Well-architected

Steps

1. In the Amazon SNS console, edit the subscription details for the SNS topic.
2. In the **Subscription filter policy** area, select to filter by **Message attributes**.
3. Enable the **Subscription filter policy** option.
4. Enter a JSON filter policy in the **JSON editor** box.

For example, the following JSON filter policy accepts notifications from the Microsoft SQL Server resource that are related to the WLMDB workload, have a priority of Success or Error, and provide details on Well-architected status:

```
{  
  "accountId": [  
    "account-a"  
  ],  
  "resourceType": [  
    "Microsoft SQL Server host"  
  ],  
  "workload": [  
    "WLMDB"  
  ],  
  "priority": [  
    "Success",  
    "Error"  
  ],  
  "notificationType": [  
    "Well-architected"  
  ]  
}
```

5. Select **Save changes**.

For other examples of filter policies, refer to [Amazon SNS example filter policies](#).

For further information about creating filter policies, refer to the [Amazon SNS documentation](#).

Filter notifications in the NetApp Console

You can use the NetApp Console notifications settings to filter notifications that you receive in the Console by severity level, such as Critical, Info, or Warning.

For more information about filtering notifications in the Console, refer to the [NetApp Console documentation](#).

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 NetApp Workload Factory. Codebox is aligned with the Workload Factory permission policies 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 customizable. 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
- Terraform

Related information

[Learn how to use Codebox](#).

[Workload Factory REST API documentation](#).

Use Codebox for automation in NetApp Workload Factory

You can use Codebox to generate the code needed to execute any operation supported by NetApp 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 permission policies 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.

The screenshot shows the AWS Workload Factory UI for creating a Microsoft SQL server. On the left, the 'Create new Microsoft SQL server' configuration page is displayed, showing fields for Region & VPC (us-east-1 | US East (N. Virginia), VPC-1 | 172.30.0.0/20), Availability zones, Cluster configuration for Node 1 and Node 2, and a Security group. On the right, the 'Codebox' interface shows a 'Create database' section with a 'REST API' tab. A 'curl' command is displayed, and a 'Copy' button is highlighted with a green box and arrow. Green arrows also point from the configuration fields in the UI to the corresponding code in the 'Codebox' command.

```

curl --location --request POST https://api.workloads.netapp.com/accounts/acc
--header 'Authorization: Bearer <Token> \
--header 'Content-Type: application/json' \
--data-raw '{
  "networkConfiguration": {
    "vpclId": "vpc-7d4a2818",
    "vpcCidr": "172.30.0.0/20",
    "availabilityZone1": "us-east-1d",
    "privateSubnet1Id": "subnet-5a37222d",
    "routeTable1Id": "rtb-0de1132a1c54f5e6",
    "availabilityZone2": "us-east-2d",
    "privateSubnet2Id": "subnet-74a1b303",
    "routeTable2Id": "rtb-00d7acd615fac5414",
  },
  "ec2Configuration": {
    "workloadInstanceType": "m5.xlarge",
    "keyPairName": "Key-Pair-1",
  }
}'
```

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 Workload Factory console 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 Workload Factory console 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 Workload Factory console 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 Workload Factory console 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 NetApp Workload Factory

Open CloudShell to execute AWS or ONTAP CLI commands from anywhere in the NetApp Workload Factory console.

About this task

CloudShell allows you to execute AWS CLI commands or ONTAP CLI commands in a shell-like environment from within the Workload Factory console. 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 NetApp 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 NetApp 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 NetApp 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>`.

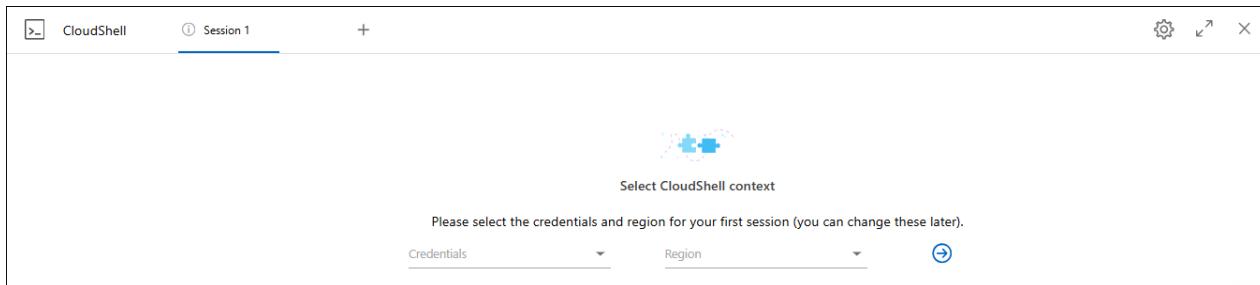
Deploy CloudShell

You can deploy CloudShell from anywhere in the NetApp Workload Factory console. You can also deploy CloudShell from the NetApp Console.

Deploy from Workload Factory console

Steps

1. Log in to the [Workload Factory console](#).
2. From the menu, select **Administration** and then **CloudShell**.
3. In the CloudShell window, select credentials and region for the CloudShell session and then select the arrow to continue.



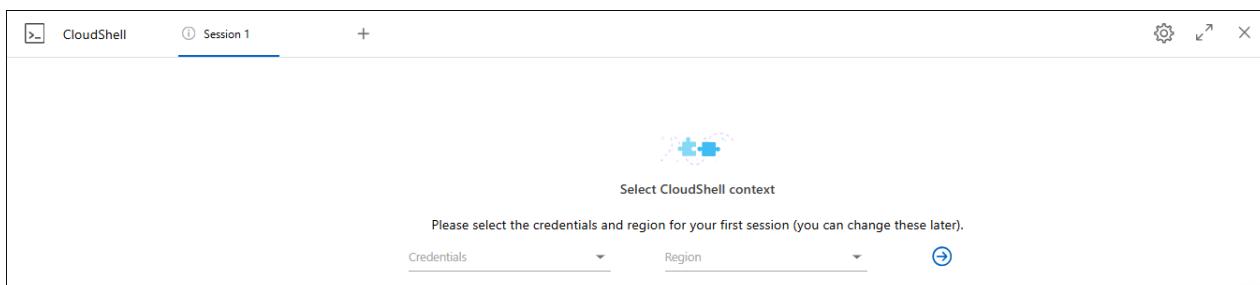
4. Enter `help` to view available [CloudShell commands](#) and instructions or refer to the following CLI reference documents for available commands:
 - [AWS CLI reference](#): For commands related to FSx for ONTAP, select **fsx**.
 - [ONTAP CLI reference](#)
5. Issue commands within the CloudShell session.

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 the NetApp Console

Steps

1. Log in to the [NetApp Console](#).
2. From the menu, select **Workloads** and then **Administration**.
3. From the Administration menu, select **CloudShell**.
4. In the CloudShell window, select credentials and region for the CloudShell session and then select the arrow to continue.



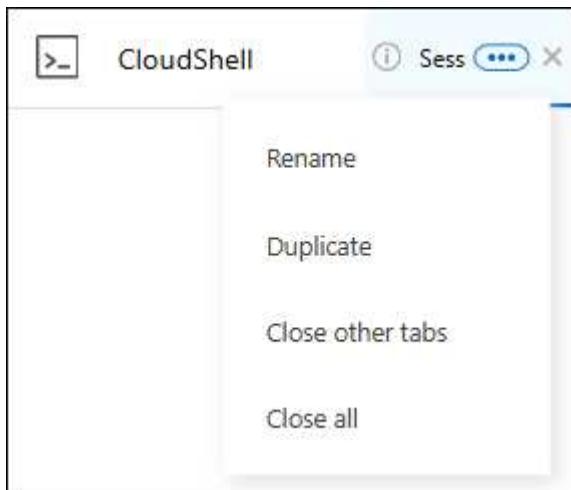
5. Enter `help` to view available CloudShell commands and instructions or refer to the following CLI reference documents for available commands:
 - [AWS CLI reference](#): For commands related to FSx for ONTAP, select **fsx**.

- [ONTAP CLI reference](#)

6. 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 actions 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 actions 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 actions 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 actions 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

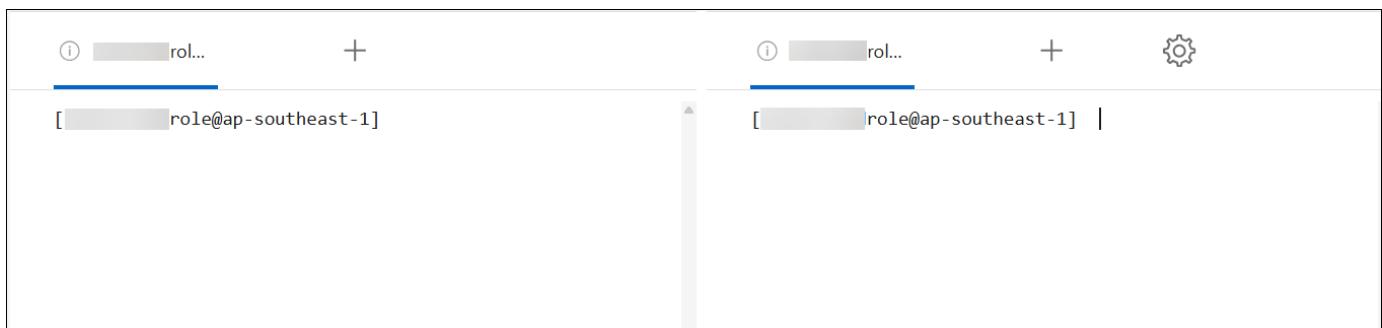
The selected CloudShell session tabs close.

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.



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 NetApp 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. From the menu, select **Administration** and then **Credentials**.
3. On the **Credentials** page, do the following:
 - In the Workload Factory console, select the action menu for a set of credentials and then select **Remove**. Select **Remove** to confirm.
 - In the NetApp Console, select the action menu for a set of credentials and then select **Delete**. Select **Delete** to confirm.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to NetApp Workload Factory and its storage solutions and services. You must register for support from the NetApp 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 960xxxxxxxxx serial number located on the Support Resources page in the NetApp Console) serves as your single support subscription ID. Each NetApp 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 the NetApp Console 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 NetApp Console login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

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

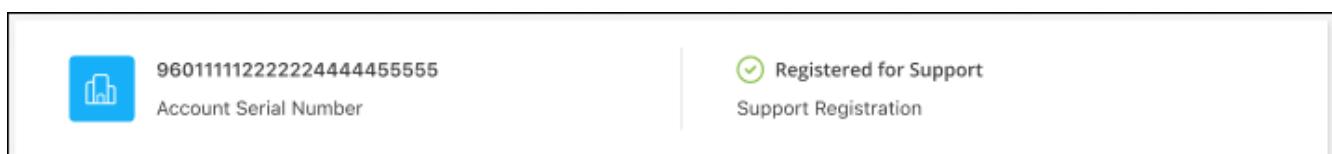
Steps

1. In the upper right of the Workload Factory console, select **Help > Support**.

Selecting this option opens the NetApp Console in a new browser tab and loads the Support dashboard.

2. From the NetApp Console menu, select **Administration**, and then 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 NetApp Console users will not see this same support registration status if they have not associated a NetApp Support Site account with their NetApp Console login. However, that doesn't mean that your NetApp 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 NetApp Console login.

Steps

1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the NetApp 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 NetApp Console login by completing the steps under [Existing customer with an NSS account](#).

Brand new to NetApp

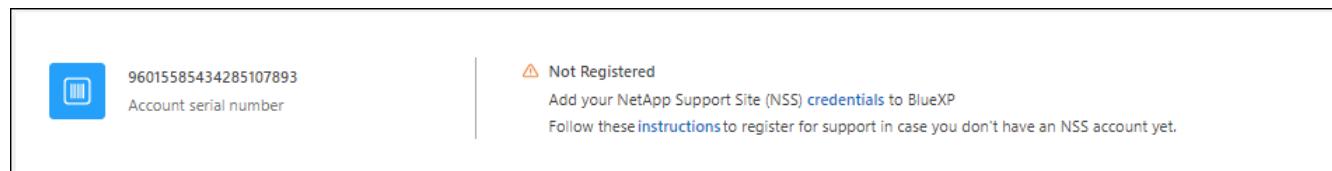
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the Workload Factory console, select **Help > Support**.

Selecting this option opens the NetApp Console in 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 NetApp Console login by completing the steps under [Existing customer with an NSS account](#).

Get help

NetApp provides support for 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 NetApp Console in 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.

ntapitdemo 

NetApp Support Site Account

Service Working Environment

Select Select

Case Priority i

Low - General guidance

Issue Description

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

Additional Email Addresses (Optional) i

Type here

Attachment (Optional) Upload  i

No files selected 

After you finish

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

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

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

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

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the NetApp Console account serial number (ie. 960xxxx) or the system 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 the NetApp Console. 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**.

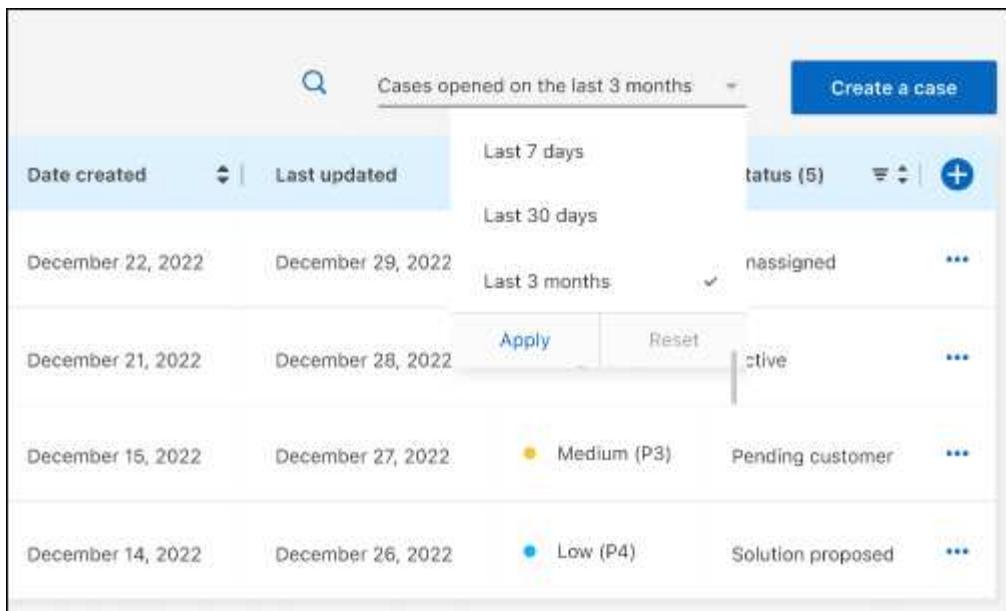
Selecting this option opens the NetApp Console a new browser tab and loads the Support dashboard.

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

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

3. Optionally modify the information that displays in the table:

- Under **Organization's cases**, select **View** to view all cases associated with your company.
- Modify the date range by choosing an exact date range or by choosing a different time frame.



Search: Cases opened on the last 3 months

Create a case

Date created: December 22, 2022 | Last updated: December 29, 2022 | Status (5):

Last 7 days | Last 30 days | Last 3 months

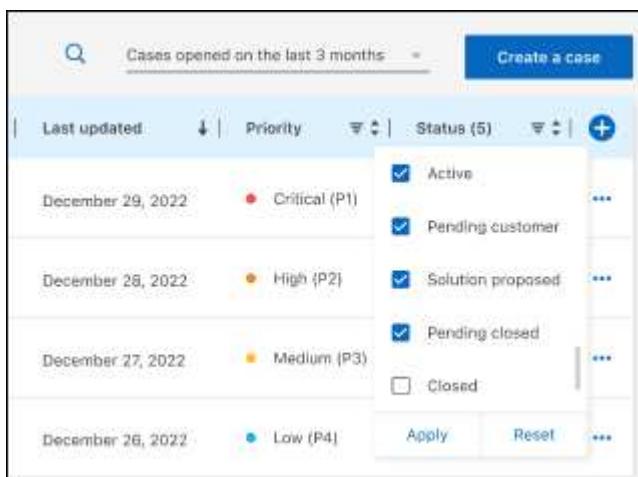
Assigned | Active | Pending customer | Pending closed | Closed

December 21, 2022 | December 28, 2022 | Apply | Reset

December 15, 2022 | December 27, 2022 | Medium (P3)

December 14, 2022 | December 26, 2022 | Low (P4)

- Filter the contents of the columns.



Search: Cases opened on the last 3 months

Create a case

Last updated: December 29, 2022 | Priority: Critical (P1) | Status (5):

Active (selected) | Pending customer | Solution proposed | Pending closed | Closed

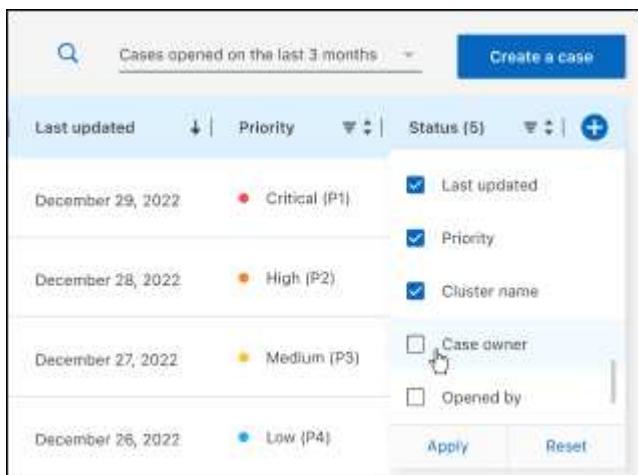
December 28, 2022 | High (P2)

December 27, 2022 | Medium (P3)

December 26, 2022 | Low (P4)

Apply | Reset

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



Search: Cases opened on the last 3 months

Create a case

Last updated: December 29, 2022 | Priority: Critical (P1) | Status (5):

Last updated | Priority | Cluster name

December 28, 2022 | High (P2) | Case owner | Opened by

December 27, 2022 | Medium (P3)

December 26, 2022 | Low (P4)

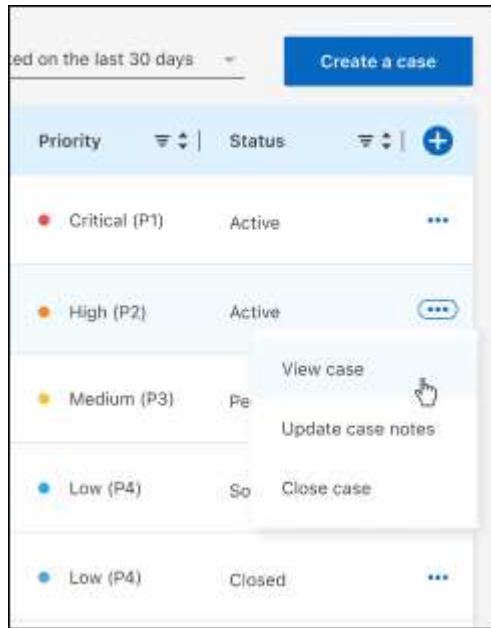
Apply | Reset

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

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

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

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



Legal notices for NetApp 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.

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

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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