# Aprenda lo básico

## Setup and administration

NetApp
February 02, 2026

# Tabla de contenidos

# Aprenda lo básico

## Obtenga más información sobre NetApp Workload Factory

NetApp Workload Factory es una potente plataforma de gestión del ciclo de vida diseñada para ayudarlo a optimizar sus cargas de trabajo utilizando Amazon FSx for NetApp ONTAP . Las cargas de trabajo que se pueden optimizar con Workload Factory y FSx para ONTAP incluyen bases de datos, migraciones de VMware a VMware Cloud en AWS, chatbots de IA y más.

Una *carga de trabajo* abarca una combinación de recursos, código y servicios o aplicaciones, diseñados para alcanzar un objetivo comercial. Esto podría ser cualquier cosa, desde una aplicación orientada al cliente hasta un proceso backend. Las cargas de trabajo pueden involucrar un subconjunto de recursos dentro de una sola cuenta de AWS o abarcar varias cuentas.

Amazon FSx for NetApp ONTAP proporciona volúmenes de almacenamiento NFS, SMB/CIFS e iSCSI totalmente administrados y nativos de AWS para aplicaciones de misión crítica, bases de datos, contenedores, almacenes de datos de VMware Cloud y archivos de usuario. Puede administrar FSx para ONTAP a través de Workload Factory y utilizando herramientas de administración nativas de AWS.

### Funciones

La plataforma Workload Factory ofrece las siguientes capacidades principales.

**Almacenamiento flexible y de bajo coste**

Detecta, implementa y gestiona los sistemas de archivos de Amazon FSx para NetApp ONTAP en la nube. FSX para ONTAP incorpora todas las funcionalidades de ONTAP en un servicio gestionado de AWS nativo que ofrece una experiencia de nube híbrida constante.

**Migra los entornos vSphere on-premises a VMware Cloud on AWS**

El asesor de migración de VMware Cloud on AWS le permite analizar sus configuraciones de máquinas virtuales actuales en entornos vSphere locales, generar un plan para implementar diseños de máquinas virtuales recomendados en VMware Cloud on AWS y utilizar sistemas de archivos personalizados de Amazon FSx para NetApp ONTAP como almacenes de datos externos.

**Gestión del ciclo de vida de las bases de**

Detecte cargas de trabajo de bases de datos y analice el ahorro de costes con Amazon FSx para NetApp ONTAP; aproveche las ventajas de almacenamiento y aplicaciones al migrar bases de datos de SQL Server a FSx para almacenamiento de ONTAP; ponga en marcha servidores SQL, bases de datos y clones de bases de datos que implementen prácticas recomendadas de proveedores; utilice un piloto conjunto de Infraestructura como código para automatizar operaciones; y supervise y optimice continuamente las propiedades de SQL Server para mejorar el rendimiento, la disponibilidad, la protección y la rentabilidad.

**Desarrollo de bots conversacionales de IA**

Aprovecha tus sistemas de archivos FSx para ONTAP para almacenar las fuentes de chatbot de tu organización y las bases de datos del motor de IA. Esto le permite integrar los datos no estructurados de su organización en una aplicación de chatbot empresarial.

**Calculadoras de ahorro para ahorrar costes**

Analiza tus implementaciones actuales con el almacenamiento de Amazon Elastic Block Store (EBS) o Elastic File System (EFS), o Amazon FSx para el servidor de archivos de Windows, para descubrir cuánto

dinero puedes ahorrar al pasar a Amazon FSx para NetApp ONTAP. También puede utilizar la calculadora para realizar un escenario hipotético de una puesta en marcha futura que esté planificando.

**Cuentas de servicio para promover la automatización**

Utilice cuentas de servicio para automatizar las operaciones de NetApp Workload Factory de forma segura y confiable. Las cuentas de servicio proporcionan una automatización confiable y duradera sin restricciones de administración de usuarios y son más seguras porque solo brindan acceso a la API.

**Asistente de inteligencia artificial Ask Me**

Haga preguntas al asistente de IA sobre la administración y el funcionamiento de FSx para sistemas de archivos ONTAP . Al utilizar el Protocolo de contexto de modelo (MCP), Ask Me interactúa de forma segura con entornos externos y consulta herramientas API para brindar respuestas adaptadas a su entorno de almacenamiento específico.

## Proveedores de cloud compatibles

Workload Factory le permite administrar el almacenamiento en la nube y utilizar las capacidades de carga de trabajo en Amazon Web Services.

## Seguridad

La seguridad de NetApp Workload Factory es una prioridad máxima para NetApp. Todas las cargas de trabajo en Workload Factory se ejecutan en Amazon FSx for NetApp ONTAP. Además de todo "Funciones de seguridad de AWS"NetApp Workload Factory ha recibido "Cumplimiento de SOC2 Tipo 1, Cumplimiento de SOC2 Tipo 2 y Cumplimiento de HIPAA".

Amazon FSx for NetApp ONTAP para NetApp Workload Factory es una"Solución de AWS para implementar aplicaciones empresariales" que fue creado teniendo en mente las mejores prácticas bien diseñadas.

## Coste

Workload Factory es de uso gratuito. El costo que paga a Amazon Web Services (AWS) depende de los servicios de almacenamiento y carga de trabajo que planea implementar. Esto incluye el costo de Amazon FSx for NetApp ONTAP , la infraestructura de VMware Cloud on AWS, los servicios de AWS y más.

## Cómo funciona Workload Factory

Workload Factory incluye una consola basada en web que se proporciona a través de la capa SaaS, una cuenta, modos operativos que controlan el acceso a su patrimonio en la nube, enlaces que brindan conectividad segregada entre Workload Factory y una cuenta de AWS, y más.

### Software como servicio

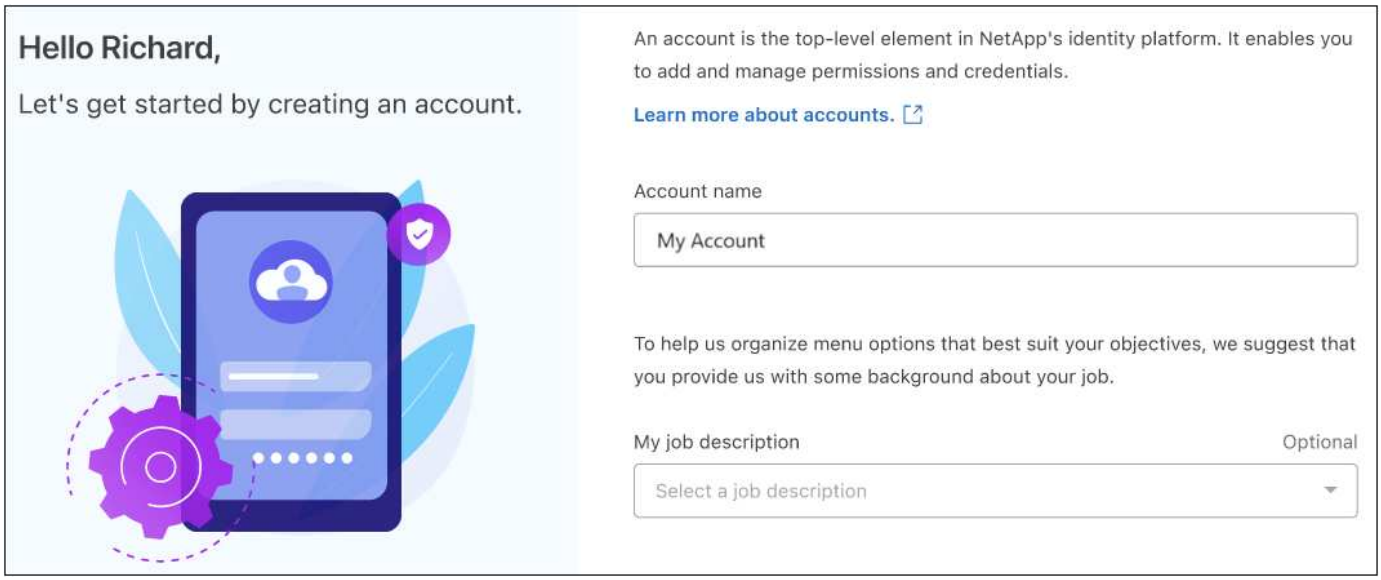
Se puede acceder a Workload Factory a través de"Consola de NetApp Workload Factory" y el"Consola de NetApp" . Estas experiencias SaaS le permiten acceder automáticamente a las últimas funciones a medida que se lanzan y cambiar fácilmente entre sus cuentas y enlaces de Workload Factory.

"Obtenga más información sobre las diferentes experiencias de consola"

### Cuentas

Cuando inicia sesión en Workload Factory por primera vez, se le solicitará que cree una cuenta. Esta cuenta le permite organizar sus recursos, cargas de trabajo y acceso a las cargas de trabajo para su organización

mediante credenciales.




Cuando crea una cuenta, usted es el usuario *account admin* único de esa cuenta.

Si su organización requiere una cuenta adicional o administración de usuarios, comuníquese con nosotros mediante el chat del producto.

Si usa la consola de NetApp , ya pertenecerá a una cuenta porque Workload Factory aprovecha las cuentas de NetApp .

#### Cuentas de servicio

Una cuenta de servicio actúa como un "usuario" que puede realizar llamadas API autorizadas a NetApp Workload Factory para fines de automatización. Esto facilita la gestión de la automatización porque no es necesario crear scripts de automatización basados en la cuenta de usuario de una persona real que puede abandonar la empresa en cualquier momento. Todos los titulares de cuentas en Workload Factory se consideran administradores de cuentas. Los administradores de cuentas pueden crear y eliminar varias cuentas de servicio.

"Aprenda a administrar cuentas de servicio"

### Permisos

Workload Factory proporciona políticas de permisos flexibles que le permiten controlar cuidadosamente el acceso a su entorno en la nube y asignar un nivel de confianza incremental a Workload Factory en función de sus políticas de TI.

"Obtenga más información sobre las políticas de permisos de Workload Factory."

### Enlaces de conectividad

Un vínculo de Workload Factory crea una relación de confianza y conectividad entre Workload Factory y uno o más sistemas de archivos FSx para ONTAP . Esto le permite monitorear y administrar ciertas características del sistema de archivos directamente desde las llamadas API REST de ONTAP que no están disponibles a través de la API de Amazon FSx para ONTAP .

No necesita un enlace para comenzar a usar Workload Factory, pero en algunos casos necesitará crear un

enlace para desbloquear todas las funciones y capacidades de carga de trabajo de Workload Factory.

Los enlaces aprovechan actualmente AWS Lambda.

"Más información sobre Links"

#### Automatización de CodeBox

Codebox es un copiloto de Infraestructura como Código (IaC) que ayuda a los desarrolladores e ingenieros de DevOps a generar el código necesario para ejecutar cualquier operación compatible con Workload Factory. Los formatos de código incluyen la API REST de Workload Factory, AWS CLI y AWS CloudFormation.

Codebox está alineado con los modos de operación de Workload Factory (*básico*, *solo lectura* y *lectura/escritura*) y establece una ruta clara para la preparación de la ejecución, así como un catálogo de automatización para una rápida reutilización futura.

El panel CodeBox muestra el IAC generado por una operación de flujo de trabajo específica, y coincide con un asistente gráfico o una interfaz de chat conversacional. Si bien CodeBox admite codificación de colores y búsqueda para facilitar la navegación y el análisis, no permite la edición. Sólo puede copiar o guardar en el catálogo de automatización.

"Más información sobre CodeBox"

#### Calculadoras de ahorro

Workload Factory ofrece calculadoras de ahorro para que pueda comparar los costos de sus entornos de almacenamiento, bases de datos o cargas de trabajo de VMware en los sistemas de archivos FSx para ONTAP con otros servicios de Amazon. Dependiendo de sus requisitos de almacenamiento, es posible que descubra que los sistemas de archivos FSx para ONTAP son la opción más rentable para usted.

- "Descubra cómo analizar el ahorro para sus entornos de almacenamiento"
- "Aprenda a analizar el ahorro para sus cargas de trabajo de base de datos"
- "Descubra cómo explorar los ahorros para sus cargas de trabajo de VMware"

#### Cargas de trabajo bien diseñadas

Workload Factory le ayuda a mantener y operar configuraciones de almacenamiento y bases de datos confiables, seguras, eficientes y rentables que se alinean con AWS Well-Architected Framework. Workload Factory escanea FSx diariamente en busca de sistemas de archivos ONTAP , SQL Server e implementaciones de bases de datos Oracle para brindar información sobre posibles configuraciones incorrectas y recomienda acciones manuales o automatizadas para solucionar problemas.

"Obtenga más información sobre cargas de trabajo bien diseñadas"

## Herramientas para utilizar NetApp Workload Factory

Puede utilizar NetApp Workload Factory con las siguientes herramientas:

- **Consola Workload Factory**: La consola Workload Factory proporciona una vista visual y holística de sus aplicaciones y proyectos.
- *Consola NetApp *: La consola NetApp proporciona una experiencia de interfaz híbrida para que pueda utilizar Workload Factory junto con otros servicios de datos de NetApp .
- **Pregúntame**: utiliza el asistente de IA Pregúntame para hacer preguntas y obtener más información sobre

Workload Factory sin salir de la consola de Workload Factory. Accede a Pregúntame desde el menú de ayuda de Workload Factory.

- **CloudShell CLI**: Workload Factory incluye una CLI de CloudShell para administrar y operar entornos de AWS y NetApp en todas las cuentas desde una única CLI basada en navegador. Acceda a CloudShell desde la barra superior de la consola de Workload Factory.
- **API REST**: utilice las API REST de Workload Factory para implementar y administrar sus sistemas de archivos FSx para ONTAP y otros recursos de AWS.
- **CloudFormation**: use el código de AWS CloudFormation para realizar las acciones que definió en la consola de Workload Factory para modelar, aprovisionar y administrar recursos de AWS y de terceros desde la pila de CloudFormation en su cuenta de AWS.
- **Proveedor de Terraform NetApp Workload Factory**: utilice Terraform para crear y administrar flujos de trabajo de infraestructura generados en la consola de Workload Factory.

#### API de REST

Workload Factory le permite optimizar, automatizar y operar sus sistemas de archivos FSx for ONTAP para cargas de trabajo específicas. Cada carga de trabajo expone una API REST asociada. En conjunto, estas cargas de trabajo y API forman una plataforma de desarrollo flexible y extensible que puede utilizar para administrar sus sistemas de archivos FSx para ONTAP .

Existen varios beneficios al utilizar las API REST de Workload Factory:

- Las API se han diseñado en función de la tecnología REST y de las mejores prácticas actuales. Las tecnologías centrales incluyen HTTP y JSON.
- La autenticación de Workload Factory se basa en el estándar OAuth2. NetApp se basa en la implementación del servicio Auth0.
- La consola basada en web de Workload Factory utiliza las mismas API REST principales, por lo que existe coherencia entre las dos rutas de acceso.

"Ver la documentación de la API REST de Workload Factory"

# Experiencias de consola

Se puede acceder a NetApp Workload Factory a través de dos consolas basadas en web. Aprenda cómo acceder a Workload Factory mediante la consola de Workload Factory y la consola de NetApp .

- *Consola NetApp *: ofrece una experiencia híbrida donde puede administrar sus sistemas de archivos FSx para ONTAP y cargas de trabajo que se ejecutan en Amazon FSx for NetApp ONTAP en el mismo lugar.
- **Consola Workload Factory**: ofrece una experiencia de Workload Factory dedicada y enfocada en cargas de trabajo que se ejecutan en Amazon FSx for NetApp ONTAP.

## Acceda a Workload Factory en la consola de NetApp

Puede acceder a Workload Factory desde la NetApp Console. Además de utilizar Workload Factory para las capacidades de almacenamiento y carga de trabajo de AWS, también puede acceder a otros servicios de datos como NetApp Copy and Sync y más.

#### Pasos

1. Iniciar sesión en el"Consola de NetApp" .
2. Desde el menú de la consola de NetApp , seleccione **Cargas de trabajo** y luego **Descripción general**.

### Acceda a Workload Factory en la consola de Workload Factory

Puede acceder a Workload Factory desde la consola de Workload Factory.

**Paso**

1. Iniciar sesión en el"Consola de Workload Factory" .

# Permisos para NetApp Workload Factory

Para utilizar las funciones y los servicios de NetApp Workload Factory, deberá proporcionar permisos para que Workload Factory pueda realizar operaciones en su entorno de nube.

## Por qué usar permisos

Cuando otorgas permisos, Workload Factory adjunta una política a la instancia con permisos para administrar recursos y procesos dentro de esa cuenta de AWS. Esto permite a Workload Factory ejecutar diversas operaciones, desde el descubrimiento de sus entornos de almacenamiento hasta la implementación de recursos de AWS, como sistemas de archivos en la administración del almacenamiento o bases de conocimiento para cargas de trabajo de GenAI.

Por ejemplo, para las cargas de trabajo de bases de datos, cuando se le otorgan a Workload Factory los permisos necesarios, escanea todas las instancias de EC2 en una cuenta y región determinadas, y filtra todas las máquinas basadas en Windows. Si el agente de AWS Systems Manager (SSM) está instalado y ejecutándose en el host y la red de System Manager está configurada correctamente, Workload Factory puede acceder a la máquina Windows y verificar si el software de SQL Server está instalado o no.

## Permisos por carga de trabajo

Cada carga de trabajo utiliza permisos para realizar ciertas tareas en Workload Factory. Los permisos se agrupan en políticas de permisos predefinidas. Desplácese hasta la carga de trabajo que utiliza para obtener información sobre las políticas de permisos, un JSON copiable para las políticas de permisos y una tabla que enumera todos los permisos, su propósito, dónde se utilizan y qué políticas de permisos los admiten.

#### Permisos para almacenamiento

Las políticas de IAM disponibles para Storage proporcionan los permisos que Workload Factory necesita para administrar recursos y procesos dentro de su entorno de nube pública.

El almacenamiento ofrece las siguientes políticas de permisos para elegir:

- **Visualización, planificación y análisis**: Visualice los sistemas de archivos FSx para ONTAP , conozca el estado del sistema, obtenga un análisis bien diseñado para sus sistemas y explore las posibilidades de ahorro.
- **Operaciones y corrección**: Realice tareas operativas como ajustar la capacidad del sistema de archivos y solucionar problemas en las configuraciones de su sistema de archivos.
- **Creación y eliminación de sistemas de archivos**: Crear y eliminar sistemas de archivos FSx para ONTAP y máquinas virtuales de almacenamiento.

Consulte las políticas IAM requeridas:

## Políticas de IAM para almacenamiento

**Visualización, planificación y análisis**

```
{
  "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": "*"
    }
  ]
}
```

**Operaciones y remediación**

```
{
  "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": "*"
    }
  ]
}
```

**Creación y eliminación de archivos**

```
{
  "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": "*"
    }
  ]
}
```

La siguiente tabla muestra los permisos para Storage.

**Tabla de permisos para almacenamiento**

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Crea un sistema de archivos FSx for ONTAP | fsx:CreateFileSystem | Puesta en marcha | Creación y eliminación de archivos |
| Cree un grupo de seguridad para un sistema de archivos FSx for ONTAP | ec2:CreateSecurityGroup | Puesta en marcha | Creación y eliminación de archivos |
| Agregue etiquetas a un grupo de seguridad para un sistema de archivos FSx para ONTAP | ec2:CreateTags | Puesta en marcha | Creación y eliminación de archivos |
| Autorizar la salida e ingreso de grupos de seguridad para un sistema de archivos FSx para ONTAP | ec2:AuthorizeSecurityGroupEgress | Puesta en marcha | Creación y eliminación de archivos |
| | ec2:AuthorizeSecurityGroupIngress | Puesta en marcha | Creación y eliminación de archivos |
| El rol otorgado proporciona comunicación entre FSx para ONTAP y otros servicios de AWS | iam:CreateServiceLinkedIn | Puesta en marcha | Creación y eliminación de archivos |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Consulta los detalles que necesitas para rellenar el formulario de puesta en marcha del sistema de archivos FSx para ONTAP | ec2:DescribeVpcs | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| | ec2:DescribeSubnets | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| | ec2:DescribeSecurityGroups | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| | ec2:DescribeRouteTables | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| | ec2:DescribeNetworkinterfaces | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| | EC2:DescripbeVolumeStatus | • Puesta en marcha<br>• Explora el ahorro | Creación y eliminación de archivos |
| Obtén los detalles clave de KMS y utilízalos para el cifrado FSx para ONTAP | Kms:CreateGrant | Puesta en marcha | Creación y eliminación de archivos |
| | Km:DescripbeKey | Puesta en marcha | Creación y eliminación de archivos |
| | Km:ListKeys | Puesta en marcha | Creación y eliminación de archivos |
| | Kms:ListAliases | Puesta en marcha | Creación y eliminación de archivos |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Obtenga detalles de volumen para las instancias de EC2 | ec2:DescribeVolumes | • Inventario<br>• Explora el ahorro | Visualización, planificación y análisis |
| Obtenga detalles para las instancias de EC2 | ec2:DescribInstances | Explora el ahorro | Visualización, planificación y análisis |
| Describa Elastic File System en la calculadora de ahorro | Sistema de archivos elástico: Describir sistemas de archivos | Explora el ahorro | Visualización, planificación y análisis |
| Enumera las etiquetas de los recursos de FSx for ONTAP | fsx:ListTagsForResource | Inventario | Visualización, planificación y análisis |
| Gestionar la salida y el ingreso de grupos de seguridad para un sistema de archivos FSx para ONTAP | ec2:RevokeSecurityGroupIngress | Operaciones de gestión | Creación y eliminación de archivos |
| | ec2: Revocar la salida del grupo de seguridad | Operaciones de gestión | Creación y eliminación de archivos |
| | ec2:DeleteSecurityGroup | Operaciones de gestión | Creación y eliminación de archivos |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Cree, vea y gestione recursos del sistema de archivos FSx para ONTAP | | | |

| | | | |
|---|---|---|---|
| | fsx:CrearCopiaDeSeguridad | Operaciones de gestión | Operaciones y remediación |
| **Específico** | **Acción** | **Dónde se utiliza** | **Política de permisos** |
| | fsx:CrearVolumenDesdeCopiaDeSeguridad | Operaciones de gestión | Operaciones y remediación |
| | fsx:Eliminar copia de seguridad | Operaciones de gestión | Operaciones y remediación |
| Obtenga métricas de volumen y sistema de archivos | Cloudwatch:GetMetricData | Operaciones de gestión | Visualización, planificación y análisis |
| | Cloudwatch:GetMetricStatistics | Operaciones de gestión | Visualización, planificación y análisis |
| Simule operaciones de carga de trabajo para validar los permisos disponibles y compárelos con los permisos necesarios para la cuenta de AWS | iam: Política de SimulatePrincipalPolicy | Puesta en marcha | Todo |
| Proporcionar información basada en IA para FSx para eventos de ONTAP EMS | Bedrock:ListInferenceProfiles | FSx para el análisis de ONTAP EMS | Operaciones y remediación |
| | lecho de roca: Obtener perfil de inferencia | FSx para el análisis de ONTAP EMS | Operaciones y remediación |
| | lecho de roca: InvokeModelWihResponseStream | FSx para el análisis de ONTAP EMS | Operaciones y remediación |
| | Bedrock:InvokeModel | FSx para el análisis de ONTAP EMS | Operaciones y remediación |
| Obtenga datos de costos y uso de FSx para sistemas de archivos ONTAP desde AWS Cost Explorer | ce:ObtenerCostoYUso | Análisis de costos y uso | Visualización, planificación y análisis |
| | ce:Obtener etiquetas | Análisis de costos y uso | Visualización, planificación y análisis |
| Crea un punto de acceso S3 y lo adjunta a un sistema de archivos FSx for ONTAP | fsx:CreateAndAttachS3AccessPoint | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Desvincula un punto de acceso S3 de un sistema de archivos FSx for ONTAP y elimínalo | fsx:DetachAndDeleteS3AccessPoint | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Crea un punto de acceso S3 para simplificar la gestión del acceso a los buckets | s3:CreateAccessPoint | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Eliminar un punto de acceso S3 | s3:DeleteAccessPoint | Gestión de puntos de acceso S3 | Operaciones y remediación |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Agrega etiquetas a un punto de acceso S3 | s3:TagResource | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Lista y visualiza etiquetas en un punto de acceso S3 | s3:ListTagsForResource | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Eliminar etiquetas de un punto de acceso S3 | s3:UntagResource | Gestión de puntos de acceso S3 | Operaciones y remediación |
| Descubre objetos en un bucket de punto de acceso S3 | s3:ListBucket | Operaciones de bucket S3 | Operaciones y remediación |
| Enumera, crea y describe buckets de tablas S3 | s3tables:ListTableBuckets<br>s3tables:CreateTableBucket<br>s3tables:GetTableBucket | Gestión de buckets de tablas S3 | Operaciones y remediación |
| Listar, crear y recuperar tablas S3 | s3tables:ListTables<br>s3tables:CreateTable<br>s3tables:GetTable | Operaciones de tabla S3 | Operaciones y remediación |
| Leer la ubicación de los metadatos de la tabla | s3tables:GetTableMetadataLocation | Operaciones de metadatos de tabla S3 | Operaciones y remediación |
| Actualizar la ubicación de los metadatos de la tabla | s3tables:UpdateTableMetadataLocation | Operaciones de metadatos de tabla S3 | Operaciones y remediación |
| Lista, crea y recupera espacios de nombres de tablas | s3tables:ListNamespaces<br>s3tables:CreateNamespace<br>s3tables:GetNamespace | Operaciones del espacio de nombres S3 | Operaciones y remediación |
| Leer datos de la tabla (select, scan) | s3tables:GetTableData | Operaciones de datos de tablas S3 | Operaciones y remediación |
| Escribir datos de tabla (insert) | s3tables:PutTableData | Operaciones de datos de tablas S3 | Operaciones y remediación |
| Listar etiquetas en una tabla de inventario (obtener FSx for ONTAP, storage VM, IDs de volumen) | s3tables:ListTagsForResource | Operaciones de etiquetas de tabla S3 | Operaciones y remediación |
| Etiqueta una tabla de inventario para la búsqueda de Workload Factory | s3tables:TagResource | Operaciones de etiquetas de tabla S3 | Operaciones y remediación |
| Recupera el etiquetado de objetos a través del punto de acceso | s3:GetObjectTagging | Operaciones de objetos S3 | Operaciones y remediación |

### Permisos para cargas de trabajo de bases de datos

Las políticas de IAM disponibles para las cargas de trabajo de bases de datos proporcionan los permisos que Workload Factory necesita para administrar los recursos y procesos dentro de su entorno de nube pública.

Las bases de datos ofrecen las siguientes políticas de permisos para elegir:

- **Visualización, planificación y análisis**: Consulte el inventario de recursos de la base de datos, conozca el estado de sus recursos, revise el análisis de arquitectura óptima para sus configuraciones de base de datos y explore ahorros, obtenga análisis de registros de errores y explore ahorros.
- **Operaciones y corrección**: Realice tareas operativas para los recursos de su base de datos y solucione problemas de configuración de la base de datos y del sistema de almacenamiento de archivos FSx para ONTAP subyacente.
- **Creación de hosts de base de datos**: Implemente los hosts de base de datos y el FSx subyacente para el almacenamiento del sistema de archivos ONTAP de acuerdo con las mejores prácticas.

Seleccione el modo operativo para ver las políticas de IAM necesarias:

## Políticas de IAM para cargas de trabajo de bases de datos

**Visualización, planificación y análisis**

```
{
    "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/*"
        }
    ]
}
```

**Operaciones y remediación**

```
[
    {
        "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*"
            }
        }
    }
]
```

**Creación de host de base de datos**

```
{
    "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*"
        }
    ]
}
```

En la siguiente tabla se muestran los permisos para las cargas de trabajo de la base de datos.

**Tabla de permisos para cargas de trabajo de base de datos**

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Obtenga estadísticas métricas para FSx para ONTAP, EBS y FSx para Windows File Server y para recomendaciones de optimización de cómputo | Cloudwatch:GetMetricStatistics | • Inventario<br>• Explora el ahorro | Visualización, planificación y análisis |
| Recopile métricas de rendimiento guardadas en Amazon CloudWatch desde nodos SQL registrados. Los datos se generan en gráficos de tendencias de rendimiento en la pantalla de administración de instancias para las instancias SQL registradas. | Cloudwatch:GetMetricData | Inventario | Visualización, planificación y análisis |
| Obtenga detalles para las instancias de EC2 | ec2:DescribInstances | • Inventario<br>• Explora el ahorro | Visualización, planificación y análisis |
| | ec2:DescribeKeyPairs | Puesta en marcha | Visualización, planificación y análisis |
| | ec2:DescribeNetworkinterfaces | Puesta en marcha | Visualización, planificación y análisis |
| | EC2:DescripciónTipos de InstanceTipos | • Puesta en marcha<br>• Explora el ahorro | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Obtén los detalles que necesitas para rellenar el formulario de puesta en marcha de FSx para ONTAP | ec2:DescribeVpcs | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| | ec2:DescribeSubnets | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| | ec2:DescribeSecurityGroups | Puesta en marcha | Visualización, planificación y análisis |
| | ec2:DescribeImages | Puesta en marcha | Visualización, planificación y análisis |
| | ec2:regiones describidas | Puesta en marcha | Visualización, planificación y análisis |
| | ec2:DescribeRouteTables | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| Obtenga cualquier extremo de VPC existente para determinar si es necesario crear nuevos extremos antes de las implementaciones | ec2:DescribeVpcEndpoints | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| Cree puntos finales de VPC si no existen para los servicios requeridos independientemente de la conectividad de red pública en las instancias de EC2 | EC2:CreateVpcEndpoint | Puesta en marcha | Creación de host de base de datos |
| Obtener tipos de instancias disponibles en la región para los nodos de validación (T2.micro/T3.micro) | EC2:DescripciónInstanceTypeOfferings | Puesta en marcha | Visualización, planificación y análisis |
| Obtenga detalles de snapshot de cada volumen de EBS adjunto para calcular los precios y el ahorro | ec2:DescribSnapshots | Explora el ahorro | Visualización, planificación y análisis |
| Obtén detalles de cada volumen de EBS adjunto para calcular los precios y el ahorro | ec2:DescribeVolumes | • Inventario<br>• Explora el ahorro | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Obtenga información clave de KMS para el cifrado del sistema de archivos FSx para ONTAP | Kms:ListAliases | Puesta en marcha | Visualización, planificación y análisis |
| | Km:ListKeys | Puesta en marcha | Visualización, planificación y análisis |
| | Km:DescripbeKey | Puesta en marcha | Visualización, planificación y análisis |
| Obtenga una lista de pilas de CloudFormation que se ejecutan en el entorno para comprobar el límite de cuota | Cloudformation:ListStacks | Puesta en marcha | Visualización, planificación y análisis |
| Compruebe los límites de la cuenta para los recursos antes de activar el despliegue | Formación de nubes:DescribeAccountLimits | Puesta en marcha | Visualización, planificación y análisis |
| Obtenga una lista de directorios activos gestionados por AWS en la región | ds:DescripbeDirectories | Puesta en marcha | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Obtén listas y detalles de volúmenes, backups, SVM, sistemas de archivos en AZs y etiquetas para el sistema de archivos FSx para ONTAP | fsx:DescribeVolumes | • Inventario<br>• Explore Ahorros | Visualización, planificación y análisis |
| | fsx:DescripbeBackups | • Inventario<br>• Explore Ahorros | Visualización, planificación y análisis |
| | fsx:DescribeStorageVirtualMachines | • Puesta en marcha<br>• Operaciones de gestión<br>• Inventario | Visualización, planificación y análisis |
| | fsx:DescripciónFileSystems | • Puesta en marcha<br>• Operaciones de gestión<br>• Inventario<br>• Explora el ahorro | Visualización, planificación y análisis |
| | fsx:ListTagsForResource | Operaciones de gestión | Visualización, planificación y análisis |
| Obtenga los límites de cuota de servicio para CloudFormation y VPC / Cree secretos en una cuenta de usuario para las credenciales proporcionadas para SQL, dominio y FSx para ONTAP | ServiceQuotas:ListServiceQuotas | Puesta en marcha | Visualización, planificación y análisis |
| Utilice la consulta basada en SSM para obtener la lista actualizada de regiones soportadas por FSx para ONTAP | ssm:GetParametersByPath | Puesta en marcha | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Sondea la respuesta de SSM después de enviar el comando para las operaciones de gestión posteriores al despliegue | ssm:GetCommandInvocation | • Operaciones de gestión<br>• Inventario<br>• Explora el ahorro<br>• Optimización | Visualización, planificación y análisis |
| Enviar comandos a través de SSM a instancias EC2 para su detección y gestión. | ssm:SendCommand | • Operaciones de gestión<br>• Inventario<br>• Explora el ahorro<br>• Optimización | Visualización, planificación y análisis |
| Obtener el estado de conectividad de SSM en las instancias posteriores al despliegue | ssm:GetConnectionStatus | • Operaciones de gestión<br>• Inventario<br>• Optimización | Visualización, planificación y análisis |
| Recuperar el estado de asociación de SSM para un grupo de instancias EC2 gestionadas (nodos SQL) | ssm:Descripción InstanceInformation | Inventario | Visualización, planificación y análisis |
| Obtenga la lista de líneas base de parches disponibles para la evaluación de parches del sistema operativo | ssm:DescripciónPatchBaselines | Optimización | Visualización, planificación y análisis |
| Obtener el estado de aplicación de parches en las instancias de Windows EC2 para la evaluación de parches del sistema operativo | ssm:DescripciónInstancePatchStates | Optimización | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Enumere los comandos ejecutados por AWS Patch Manager en las instancias EC2 para la gestión de parches del sistema operativo | ssm: ListCommands | Optimización | Visualización, planificación y análisis |
| Compruebe si la cuenta está inscrita en AWS Compute Optimizer | Compute-Optimizer:GetEnrollmentStatus | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |
| Actualice una preferencia de recomendación existente en AWS Compute Optimizer para adaptar las sugerencias para las cargas de trabajo de SQL Server | Compute-Optimizer:PutRecommendationPreferences | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |
| Obtener preferencias de recomendación que están en vigor para un recurso determinado de AWS Compute Optimizer | Compute-Optimizer:GetEffectiveRecommendationPreferences | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |
| Obtenga recomendaciones que AWS Compute Optimizer genera para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) | Compute-Optimizer:GetEC2InstanceRecommendations | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |
| Compruebe la asociación de instancias a grupos de escala automática | escala automática:DescripciónAutoScalingGroups | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |
| | escala automática:DescripciónAutoScalingInstances | • Explora el ahorro<br>• Optimización | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Obtenga, enumere, cree y elimine parámetros de SSM para las credenciales de usuario de AD, FSx para ONTAP y SQL utilizadas durante la implementación o administradas en su cuenta de AWS | ssm:getParameter [1] | • Puesta en marcha<br>• Operaciones de gestión<br>• Inventario | Visualización, planificación y análisis |
| | ssm:GetParameters [1] | • Puesta en marcha<br>• Operaciones de gestión<br>• Inventario | Visualización, planificación y análisis |
| | ssm:PutParameter [1] | • Puesta en marcha<br>• Operaciones de gestión | Visualización, planificación y análisis |
| | ssm:DeleteParameters [1] | • Puesta en marcha<br>• Operaciones de gestión | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Asocie recursos de red a nodos SQL y nodos de validación, y agregue IP secundarias adicionales a nodos SQL | EC2:AllocateAddress [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AllocateHosts [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AssignPrivateIpAddresses [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AssociateAddress [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AssociateRouteTable [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AssociateSubnetCidrBlock [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AssociateVpcCidrBlock [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AttachInternetGateway [1] | Puesta en marcha | Creación de host de base de datos |
| | EC2:AttachNetworkInterface [1] | Puesta en marcha | Creación de host de base de datos |
| Conecte los volúmenes de EBS necesarios a los nodos SQL para la puesta en marcha | ec2:AttachVolume | Puesta en marcha | Creación de host de base de datos |
| Adjunte grupos de seguridad y modifique reglas a las instancias EC2 aprovisionadas. | ec2:AuthorizeSecurityGroupEgress | Puesta en marcha | Creación de host de base de datos |
| | ec2:AuthorizeSecurityGroupIngress | Puesta en marcha | Creación de host de base de datos |
| Cree los volúmenes de EBS necesarios para los nodos SQL para la puesta en marcha | ec2:CreateVolume | Puesta en marcha | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Elimine los nodos de validación temporales creados del tipo T2.micro y para la reversión o el reintento de EC2 nodos SQL fallidos | ec2:DeleteNetworkInterface | Puesta en marcha | Creación de host de base de datos |
| | ec2:DeleteSecurityGroup | Puesta en marcha | Creación de host de base de datos |
| | ec2:DeleteTags | Puesta en marcha | Creación de host de base de datos |
| | ec2:DeleteVolume | Puesta en marcha | Creación de host de base de datos |
| | EC2:DetachNetworkInterface | Puesta en marcha | Creación de host de base de datos |
| | ec2:DetachVolume | Puesta en marcha | Creación de host de base de datos |
| | EC2:DisasociateAddress | Puesta en marcha | Creación de host de base de datos |
| | ec2:DisasociateIamInstanceProfile | Puesta en marcha | Creación de host de base de datos |
| | EC2:DisAssociateRouteTable | Puesta en marcha | Creación de host de base de datos |
| | EC2:DisasociateSubnetCidrBlock | Puesta en marcha | Creación de host de base de datos |
| | EC2:DisasociateVpcCidrBlock | Puesta en marcha | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Modificar atributos para instancias SQL creadas. Solo se aplica a los nombres que comienzan con WLMDB. | ec2:ModificyInstanceAttribute | Puesta en marcha | Operaciones y remediación |
| | EC2:ModifyInstanceColocación | Puesta en marcha | Creación de host de base de datos |
| | ec2:ModificyNetworkInterfaceAttribute | Puesta en marcha | Creación de host de base de datos |
| | EC2:ModifySubnetAttribute | Puesta en marcha | Creación de host de base de datos |
| | ec2:ModifiyVolume | Puesta en marcha | Creación de host de base de datos |
| | ec2:ModifyVolumeAttribute | Puesta en marcha | Creación de host de base de datos |
| | EC2:ModifyVpcAttribute | Puesta en marcha | Creación de host de base de datos |
| Desasociar y destruir instancias de validación | EC2:Release Address | Puesta en marcha | Creación de host de base de datos |
| | EC2:ReplaceRoute | Puesta en marcha | Creación de host de base de datos |
| | EC2:ReplaceRouteTableAssociation | Puesta en marcha | Creación de host de base de datos |
| | ec2:RevokeSecurityGroupEgress | Puesta en marcha | Creación de host de base de datos |
| | ec2:RevokeSecurityGroupIngress | Puesta en marcha | Creación de host de base de datos |
| Inicie las instancias desplegadas | ec2:StartuStarInstances | Puesta en marcha | Operaciones y remediación |
| Pare las instancias desplegadas | ec2:StopInstances | Puesta en marcha | Operaciones y remediación |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Etiquete valores personalizados para los recursos de Amazon FSx for NetApp ONTAP creados por WLMDB para obtener detalles de facturación durante la gestión de recursos | fsx:TagResource [1] | • Puesta en marcha<br>• Operaciones de gestión | Creación de host de base de datos |
| Cree y valide la plantilla de CloudFormation para el despliegue | Cloudformation:CreateStack | Puesta en marcha | Creación de host de base de datos |
| | Cloudformation:DescribeStackEvents | Puesta en marcha | Creación de host de base de datos |
| | Cloudformation:Describacks | Puesta en marcha | Creación de host de base de datos |
| | Cloudformation:ListStacks | Puesta en marcha | Visualización, planificación y análisis |
| | Cloudformation:ValidateTemplate | Puesta en marcha | Creación de host de base de datos |
| Cree plantillas de pila anidadas para reintentos y rollback | EC2:CreateLaunchTemplate | Puesta en marcha | Creación de host de base de datos |
| | EC2:CreateLaunchTemplateVersion | Puesta en marcha | Creación de host de base de datos |
| Gestionar etiquetas y seguridad de red en las instancias creadas | ec2:CreateNetworkInterface | Puesta en marcha | Creación de host de base de datos |
| | ec2:CreateSecurityGroup | Puesta en marcha | Creación de host de base de datos |
| | ec2:CreateTags | Puesta en marcha | Creación de host de base de datos |
| Obtener detalles de instancia para el provisionamiento | ec2:DescribeDirecciones | Puesta en marcha | Visualización, planificación y análisis |
| | ec2:DescribeLaunchTemplates | Puesta en marcha | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Inicie las instancias creadas | ec2:RunInstances | Puesta en marcha | Creación de host de base de datos |
| Crear FSx para los recursos de ONTAP necesarios para aprovisionamiento. Para los sistemas FSx para ONTAP existentes, se crea un nuevo SVM para alojar los volúmenes de SQL. | fsx:CreateFileSystem | Puesta en marcha | Creación de host de base de datos |
| | fsx:CreateStorageVirtualMachine | Puesta en marcha | Creación de host de base de datos |
| | fsx:CreateVolume | • Puesta en marcha<br>• Operaciones de gestión | Creación de host de base de datos |
| Obtén más información sobre FSx para ONTAP | fsx:DescribeFileSystemAliases | Puesta en marcha | Creación de host de base de datos |
| Cambie el tamaño de FSx para el sistema de archivos ONTAP para solucionar el margen adicional del sistema de archivos | fsx:UpdateFilesystem | Optimización | Operaciones y remediación |
| Cambie el tamaño de los volúmenes para corregir los tamaños de los registros y las unidades de TempDB | fsx:UpdateVolume | Optimización | Operaciones y remediación |
| Obtén los detalles clave de KMS y utilízalos para el cifrado FSx para ONTAP | Kms:CreateGrant | Puesta en marcha | Creación de host de base de datos |
| | kms:DescribeCustomKeyStores | Puesta en marcha | Creación de host de base de datos |
| | Km:GenerateDataKey | Puesta en marcha | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Cree registros de CloudWatch para la validación y el aprovisionamiento de scripts que se ejecutan en instancias EC2 | Registros:CreateLogGroup | Puesta en marcha | Creación de host de base de datos |
| | Registros:CreateLogStream | Puesta en marcha | Creación de host de base de datos |
| | registros:Obtener campos del grupo de registros | Puesta en marcha | Creación de host de base de datos |
| | registros:ObtenerRegistro | Puesta en marcha | Creación de host de base de datos |
| | Logs:ListLogDeliveries | Puesta en marcha | Creación de host de base de datos |
| | Logs:PutLogEvents | • Puesta en marcha<br>• Operaciones de gestión | Creación de host de base de datos |
| | Logs:TagResource | Puesta en marcha | Creación de host de base de datos |
| Workload Factory cambia a los registros de Amazon CloudWatch para la instancia de SQL al detectar un truncamiento de la salida de SSM | Logs:GetLogEvents | • Evaluación del almacenamiento (optimización)<br>• Inventario | Visualización, planificación y análisis |
| Permitir que Workload Factory obtenga grupos de registros actuales y verificar que la retención esté configurada para los grupos de registros creados por Workload Factory | Logs:DescripbeLogGroups | • Evaluación del almacenamiento (optimización)<br>• Inventario | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Permitir que Workload Factory establezca una política de retención de un día para los grupos de registros creados por Workload Factory para evitar la acumulación innecesaria de flujos de registros para las salidas del comando SSM | Logs:PutRetentionPolicy | • Evaluación del almacenamiento (optimización)<br>• Inventario | Visualización, planificación y análisis |
| Enumere los temas de SNS del cliente y publique en el SNS de backend de WLMDB, así como en el SNS del cliente, si está seleccionado | sns:ListTopics | Puesta en marcha | Visualización, planificación y análisis |
| | sns: Publicar | Puesta en marcha | Creación de host de base de datos |
| Permisos SSM necesarios para ejecutar el script de detección en instancias SQL aprovisionadas y para obtener la lista más reciente de regiones AWS compatibles con FSx para ONTAP. | ssm:PutComplianceItems | Puesta en marcha | Creación de host de base de datos |
| | ssm:PutConfigurePackageResult | Puesta en marcha | Creación de host de base de datos |
| | ssm: Inventario de PutInventory | Puesta en marcha | Creación de host de base de datos |
| | ssm: UpdateAssociationStatus | Puesta en marcha | Creación de host de base de datos |
| | ssm:UpdateInstanceAssociationStatus | Puesta en marcha | Creación de host de base de datos |
| | ssm:UpdateInstanceInformation | Puesta en marcha | Creación de host de base de datos |
| | ssmmessages:CrearCanalDeControl | Puesta en marcha | Creación de host de base de datos |
| | ssmmessages:CrearCanalDeDatos | Puesta en marcha | Creación de host de base de datos |
| | ssmmessages:Abrir canal de control | Puesta en marcha | Creación de host de base de datos |
| | mensajes ssmmessages:Canal de datos abiertos | Puesta en marcha | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| La pila de CloudFormation de señales se ha producido correctamente o ha fallado. | Formación de nubes:SignalResource [1] | Puesta en marcha | Creación de host de base de datos |
| Agregue el rol EC2 creado por la plantilla al perfil de instancia de EC2 para permitir que los scripts de EC2 accedan a los recursos necesarios para el despliegue. | iam:AddRoleToInstanceProfile | Puesta en marcha | Creación de host de base de datos |
| Cree un perfil de instancia para EC2 y adjunte el rol EC2 creado. | iam:CreateInstanceProfile | Puesta en marcha | Creación de host de base de datos |
| Cree un rol EC2 a través de una plantilla con los permisos enumerados a continuación | iam:CreateRole | Puesta en marcha | Creación de host de base de datos |
| Crear rol vinculado al servicio EC2 | iam:CreateServiceLinkedRole [2] | Puesta en marcha | Creación de host de base de datos |
| Suprimir perfil de instancia creado durante el despliegue específicamente para los nodos de validación | iam:DeleteInstanceProfile | Puesta en marcha | Creación de host de base de datos |
| Obtenga los detalles del rol y la política para determinar las brechas en los permisos y validarlas para la implementación | iam: GetPolicy | Puesta en marcha | Creación de host de base de datos |
| | iam:GetPolicyVersion | Puesta en marcha | Creación de host de base de datos |
| | iam:GetRole | Puesta en marcha | Creación de host de base de datos |
| | iam: GetRolePolicy | Puesta en marcha | Creación de host de base de datos |
| | iam: GetUser | Puesta en marcha | Creación de host de base de datos |
| Transfiera el rol creado a la instancia EC2 | iam:PassRole [3] | Puesta en marcha | Creación de host de base de datos |
| Agregue una política con los permisos necesarios al rol EC2 creado | iam:PutRolePolicy | Puesta en marcha | Creación de host de base de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Separe el rol del perfil de instancia de EC2 aprovisionado | iam:RemoveRoleFromInstanceProfile | Puesta en marcha | Creación de host de base de datos |
| Simule operaciones de carga de trabajo para validar los permisos disponibles y compárelos con los permisos necesarios para la cuenta de AWS | iam: Política de SimulatePrincipalPolicy | Puesta en marcha | Todo |
| Obtenga los modelos base disponibles para el análisis de registros de errores. | Bedrock:GetFoundationModelAvailability | Análisis del registro de errores | Visualización, planificación y análisis |
| Enumera los perfiles de interfaz disponibles en Amazon Bedrock para el análisis de registros de errores. | Bedrock:ListInferenceProfiles | Análisis del registro de errores | Visualización, planificación y análisis |

1. El permiso está restringido a los recursos que comienzan con WLMDB.
2. «iam:CreateServiceLinkedRole» limitado por «iam:AWSServiceName»: «ec2.amazonaws.com"*
3. “iam:PassRole” limitado por “iam:PassedToService”: “ec2.amazonaws.com"*

**Permisos para cargas de trabajo de GenAI**

Las políticas de IAM para cargas de trabajo de VMware proporcionan los permisos que Workload Factory for VMware necesita para administrar recursos y procesos dentro de su entorno de nube pública en función del modo operativo en el que opera.

Las políticas de IAM de GenAI solo están disponibles con permisos de lectura/escritura:

- **Lectura/Escritura**: ejecuta y automatiza operaciones en AWS en su nombre junto con las credenciales asignadas que tienen los permisos necesarios y validados para la ejecución.

**Políticas de IAM para las cargas de trabajo de GenAI**

```
{
  "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": "*"
    }
  ]
}
```

En la siguiente tabla se ofrecen detalles sobre los permisos para las cargas de trabajo de GenAI.

**Tabla de permisos para cargas de trabajo de GenAI**

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Cree una pila de formación de cloud del motor de IA durante las operaciones de puesta en marcha y recompilación | Cloudformation:CreateStack | Puesta en marcha | Lectura/Escritura |
| Cree la pila de formación de cloud del motor de IA | Cloudformation:Describacks | Puesta en marcha | Lectura/Escritura |
| Enumere las regiones del asistente de despliegue del motor AI | ec2:regiones describidas | Puesta en marcha | Lectura/Escritura |
| Mostrar etiquetas de motor AI | ec2:etiquetas a describTags | Puesta en marcha | Lectura/Escritura |
| Lista de depósitos S3 | s3:ListAllMyBuckets | Puesta en marcha | Lectura/Escritura |
| Enumere los extremos de VPC antes de crear la pila del motor de AI | EC2:CreateVpcEndpoint | Puesta en marcha | Lectura/Escritura |
| Cree un grupo de seguridad del motor de IA durante la creación de la pila del motor de IA durante las operaciones de implementación y reconstrucción | ec2:CreateSecurityGroup | Puesta en marcha | Lectura/Escritura |
| Etiquete los recursos creados por la creación de pila de motores de IA durante las operaciones de implementación y recompilación | ec2:CreateTags | Puesta en marcha | Lectura/Escritura |
| Publique eventos cifrados en el backend WLMAI desde la pila del motor AI | Km:GenerateDataKey | Puesta en marcha | Lectura/Escritura |
| | Km:descifrar | Puesta en marcha | Lectura/Escritura |
| Publique eventos y recursos personalizados en el backend WLMAI desde la pila ai-engine | sns: Publicar | Puesta en marcha | Lectura/Escritura |
| Mostrar los PC virtuales durante el asistente de despliegue del motor AI | ec2:DescribeVpcs | Puesta en marcha | Lectura/Escritura |
| Muestra las subredes del asistente de despliegue del motor AI | ec2:DescribeSubnets | Puesta en marcha | Lectura/Escritura |
| Obtenga tablas de ruta durante la puesta en marcha y recompilación del motor de IA | ec2:DescribeRouteTables | Puesta en marcha | Lectura/Escritura |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Enumere los pares de claves durante el asistente de implementación del motor de IA | ec2:DescribeKeyPairs | Puesta en marcha | Lectura/Escritura |
| Enumerar los grupos de seguridad durante la creación de la pila del motor AI (para buscar grupos de seguridad en los extremos privados) | ec2:DescribeSecurityGroups | Puesta en marcha | Lectura/Escritura |
| Consigue extremos de VPC para determinar si se deben crear alguno durante la puesta en marcha del motor de IA | ec2:DescribeVpcEndpoints | Puesta en marcha | Lectura/Escritura |
| Enumere las aplicaciones de Amazon Q Business | Qbusiness:ListApplications | Puesta en marcha | Lectura/Escritura |
| Enumere las instancias para averiguar el estado del motor de IA | ec2:DescribInstances | Resolución de problemas | Lectura/Escritura |
| Enumera imágenes durante la creación de la pila del motor de IA durante las operaciones de implementación y recompilación | ec2:DescribeImages | Puesta en marcha | Lectura/Escritura |
| Cree y actualice la instancia de IA y el grupo de seguridad de punto final privado durante la creación de la pila de instancias de AI durante las operaciones de despliegue y reconstrucción | ec2:RevokeSecurityGroupEgress | Puesta en marcha | Lectura/Escritura |
| | ec2:RevokeSecurityGroupIngress | Puesta en marcha | Lectura/Escritura |
| Ejecutar el motor de IA durante la creación de pilas de formación de nube durante las operaciones de puesta en marcha y recompilación | ec2:RunInstances | Puesta en marcha | Lectura/Escritura |
| Asocie grupos de seguridad y modifique las reglas del motor de IA durante la creación de la pila durante las operaciones de puesta en marcha y recompilación | ec2:AuthorizeSecurityGroupEgress | Puesta en marcha | Lectura/Escritura |
| | ec2:AuthorizeSecurityGroupIngress | Puesta en marcha | Lectura/Escritura |
| Inicie una solicitud de chat para uno de los modelos básicos | Bedrock:InvokeModelWithResponseStream | Puesta en marcha | Lectura/Escritura |
| Iniciar solicitud de chat/inserción para modelos de base | Bedrock:InvokeModel | Puesta en marcha | Lectura/Escritura |
| Muestra los modelos de base disponibles en una región | Bedrock:ListFoundationModels | Puesta en marcha | Lectura/Escritura |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Obtenga información sobre un modelo de fundación | Bedrock:GetFoundationModel | Puesta en marcha | Lectura/Escritura |
| Verifique el acceso al modelo de base | Bedrock:GetFoundationModelAvailability | Puesta en marcha | Lectura/Escritura |
| Verifique la necesidad de crear un grupo de registros de Amazon CloudWatch durante las operaciones de despliegue y reconstrucción | Logs:DescripbeLogGroups | Puesta en marcha | Lectura/Escritura |
| Obtén regiones que dan soporte a FSx y Amazon Bedrock durante el asistente del motor de IA | ssm:GetParametersByPath | Puesta en marcha | Lectura/Escritura |
| Obtenga la imagen más reciente de Amazon Linux para la puesta en marcha del motor de IA durante las operaciones de puesta en marcha y recompilación | ssm: GetParameters | Puesta en marcha | Lectura/Escritura |
| Obtenga la respuesta SSM del comando enviado al motor AI | ssm:GetCommandInvocation | Puesta en marcha | Lectura/Escritura |
| Compruebe la conexión del SSM al motor AI | ssm:SendCommand | Puesta en marcha | Lectura/Escritura |
| | ssm:GetConnectionStatus | Puesta en marcha | Lectura/Escritura |
| Cree un perfil de instancia del motor de IA durante la creación de pila durante las operaciones de puesta en marcha y recompilación | iam:CreateRole | Puesta en marcha | Lectura/Escritura |
| | iam:CreateInstanceProfile | Puesta en marcha | Lectura/Escritura |
| | iam:AddRoleToInstanceProfile | Puesta en marcha | Lectura/Escritura |
| | iam:PutRolePolicy | Puesta en marcha | Lectura/Escritura |
| | iam: GetRolePolicy | Puesta en marcha | Lectura/Escritura |
| | iam:GetRole | Puesta en marcha | Lectura/Escritura |
| | iam:TagRole | Puesta en marcha | Lectura/Escritura |
| | iam:PassRole | Puesta en marcha | Lectura/Escritura |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Simule operaciones de carga de trabajo para validar los permisos disponibles y compárelos con los permisos necesarios para la cuenta de AWS | iam: Política de SimulatePrincipalPolicy | Puesta en marcha | Lectura/Escritura |
| Enumere los sistemas de archivos FSx para ONTAP durante el asistente para crear base de conocimientos | fsx:DescribeVolumes | Creación de la base de conocimientos | Lectura/Escritura |
| Enumera los volúmenes del sistema de archivos FSx para ONTAP durante el asistente para crear base de conocimientos | fsx:DescripciónFileSystems | Creación de la base de conocimientos | Lectura/Escritura |
| Gestionar las bases de conocimientos en el motor de IA durante las operaciones de recompilación | fsx:ListTagsForResource | Resolución de problemas | Lectura/Escritura |
| Enumere las máquinas virtuales de almacenamiento del sistema de archivos FSx para ONTAP durante el asistente de creación de base de conocimientos | fsx:DescribeStorageVirtualMachines | Puesta en marcha | Lectura/Escritura |
| Mueva la base de conocimientos a una nueva instancia | fsx:UntagResource | Resolución de problemas | Lectura/Escritura |
| Gestione la base de conocimientos en el motor de IA durante la recompilación | fsx:TagResource | Resolución de problemas | Lectura/Escritura |
| Guardar los secretos SSM (token ECR, credenciales CIFS, claves de las cuentas de servicio de inquilino) de una forma segura | ssm:getParameter | Puesta en marcha | Lectura/Escritura |
| | ssm: Parámetro de PutParameter | Puesta en marcha | Lectura/Escritura |
| Envíe los registros del motor de IA al grupo de registros de Amazon CloudWatch durante las operaciones de implementación y reconstrucción | Registros:CreateLogGroup | Puesta en marcha | Lectura/Escritura |
| | Logs:PutRetentionPolicy | Puesta en marcha | Lectura/Escritura |
| Envíe los registros del motor de IA al grupo de registros de Amazon CloudWatch | Logs:TagResource | Resolución de problemas | Lectura/Escritura |
| Obtener respuesta SSM de Amazon CloudWatch (cuando la respuesta es demasiado larga) | Registros:DescripbeLogStreams | Resolución de problemas | Lectura/Escritura |
| Obtén la respuesta SSM de Amazon CloudWatch | Logs:GetLogEvents | Resolución de problemas | Lectura/Escritura |

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Cree un grupo de registros de Amazon CloudWatch para los registros de base de Amazon durante la creación de la pila durante las operaciones de implementación y reconstrucción | Registros:CreateLogGroup | Puesta en marcha | Lectura/Escritura |
| | Logs:PutRetentionPolicy | Puesta en marcha | Lectura/Escritura |
| | Logs:TagResource | Puesta en marcha | Lectura/Escritura |
| Listar perfiles de inferencia para el modelo | Bedrock:ListInferenceProfiles | Resolución de problemas | Lectura/Escritura |

**Permisos para cargas de trabajo de VMware**

Las cargas de trabajo de VMware tienen las siguientes políticas de permisos para elegir:

- **Visualización, planificación y análisis**: Consulte el inventario de entornos de virtualización de EVS, obtenga un análisis bien diseñado para sus sistemas y explore las posibilidades de ahorro.
- **Implementación y conectividad del almacenamiento de datos**: Implemente las configuraciones de máquinas virtuales recomendadas en clústeres de Amazon EVS, Amazon EC2 o VMware Cloud on AWS vSphere y utilice sistemas de archivos Amazon FSx for NetApp ONTAP personalizados como almacenes de datos externos.

Seleccione la política de permisos para ver las políticas de IAM necesarias:

## Políticas de IAM para cargas de trabajo de VMware

**Visualización, planificación y análisis**

```
{
  "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": "*"
    }
  ]
}
```

**Despliegue y conectividad del almacenamiento de datos**

```
{
  "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": "*"
    }
  ]
}
```

En la siguiente tabla se ofrece información sobre los permisos para las cargas de trabajo de VMware.

**Tabla de permisos para cargas de trabajo de VMware**

| Específico | Acción | Donde se utiliza | Política de permisos |
|---|---|---|---|
| Asocie grupos de seguridad y modifique reglas para los nodos aprovisionados | ec2:AuthorizeSecurityGroupIngress | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Cree volúmenes de EBS | fsx:CreateVolume | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Etiquete valores personalizados para los recursos de FSx para NetApp ONTAP creados por las cargas de trabajo de VMware | fsx:TagResource | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Cree y valide la plantilla de CloudFormation | Cloudformation:CreateStack | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Gestionar etiquetas y seguridad de red en las instancias creadas | ec2:CreateSecurityGroup | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Inicie las instancias creadas | ec2:RunInstances | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Obtenga los detalles de las instancias de EC2 | ec2:DescribInstances | Inventario | Despliegue y conectividad del almacenamiento de datos |
| Muestre las imágenes durante la creación de la pila durante las operaciones de despliegue y reconstrucción | ec2:DescribeImages | Inventario | Despliegue y conectividad del almacenamiento de datos |
| Ver detalles de configuración de los conjuntos de opciones DHCP asociados con las VPC | ec2:DescribeDhcpOptions | Inventario | Visualización, planificación y análisis |
| Obtenga los VPC en el entorno seleccionado para completar el formulario de implementación | ec2:DescribeVpcs | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| Obtener las subredes del entorno seleccionado para completar el formulario de despliegue | ec2:DescribeSubnets | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Obtener los grupos de seguridad del entorno seleccionado para completar el formulario de implementación | ec2:DescribeSecurityGroups | Puesta en marcha | Visualización, planificación y análisis |
| Obtener las zonas de disponibilidad en el entorno seleccionado | EC2:DescripciónAvailabilityZones | • Puesta en marcha<br>• Inventario | Visualización, planificación y análisis |
| Obtén las regiones con soporte de Amazon FSx para NetApp ONTAP | ec2:regiones describidas | Puesta en marcha | Visualización, planificación y análisis |
| Obtener alias de claves KMS para utilizar para el cifrado de Amazon FSx para NetApp ONTAP | Kms:ListAliases | Puesta en marcha | Visualización, planificación y análisis |
| Obtenga las claves KMS para utilizar para el cifrado de Amazon FSx para NetApp ONTAP | Km:ListKeys | Puesta en marcha | Visualización, planificación y análisis |
| Obtener detalles de caducidad de claves KMS que se utilizarán para el cifrado de Amazon FSx para NetApp ONTAP | Km:DescripbeKey | Puesta en marcha | Visualización, planificación y análisis |
| Enumera los secretos en AWS Secrets Manager | gestor de secretos: Listar secretos | Inventario | Visualización, planificación y análisis |
| Obtén una lista de entornos de Amazon EVS | evs:ListEnvironments | Inventario | Visualización, planificación y análisis |
| Obtenga información detallada sobre un entorno específico de Amazon EVS. | evs:ObtenerEntorno | Inventario | Visualización, planificación y análisis |
| Enumera las VLAN asociadas a un entorno de Amazon EVS. | evs:ListEnvironmentVlans | Inventario | Visualización, planificación y análisis |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Cree los recursos de Amazon FSx para NetApp ONTAP necesarios para el aprovisionamiento | fsx:CreateFileSystem | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| | fsx:CreateStorageVirtualMachine | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| | fsx:CreateVolume | • Puesta en marcha<br>• Operaciones de gestión | Despliegue y conectividad del almacenamiento de datos |
| Obtén los detalles de Amazon FSx para NetApp ONTAP | fsx:describe* | • Puesta en marcha<br>• Inventario<br>• Operaciones de gestión<br>• Explora el ahorro | Despliegue y conectividad del almacenamiento de datos |
| Obtenga los detalles clave de KMS y utilícelos para el cifrado de Amazon FSx para NetApp ONTAP | Kms:CreateGrant | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| | Kms:describir* | Puesta en marcha | Visualización, planificación y análisis |
| | Kms:Lista* | Puesta en marcha | Visualización, planificación y análisis |
| | Km:descifrar | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| | Km:GenerateDataKey | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |

| Específico | Acción | Donde se utiliza | Política de permisos |
| --- | --- | --- | --- |
| Enumere los temas de SNS del cliente y publique en el SNS de backend de WLMVMC, así como en el SNS del cliente, si se selecciona | sns: Publicar | Puesta en marcha | Despliegue y conectividad del almacenamiento de datos |
| Simule operaciones de carga de trabajo para validar los permisos disponibles y compárelos con los permisos necesarios para la cuenta de AWS | iam: Política de SimulatePrincipalPolicy | Puesta en marcha | • Despliegue y conectividad del almacenamiento de datos<br>• Visualización, planificación y análisis |

## Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

#### 1 de febrero de 2025

Se agregaron los siguientes permisos a la carga de trabajo de almacenamiento:

- `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 de diciembre de 2025**

Se agregaron los siguientes permisos a la carga de trabajo de almacenamiento:

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

**27 de noviembre de 2025**

Se agregaron los siguientes permisos a la carga de trabajo de almacenamiento:

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

**2 de noviembre de 2025**

Las políticas de permisos "solo lectura" y "lectura/escritura" se han reemplazado en las cargas de trabajo de almacenamiento, bases de datos y VMware para proporcionar mayor granularidad y flexibilidad en la asignación de permisos.

**5 de octubre de 2025**

Los siguientes permisos se eliminaron de GenAI y ahora son manejados por el motor GenAI:

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

**29 de junio de 2025**

El siguiente permiso ahora está disponible en modo de solo lectura para bases de datos:

`cloudwatch:GetMetricData` .

### 3 de junio de 2025

El siguiente permiso ahora está disponible en modo *lectura/escritura* para GenAI: `s3:ListAllMyBuckets` .

### 4 de mayo de 2025

El siguiente permiso ahora está disponible en modo *lectura/escritura* para GenAI: `qbusiness:ListApplications` .

Los siguientes permisos ahora están disponibles en modo de solo lectura para bases de datos:

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

El siguiente permiso ahora está disponible en modo *lectura/escritura* para bases de datos: `logs:PutRetentionPolicy` .

### 2 de abril de 2025

El siguiente permiso ahora está disponible en modo de solo lectura para bases de datos: `ssm:DescribeInstanceInformation` .

### 30 de marzo de 2025

#### Actualización de permisos de carga de trabajo de GenAI

Los siguientes permisos ahora están disponibles en *modo lectura/escritura* para GenAI:

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

Se ha eliminado el siguiente permiso del *modo lectura/escritura* para GenAI: `Bedrock:GetFoundationModel` .

#### iam:SimulatePrincipalPolicy actualización de permisos

El `iam:SimulatePrincipalPolicy` El permiso es parte de todas las políticas de permisos de carga de trabajo si habilita la verificación automática de permisos al agregar credenciales de cuenta de AWS adicionales o agregar una nueva capacidad de carga de trabajo desde la consola de Workload Factory. El permiso simula operaciones de carga de trabajo y verifica si tiene los permisos de cuenta de AWS necesarios antes de implementar recursos desde Workload Factory. Habilitar esta verificación reduce el tiempo y el esfuerzo que podría necesitar para limpiar recursos de operaciones fallidas y agregar permisos faltantes.

**2 de marzo de 2025**

El siguiente permiso ahora está disponible en modo *lectura/escritura* para GenAI: `bedrock:GetFoundationModel` .

**3 de febrero de 2025**

El siguiente permiso ahora está disponible en modo de solo lectura para bases de datos: `iam:SimulatePrincipalPolicy` .

## Información de copyright



## Información de la marca comercial