Learn the basics

Setup and administration

NetApp
February 02, 2026

Table of Contents

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 organizations chatbot sources and the AI Engine databases. This allows you to embed your organization’s unstructured data into an enterprise chatbot application.

Savings calculators to save costs

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

Service accounts to promote automation

Use service accounts to automate 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.

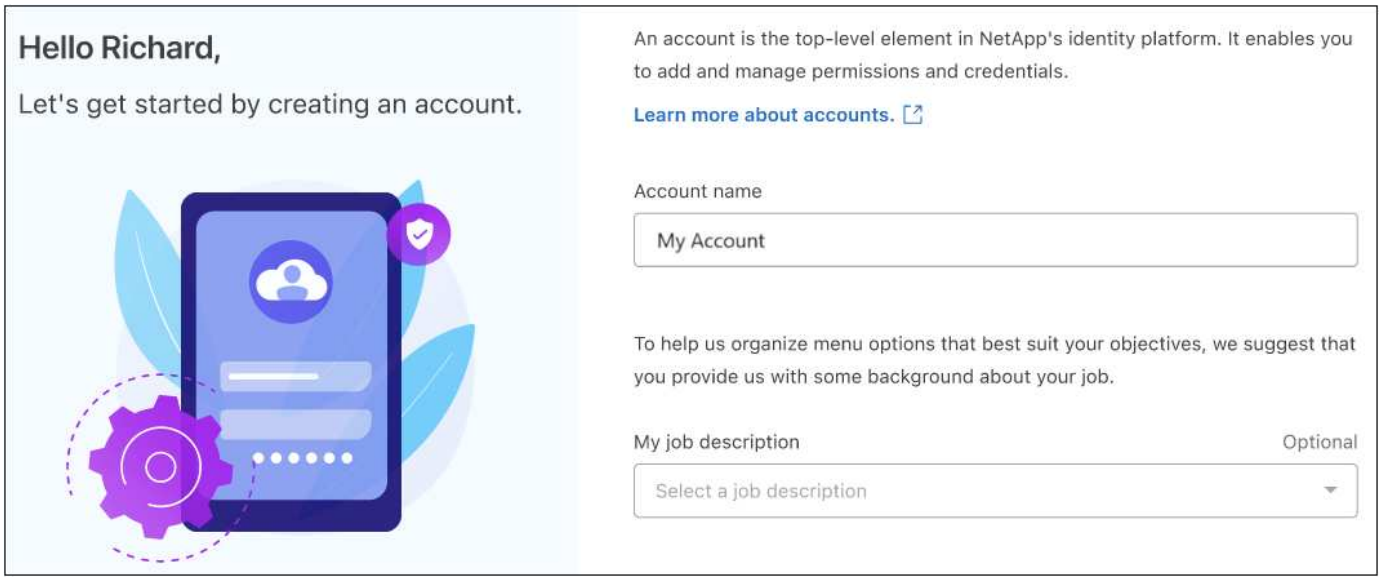
Software-as-a-service

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.



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, copiable 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	• Deployment • Explore savings	File system creation and deletion
	ec2:DescribeSubnets	• Deployment • Explore savings	File system creation and deletion
	ec2:DescribeSecurityGroups	• Deployment • Explore savings	File system creation and deletion
	ec2:DescribeRouteTables	• Deployment • Explore savings	File system creation and deletion
	ec2:DescribeNetworkInterfaces	• Deployment • Explore savings	File system creation and deletion
	ec2:DescribeVolumeStatus	• 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	• 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:InvokeModelWihResponseStream	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	s3:GetObjectTagging	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: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:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
```

```
                "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	• 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	• Inventory • Explore savings	View, planning, and analysis
	ec2:DescribeKeyPairs	Deployment	View, planning, and analysis
	ec2:DescribeNetworkInterfaces	Deployment	View, planning, and analysis
	ec2:DescribeInstanceTypes	• Deployment • Explore savings	View, planning, and analysis
Get details to fill in the FSx for ONTAP deployment form	ec2:DescribeVpcs	• Deployment • Inventory	View, planning, and analysis
	ec2:DescribeSubnets	• 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	• 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	• 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	• 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	• Inventory • Explore Savings	View, planning, and analysis
	fsx:DescribeBackups	• Inventory • Explore Savings	View, planning, and analysis
	fsx:DescribeStorageVirtualMachines	• Deployment • Management operations • Inventory	View, planning, and analysis
	fsx:DescribeFileSystems	• 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	• Management operations • Inventory • Explore savings • Optimization	View, planning, and analysis
Send commands over SSM to EC2 instances for discovery and management	ssm:SendCommand	• Management operations • Inventory • Explore savings • Optimization	View, planning, and analysis
Get the SSM connectivity status on instances post deployment	ssm:GetConnectionStatus	• 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	• 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	• Explore savings • Optimization	Database host creation
Get recommendation preferences that are in effect for a given resource from AWS Compute Optimizer	compute-optimizer:GetEffectiveRecommendationPreferences	• Explore savings • Optimization	Database host creation
Fetch recommendations that AWS Compute Optimizer generates for Amazon Elastic Compute Cloud (Amazon EC2) instances	compute-optimizer:GetEC2InstanceRecommendations	• Explore savings • Optimization	Database host creation
Check for instance association to auto-scaling groups	autoscaling:DescribeAutoScalingGroups	• Explore savings • Optimization	Database host creation
	autoscaling:DescribeAutoScalingInstances	• 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]	• Deployment • Management operations • Inventory	View, planning, and analysis
	ssm:GetParameters [1]	• Deployment • Management operations • Inventory	View, planning, and analysis
	ssm:PutParameter [1]	• Deployment • Management operations	View, planning, and analysis
	ssm:DeleteParameters [1]	• 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]	• 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	• 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	• 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	• 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	• 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	• 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
Required SSM permissions to run the discovery script on provisioned SQL instances and to fetch latest list of FSx for ONTAP supported AWS regions.	ssm: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:AWSServiceName": "ec2.amazonaws.com"*
3. "iam:PassRole" limited by "iam:PassedToService": "ec2.amazonaws.com"*

Permissions for GenAI workloads

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

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

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

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

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

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

Purpose	Action	Where used	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	• Deployment • Inventory	View, planning, and analysis
Get the subnets in selected environment to complete deployment form	ec2:DescribeSubnets	• 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	• 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	• Deployment • Management operations	Datastore deployment and connectivity
Get Amazon FSx for NetApp ONTAP details	fsx:Describe*	• 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	• 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:GetModelInvocationLoggingConfiguration`

- `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`.

Copyright information

Trademark information