



Manos a la obra

Setup and administration

NetApp
February 02, 2026

Tabla de contenidos

- Manos a la obra 1
 - Aprenda lo básico 1
 - Obtenga más información sobre NetApp Workload Factory 1
 - Experiencias de consola 5
 - Permisos para NetApp Workload Factory 6
 - Inicio rápido para NetApp Workload Factory 64
 - Regístrese en NetApp Workload Factory 64
 - Regístrate en Workload Factory 65
 - Invitar a otros a unirse a una cuenta en Workload Factory 66
 - Agregar credenciales de AWS a Workload Factory 67
 - Descripción general 67
 - Credenciales de AWS 67
 - Agregar credenciales a una cuenta manualmente 68
 - Agregue credenciales a una cuenta usando CloudFormation 71
 - Optimice las cargas de trabajo con NetApp Workload Factory 73

Manos a la obra

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.

Hello Richard,

Let's get started by creating an account.



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

[Learn more about accounts.](#) 

Account name

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

My job description Optional

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:

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	<ul style="list-style-type: none"> • Puesta en marcha • Explora el ahorro 	Creación y eliminación de archivos
	ec2:DescribeSubnets	<ul style="list-style-type: none"> • Puesta en marcha • Explora el ahorro 	Creación y eliminación de archivos
	ec2:DescribeSecurityGroups	<ul style="list-style-type: none"> • Puesta en marcha • Explora el ahorro 	Creación y eliminación de archivos
	ec2:DescribeRouteTables	<ul style="list-style-type: none"> • Puesta en marcha • Explora el ahorro 	Creación y eliminación de archivos
	ec2:DescribeNetworkInterfaces	<ul style="list-style-type: none"> • Puesta en marcha • Explora el ahorro 	Creación y eliminación de archivos
	EC2:DescribeVolumeStatus	<ul style="list-style-type: none"> • Puesta en marcha • 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:DescribeKey	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	<ul style="list-style-type: none"> • Inventario • Explora el ahorro 	Visualización, planificación y análisis
Obtenga detalles para las instancias de EC2	ec2:DescribeInstances	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 fsx:EliminarCopiaDeSeguridad	Donde se gestiona	Política de permisos
	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: InvokeModelWithResponseStream	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 s3tables:CreateTableBucket s3tables:GetTableBucket	Gestión de buckets de tablas S3	Operaciones y remediación
Listar, crear y recuperar tablas S3	s3tables:ListTables s3tables:CreateTable 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 s3tables:CreateNamespace 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:



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	<ul style="list-style-type: none"> • Inventario • 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:DescribeInstances	<ul style="list-style-type: none"> • Inventario • 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	<ul style="list-style-type: none"> • Puesta en marcha • 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	<ul style="list-style-type: none"> • Puesta en marcha • Inventario 	Visualización, planificación y análisis
	ec2:DescribeSubnets	<ul style="list-style-type: none"> • Puesta en marcha • 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 descritas	Puesta en marcha	Visualización, planificación y análisis
	ec2:DescribeRouteTables	<ul style="list-style-type: none"> • Puesta en marcha • 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	<ul style="list-style-type: none"> • Puesta en marcha • 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:DescribeSnapshots	Explora el ahorro	Visualización, planificación y análisis
Obtén detalles de cada volumen de EBS adjunto para calcular los precios y el ahorro	ec2:DescribeVolumes	<ul style="list-style-type: none"> • Inventario • 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:DescribeKey	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:DescribeDirectories	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	<ul style="list-style-type: none"> • Inventario • Explore Ahorros 	Visualización, planificación y análisis
	fsx:DescribeBackups	<ul style="list-style-type: none"> • Inventario • Explore Ahorros 	Visualización, planificación y análisis
	fsx:DescribeStorageVirtualMachines	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión • Inventario 	Visualización, planificación y análisis
	fsx:DescribeFileSystems	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión • Inventario • 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	<ul style="list-style-type: none"> Operaciones de gestión Inventario Explora el ahorro Optimización 	Visualización, planificación y análisis
Enviar comandos a través de SSM a instancias EC2 para su detección y gestión.	ssm:SendCommand	<ul style="list-style-type: none"> Operaciones de gestión Inventario Explora el ahorro Optimización 	Visualización, planificación y análisis
Obtener el estado de conectividad de SSM en las instancias posteriores al despliegue	ssm:GetConnectionStatus	<ul style="list-style-type: none"> Operaciones de gestión Inventario 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	<ul style="list-style-type: none"> • Explora el ahorro • 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	<ul style="list-style-type: none"> • Explora el ahorro • 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	<ul style="list-style-type: none"> • Explora el ahorro • 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	<ul style="list-style-type: none"> • Explora el ahorro • Optimización 	Creación de host de base de datos
Compruebe la asociación de instancias a grupos de escala automática	escala automática:DescripciónAutoScalingGroups	<ul style="list-style-type: none"> • Explora el ahorro • Optimización 	Creación de host de base de datos
	escala automática:DescripciónAutoScalingInstances	<ul style="list-style-type: none"> • Explora el ahorro • 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	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión • Inventario 	Visualización, planificación y análisis
	ssm:GetParameters ¹	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión • Inventario 	Visualización, planificación y análisis
	ssm:PutParameter ¹	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión 	Visualización, planificación y análisis
	ssm>DeleteParameters ¹	<ul style="list-style-type: none"> • Puesta en marcha • 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:DisassociateAddress	Puesta en marcha	Creación de host de base de datos
	ec2:DisassociateIamInstanceProfile	Puesta en marcha	Creación de host de base de datos
	EC2:DisassociateRouteTable	Puesta en marcha	Creación de host de base de datos
	EC2:DisassociateSubnetCidrBlock	Puesta en marcha	Creación de host de base de datos
	EC2:DisassociateVpcCidrBlock	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:ModifyInstanceAttribute	Puesta en marcha	Operaciones y remediación
	EC2:ModifyInstanceColocación	Puesta en marcha	Creación de host de base de datos
	ec2:ModifyNetworkInterfaceAttribute	Puesta en marcha	Creación de host de base de datos
	EC2:ModifySubnetAttribute	Puesta en marcha	Creación de host de base de datos
	ec2:ModifyVolume	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:StartInstances	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	<ul style="list-style-type: none"> Puesta en marcha 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:DescribeStacks	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:DescribeInstances	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	<ul style="list-style-type: none"> • Puesta en marcha • 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 utilícelos 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	<ul style="list-style-type: none"> • Puesta en marcha • 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	<ul style="list-style-type: none"> • Evaluación del almacenamiento (optimización) • 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:DescribeLogGroups	<ul style="list-style-type: none"> • Evaluación del almacenamiento (optimización) • 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	<ul style="list-style-type: none"> Evaluación del almacenamiento (optimización) 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.

```
{
  "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:DescribeStacks	Puesta en marcha	Lectura/Escritura
Enumere las regiones del asistente de despliegue del motor AI	ec2:regiones descritas	Puesta en marcha	Lectura/Escritura
Mostrar etiquetas de motor AI	ec2:etiquetas a describirTags	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:DescribeInstances	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:DescribeLogGroups	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:DescribeLogStreams	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:



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 o de datos
Cree volúmenes de EBS	fsx:CreateVolume	Puesta en marcha	Despliegue y conectividad del almacenamiento o 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 o de datos
Cree y valide la plantilla de CloudFormation	Cloudformation:CreateStack	Puesta en marcha	Despliegue y conectividad del almacenamiento o de datos
Gestionar etiquetas y seguridad de red en las instancias creadas	ec2:CreateSecurityGroup	Puesta en marcha	Despliegue y conectividad del almacenamiento o de datos
Inicie las instancias creadas	ec2:RunInstances	Puesta en marcha	Despliegue y conectividad del almacenamiento o de datos
Obtenga los detalles de las instancias de EC2	ec2:DescribeInstances	Inventario	Despliegue y conectividad del almacenamiento o 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 o 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	<ul style="list-style-type: none"> • Puesta en marcha • Inventario 	Visualización, planificación y análisis
Obtener las subredes del entorno seleccionado para completar el formulario de despliegue	ec2:DescribeSubnets	<ul style="list-style-type: none"> • Puesta en marcha • 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	<ul style="list-style-type: none"> • Puesta en marcha • Inventario 	Visualización, planificación y análisis
Obtén las regiones con soporte de Amazon FSx para NetApp ONTAP	ec2:regiones descritas	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:DescribeKey	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 o de datos
	fsx:CreateStorageVirtualMachine	Puesta en marcha	Despliegue y conectividad del almacenamiento o de datos
	fsx:CreateVolume	<ul style="list-style-type: none"> • Puesta en marcha • Operaciones de gestión 	Despliegue y conectividad del almacenamiento o de datos
Obtén los detalles de Amazon FSx para NetApp ONTAP	fsx:describe*	<ul style="list-style-type: none"> • Puesta en marcha • Inventario • Operaciones de gestión • Explora el ahorro 	Despliegue y conectividad del almacenamiento o 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 o 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 o de datos
	Km:GenerateDataKey	Puesta en marcha	Despliegue y conectividad del almacenamiento o 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 o 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	<ul style="list-style-type: none"> Despliegue y conectividad del almacenamiento de datos 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`.

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

Inicio rápido para NetApp Workload Factory

Comience a utilizar NetApp Workload Factory registrándose y creando una cuenta, agregando credenciales para que Workload Factory pueda administrar los recursos de AWS directamente y luego optimice sus cargas de trabajo mediante Amazon FSx for NetApp ONTAP.

NetApp Workload Factory es accesible para los usuarios como un servicio en la nube desde la consola web. Antes de comenzar, debes comprender ["Fábrica de carga de trabajo"](#).

1

Regístrate y crea una cuenta

Ir a la ["Consola de Workload Factory"](#), regístrate y crea una cuenta.

["Aprenda a registrarse y a crear una cuenta"](#).

2

Agregar credenciales de AWS a Workload Factory

Este paso es opcional. Puede utilizar Workload Factory sin necesidad de añadir credenciales para acceder a su cuenta de AWS. Al agregar las credenciales de AWS a Workload Factory, su cuenta de Workload Factory obtiene los permisos necesarios para crear y administrar sistemas de archivos FSx para ONTAP y para implementar y administrar cargas de trabajo específicas, como bases de datos y GenAI.

["Aprenda a agregar credenciales a su cuenta"](#).

3

Optimiza tus cargas de trabajo usando FSx para ONTAP

Una vez que se haya registrado, creado una cuenta y, opcionalmente, agregado credenciales de AWS, puede comenzar a usar Workload Factory para optimizar sus cargas de trabajo usando FSx para ONTAP.

["Optimice sus cargas de trabajo con FSx para ONTAP"](#).

Regístrese en NetApp Workload Factory

Se puede acceder a NetApp Workload Factory desde una consola basada en web. Cuando comienza a utilizar Workload Factory, el primer paso es registrarse utilizando sus credenciales existentes del sitio de soporte de NetApp o creando un inicio de sesión en la nube de NetApp.

También puedes invitar a otras personas a unirse a tu cuenta de Workload Factory para que puedan acceder y utilizar Workload Factory.

Regístrate en Workload Factory

Puedes registrarte en Workload Factory utilizando una de las siguientes opciones:

- Sus credenciales existentes del sitio de soporte de NetApp (NSS)
- Inicio de sesión en el cloud de NetApp especificando su dirección de correo electrónico y una contraseña

Pasos

1. Abra un navegador web y vaya a "[Consola de Workload Factory](#)"
2. Si tienes una cuenta del sitio de soporte de NetApp, introduce la dirección de correo electrónico asociada con tu cuenta de NSS directamente en la página **Iniciar sesión**.

Puede omitir la página de registro si tiene una cuenta NSS. Workload Factory lo registrará como parte de este inicio de sesión inicial.

3. Si no tienes una cuenta NSS y quieres registrarte mediante la creación de un inicio de sesión en la nube de NetApp, selecciona **Regístrate**.

Sign up to Workload Factory

Already signed up? [Log in](#)

4. En la página **Registrarse**, ingrese la información requerida para crear un inicio de sesión en la nube de NetApp y seleccione **Siguiente**.

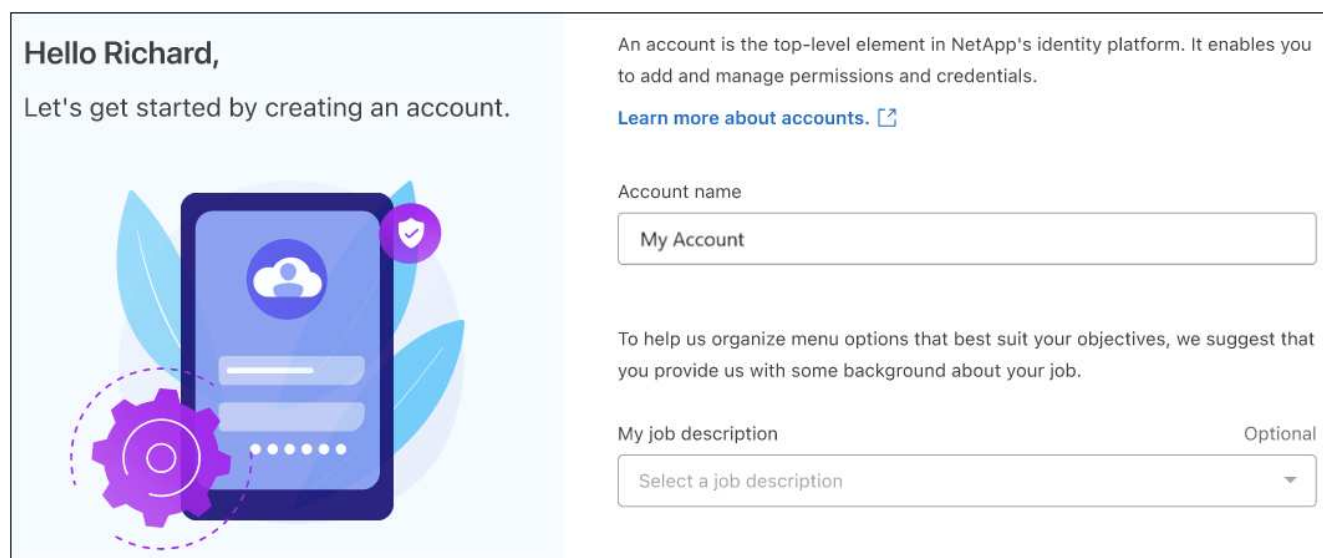
Tenga en cuenta que sólo se permiten caracteres ingleses en el formulario de registro.

5. Introduzca la información detallada de su empresa y seleccione **Registrarse**.
6. Compruebe en su bandeja de entrada si hay un correo electrónico de NetApp que incluya instrucciones para verificar su dirección de correo electrónico.


Este paso es necesario para poder iniciar sesión.

7. Cuando se le solicite, revise el Acuerdo de licencia de usuario final y acepte los términos y seleccione * Continuar *.
8. En la página **Cuenta**, ingrese un nombre para su cuenta y, opcionalmente, seleccione su descripción del trabajo.

Una cuenta es el elemento de nivel superior de la plataforma de identidad de NetApp y permite añadir y gestionar permisos y credenciales.



Hello Richard,
Let's get started by creating an account.

An account is the top-level element in NetApp's identity platform. It enables you to add and manage permissions and credentials.
[Learn more about accounts.](#) 

Account name

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

My job description Optional

9. Seleccione **Crear** y se mostrará la página de inicio de Workload Factory.

Resultado

Ahora tiene un inicio de sesión y una cuenta de Workload Factory. Se le considera administrador de cuenta y tiene acceso a todas las funciones de Workload Factory.

Invitar a otros a unirse a una cuenta en Workload Factory

Como administrador de cuenta, puede invitar a otras personas a unirse a su cuenta de Workload Factory para que puedan acceder y utilizar Workload Factory. La gestión de cuentas solo es posible desde la NetApp Console.

Consulte la documentación de la NetApp Console para "[Aprenda cómo agregar miembros \(cuentas de usuario\)](#)", a su cuenta de Workload Factory.

Resultado

El usuario invitado recibirá un correo electrónico con instrucciones para unirse a su cuenta de Workload

Agregar credenciales de AWS a Workload Factory

Agregue y administre las credenciales de AWS para que NetApp Workload Factory tenga los permisos que necesita para implementar y administrar recursos de la nube en sus cuentas de AWS.

Descripción general

Puede agregar credenciales de AWS a una cuenta de Workload Factory existente desde la página Credenciales. Esto proporciona a Workload Factory los permisos necesarios para administrar recursos y procesos dentro de su entorno de nube de AWS.

Puede agregar credenciales mediante dos métodos:

- **Manualmente:** crea la política de IAM y el rol de IAM en tu cuenta de AWS mientras agregas credenciales en Workload Factory.
- **Automáticamente:** Usted captura una cantidad mínima de información sobre los permisos y luego usa una pila CloudFormation para crear las políticas y el rol de IAM para sus credenciales.

Credenciales de AWS

Hemos diseñado un flujo de registro de credenciales de AWS Assume Role que:

- Admite permisos de cuenta de AWS más alineados, ya que le permite especificar las capacidades de carga de trabajo que desea usar y proporcionar requisitos de política de IAM de acuerdo con dichas selecciones.
- Permite ajustar los permisos de cuenta de AWS concedidos cuando se suscriban o se inhabiliten funcionalidades de cargas de trabajo específicas.
- Simplifica la creación manual de políticas de IAM al proporcionar archivos de políticas JSON personalizados que puede aplicar en la consola de AWS.
- Simplifica aún más el proceso de registro de credenciales al ofrecer a los usuarios una opción automatizada para la política de IAM requerida y la creación de roles mediante las pilas AWS CloudFormation.
- Se alinea mejor con los usuarios de FSx para ONTAP, que prefieren que sus credenciales se almacenen en los límites del ecosistema de cloud de AWS al permitir el almacenamiento de las credenciales de los servicios de FSx para ONTAP en un back-end de gestión secreta basado en AWS.

Una o más credenciales de AWS

Cuando utilice su primera capacidad (o capacidades) de Workload Factory, deberá crear las credenciales utilizando los permisos necesarios para esas capacidades de carga de trabajo. Agregará las credenciales a Workload Factory, pero necesitará acceder a la Consola de administración de AWS para crear la función y la política de IAM. Estas credenciales estarán disponibles en su cuenta cuando utilice cualquier capacidad en Workload Factory.

Tu conjunto inicial de credenciales de AWS puede incluir una política de permisos de IAM para una o varias funcionalidades. Depende de las necesidades de tu negocio.

Agregar más de un conjunto de credenciales de AWS a Workload Factory proporciona permisos adicionales

necesarios para usar capacidades adicionales, como sistemas de archivos FSx para ONTAP , implementar bases de datos en FSx para ONTAP, migrar cargas de trabajo de VMware y más.

Agregar credenciales a una cuenta manualmente

Puede agregar credenciales de AWS a Workload Factory manualmente para otorgarle a su cuenta de Workload Factory los permisos necesarios para administrar los recursos de AWS que usará para ejecutar sus cargas de trabajo únicas. Cada conjunto de credenciales que agregue incluirá una o más políticas de IAM según las capacidades de carga de trabajo que desee utilizar y un rol de IAM asignado a su cuenta.



Puede agregar credenciales de AWS a una cuenta desde la consola de Workload Factory o desde la consola de NetApp .

Hay tres partes para crear las credenciales:

- Seleccione el nivel de servicios y permisos que desea utilizar y, a continuación, cree políticas de IAM desde la consola de administración de AWS.
- Cree un rol de IAM desde la consola de administración de AWS.
- Desde Workload Factory, ingrese un nombre y agregue las credenciales.


Antes de empezar

Necesitarás disponer de credenciales para iniciar sesión en tu cuenta de AWS.

Pasos


1. Iniciar sesión en el "Consola de Workload Factory" .
2. Desde el menú, seleccione **Administración** y luego **Credenciales**.
3. En la página Credenciales, seleccione **Añadir credenciales**.
4. En la página Agregar credenciales, seleccione **Agregar manualmente** y luego use los siguientes pasos para completar cada sección en *Configuración de permisos*.


Add Credentials



Add manually

Independently create IAM policy and IAM role in you AWS account according to detailed instructions and a provided permissions list which is based on your requirements.






Add via AWS Cloud Formation

IAM policy and role creation are automated via a Cloud Formation stack which is self executed by you. No account management permissions are required by Workload Factory.


Permissions configuration


Create policies

No policies were selected





Create role

 Action required



Credentials name

 Action required



Paso 1: Seleccione las capacidades de carga de trabajo y cree las políticas de IAM

En esta sección, podrá elegir qué tipos de funcionalidades de carga de trabajo se gestionarán como parte de estas credenciales y los permisos habilitados para cada carga de trabajo. Tendrá que copiar los permisos de política para cada carga de trabajo seleccionada desde CodeBox y agregarlos a la consola de administración de AWS dentro de su cuenta de AWS para crear las políticas.

Pasos

1. Desde la sección **Crear políticas**, habilite cada una de las capacidades de carga de trabajo que desea incluir en estas credenciales.

Puede añadir más funcionalidades más adelante, solo tiene que seleccionar las cargas de trabajo que desee poner en marcha y gestionar actualmente.
2. Para aquellas funcionalidades de carga de trabajo que ofrecen una selección de políticas de permisos, seleccione el tipo de permisos que estarán disponibles con estas credenciales.
3. Opcional: Seleccione **Activar verificación automática de permisos** para comprobar si tiene los permisos de cuenta de AWS necesarios para completar las operaciones de carga de trabajo. Al activar la comprobación, se agrega `iam:SimulatePrincipalPolicy` permission a las políticas de permisos. El propósito de este permiso es confirmar los permisos solamente. Puede eliminar el permiso después de agregar credenciales, pero le recomendamos que lo mantenga para evitar la creación de recursos para operaciones parcialmente correctas y para ahorrarle cualquier limpieza manual de recursos necesaria.
4. En la ventana CodeBox, copie los permisos de la primera directiva IAM.
5. Abra otra ventana del explorador e inicie sesión en su cuenta de AWS en la consola de administración de AWS.
6. Abra el servicio IAM y seleccione **Políticas > Crear política**.
7. Seleccione JSON como tipo de archivo, pegue los permisos que copió en el paso 3 y seleccione **Siguiente**.
8. Introduzca el nombre de la política y seleccione **Crear política**.
9. Si seleccionó varias capacidades de carga de trabajo en el paso 1, repita estos pasos para crear una política para cada conjunto de permisos de carga de trabajo.

Paso 2: Cree el rol de IAM que utiliza las políticas

En esta sección, configurará un rol de IAM que Workload Factory asumirá y que incluye los permisos y las políticas que acaba de crear.

Permissions configuration

Create role

From the AWS Management Console

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

Role ARN

Pasos

1. En la consola de administración de AWS, seleccione **Roles > Crear rol**.
2. En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
 - a. Seleccione **Otra cuenta de AWS** y copie y pegue el ID de la cuenta para la administración de carga de trabajo de FSx para ONTAP desde la interfaz de usuario de Workload Factory.
 - b. Seleccione **ID externa requerida** y copie y pegue la ID externa desde la interfaz de usuario de Workload Factory.
3. Seleccione **Siguiente**.
4. En la sección Política de permisos, elige todas las políticas que definiste anteriormente y selecciona **Siguiente**.
5. Introduzca un nombre para el rol y seleccione **Crear rol**.
6. Copie el rol ARN.
7. Regrese a la página Agregar credenciales en Workload Factory, expanda la sección **Crear rol** en **Configuración de permisos** y pegue el ARN en el campo *ARN de rol*.

Paso 3: Introduzca un nombre y agregue las credenciales

El paso final es ingresar un nombre para las credenciales en Workload Factory.

Pasos

1. Desde la página Agregar credenciales en Workload Factory, expanda **Nombre de credenciales** en **Configuración de permisos**.
2. Introduzca el nombre que desee usar para estas credenciales.
3. Seleccione **Agregar** para crear las credenciales.

Resultado

Las credenciales se crean y se devuelve a la página Credenciales.

Agregue credenciales a una cuenta usando CloudFormation

Puede agregar credenciales de AWS a Workload Factory mediante una pila de AWS CloudFormation seleccionando las capacidades de Workload Factory que desea usar y luego iniciando la pila de AWS CloudFormation en su cuenta de AWS. CloudFormation creará las políticas de IAM y el rol de IAM en función de las capacidades de carga de trabajo que usted seleccionó.

Antes de empezar

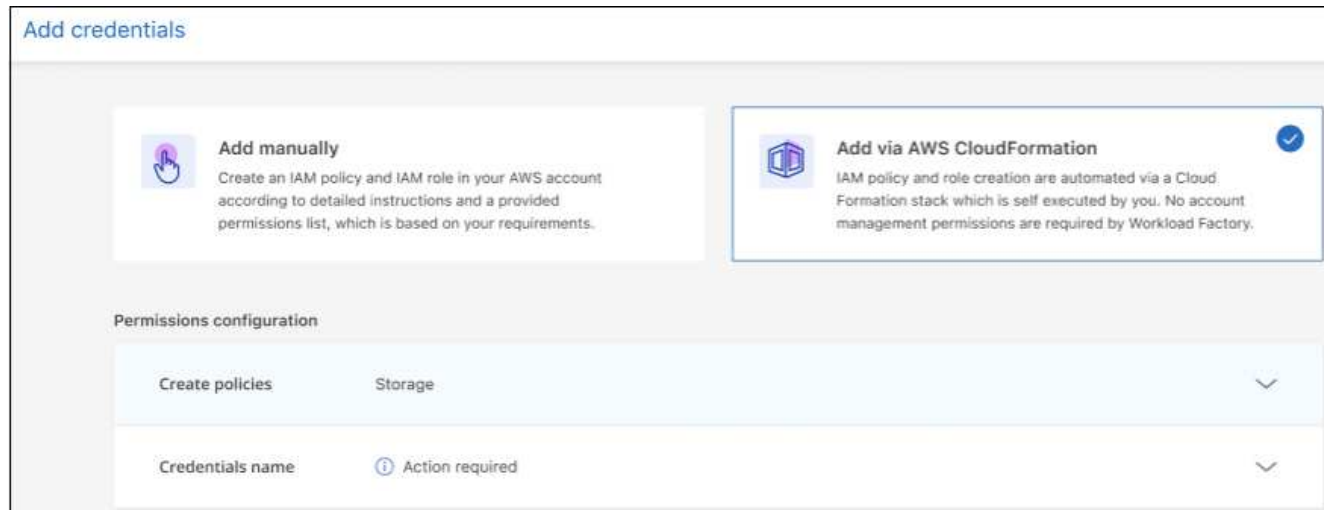
- Necesitarás disponer de credenciales para iniciar sesión en tu cuenta de AWS.
- Necesitará tener los siguientes permisos en su cuenta de AWS al agregar credenciales mediante una pila de CloudFormation:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

Pasos

1. Iniciar sesión en el ["Consola de Workload Factory"](#) .

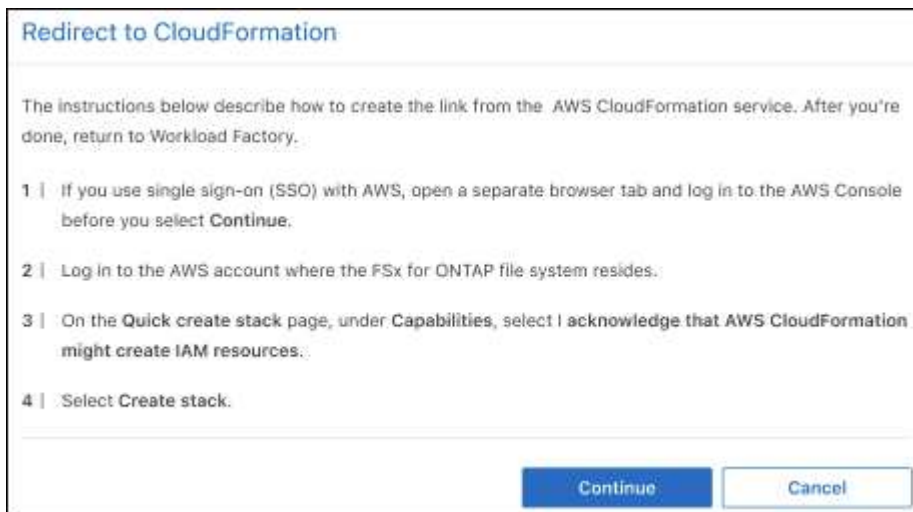
2. Desde el menú, seleccione **Administración** y luego **Credenciales**.
3. En la página Credenciales, seleccione **Añadir credenciales**.
4. Seleccione **Añadir a través de AWS CloudFormation**.



5. En **Crear políticas**, habilite cada una de las capacidades de carga de trabajo que desea incluir en estas credenciales y elija un nivel de permiso para cada carga de trabajo.

Puede añadir más funcionalidades más adelante, solo tiene que seleccionar las cargas de trabajo que desee poner en marcha y gestionar actualmente.

6. Opcional: Seleccione **Activar verificación automática de permisos** para comprobar si tiene los permisos de cuenta de AWS necesarios para completar las operaciones de carga de trabajo. Al activar la comprobación, se agrega el `iam:SimulatePrincipalPolicy` permiso a las políticas de permisos. El propósito de este permiso es confirmar los permisos solamente. Puede eliminar el permiso después de agregar credenciales, pero le recomendamos que lo mantenga para evitar la creación de recursos para operaciones parcialmente correctas y para ahorrarle cualquier limpieza manual de recursos necesaria.
7. En **Nombre de Credenciales**, introduzca el nombre que desea utilizar para estas credenciales.
8. Agregue las credenciales de AWS CloudFormation:
 - a. Seleccione **Agregar** (o seleccione **Redirigir a CloudFormation**) y se mostrará la página Redirigir a CloudFormation.



- b. Si usa el inicio de sesión único (SSO) con AWS, abra una pestaña del explorador independiente e inicie sesión en la consola de AWS antes de seleccionar **Continuar**.

Debe iniciar sesión en la cuenta de AWS en la que reside el sistema de archivos de FSx para ONTAP.

- c. Seleccione **Continuar** en la página Redirigir a CloudFormation.
- d. En la página Quick create stack, en Capacidades, seleccione **Reconozco que AWS CloudFormation podría crear recursos de IAM**.
- e. Seleccione **Crear pila**.
- f. Regrese a Workload Factory y monitoree la página Credenciales para verificar que las nuevas credenciales estén en progreso o que se hayan agregado.

Optimice las cargas de trabajo con NetApp Workload Factory

Una vez que haya iniciado sesión y configurado NetApp Workload Factory, puede comenzar a usar varias capacidades de Workload Factory, como la creación de sistemas de archivos de Amazon FSx para ONTAP, la implementación de bases de datos en sistemas de archivos de FSx para ONTAP y la migración de configuraciones de máquinas virtuales a VMware Cloud on AWS usando sistemas de archivos de FSx para ONTAP como almacenes de datos externos.

- ["Amazon FSX para ONTAP de NetApp"](#)

Evalúa y analiza el estado de los datos actuales para ahorrar posibles costes usando FSx para ONTAP como infraestructura de almacenamiento, aprovisiona y templatiza las implementaciones de FSx para ONTAP basadas en prácticas recomendadas y accede a funcionalidades de gestión avanzadas.

- ["Cargas de trabajo de base de datos"](#)

Detecta el estado de tus bases de datos actuales en AWS, evalúa el posible ahorro en costes cambiando a FSx para ONTAP, pon en marcha bases de datos integrales con prácticas recomendadas incorporadas para la optimización y automatiza la clonación ligera para las canalizaciones de CI/CD.

- ["GenAI"](#)

Implemente y gestione una infraestructura de generación aumentada de recuperación (RAG) para mejorar la precisión y la singularidad de sus aplicaciones de IA. Crea una base de conocimientos de RAG en FSx para ONTAP con seguridad de datos y cumplimiento normativo integrados.

- ["Cargas de trabajo de"](#)

Simplifique las migraciones y las operaciones con recomendaciones inteligentes y soluciones automáticas. Ponga en marcha backups eficientes y una sólida recuperación ante desastres. Supervise sus máquinas virtuales y solucione problemas.

- ["Cargas de trabajo de EDA"](#)

Optimice FSx para ONTAP en múltiples sistemas de archivos para mejorar el rendimiento y reducir los costos operativos mediante la gestión automatizada de parámetros de almacenamiento.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.