AWS Documento técnico

SageMaker Mejores prácticas de administración de Studio

SageMaker Mejores prácticas de administración de Studio: AWS Documento técnico

Table of Contents

Prácticas recomendadas de administración de SageMaker Studio

Fecha de publicación: 25 de abril de 2023 (Revisiones del documento)

Resumen

Amazon SageMaker Studio proporciona una única interfaz visual basada en la web donde puede realizar todos los pasos de desarrollo de machine learning (ML), lo que mejora la productividad del equipo de ciencia de datos. SageMaker Studio proporciona acceso, control y visibilidad completos de cada paso necesario para crear, entrenar y evaluar modelos.

En este documento técnico, analizamos las prácticas recomendadas en temas como el modelo operativo, la administración de dominios, la administración de identidades, la administración de permisos, la administración de redes, el registro, la supervisión y la personalización. Las prácticas recomendadas que se describen aquí están indicadas para la implementación empresarial de SageMaker Studio, incluidas las implementaciones de varios inquilinos. Este documento está dirigido a administradores de plataformas de ML, ingenieros de ML y arquitectos de ML.

¿Tiene Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables y sostenibles. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la AWS Management Console, puede comparar las cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

En el Enfoque de Machine Learning, nos centramos en cómo diseñar, implementar y crear las cargas de trabajo de machine learning en Nube de AWS. Este enfoque se suma a las prácticas recomendadas descritas en el Marco de Well-Architected.

Introducción

Cuando administra SageMaker Studio como su plataforma de machine learning, necesita orientación sobre las prácticas recomendadas para tomar decisiones informadas que le ayuden a escalar su

plataforma de machine learning a medida que crecen sus cargas de trabajo. Para aprovisionar, poner en funcionamiento y escalar su plataforma de machine learning, tenga en cuenta lo siguiente:

- Elija el modelo operativo adecuado y organice sus entornos de machine learning para cumplir sus objetivos empresariales.
- Elija cómo configurar la autenticación de dominios de SageMaker Studio para las identidades de usuario y tenga en cuenta las limitaciones a nivel de dominio.
- Decida cómo federar la identidad y la autorización de sus usuarios con la plataforma de machine learning para realizar auditorías y controles de acceso detallados.
- Se recomienda configurar permisos y barreras de protección para los distintos roles de las personas de machine learning.
- Planifique la topología de su red de nube privada virtual (VPC) teniendo en cuenta la sensibilidad de la carga de trabajo de machine learning, la cantidad de usuarios, los tipos de instancias, las aplicaciones y los trabajos lanzados.
- Clasifique y proteja los datos en reposo y en tránsito con cifrado.
- Considere cómo registrar y supervisar las diversas interfaces de programación de aplicaciones (API) y las actividades de los usuarios para garantizar la conformidad.
- Personalice la experiencia del cuaderno de SageMaker Studio con sus propias imágenes y scripts de configuración del ciclo de vida.

Modelo operativo

Un modelo operativo es una infraestructura que combina las personas, los procesos y las tecnologías para ayudar a una organización a ofrecer valor empresarial de manera escalable, coherente y eficiente. El modelo operativo de machine learning proporciona un proceso de desarrollo de productos estándar para los equipos de toda la organización. Hay tres modelos para implementar el modelo operativo, según el tamaño, la complejidad y los factores que impulsan el negocio:

- Equipo de ciencia de datos centralizado: en este modelo, todas las actividades de ciencia de datos se centralizan en un solo equipo u organización. Esto es similar al modelo del Centro de excelencia (COE), donde todas las unidades de negocio recurren a este equipo para realizar proyectos de ciencia de datos.
- Equipos de ciencia de datos descentralizados: en este modelo, las actividades de ciencia de datos se distribuyen en diferentes funciones o divisiones comerciales, o en función de diferentes líneas de productos.
- Equipos de ciencia de datos federados: en este modelo, las funciones de servicios compartidos como, por ejemplo, los repositorios de código, los procesos de integración y entrega continuas (CI/CD), etc., están administradas por un equipo centralizado, y cada unidad de negocio o función a nivel de producto está administrada por equipos descentralizados. Esto es similar al modelo en estrella, donde cada unidad de negocio tiene sus propios equipos de ciencia de datos; sin embargo, estos equipos de unidades de negocio coordinan sus actividades con el equipo centralizado.

Antes de decidir lanzar su primer dominio de estudio para casos de uso de producción, tenga en cuenta el modelo operativo y las prácticas recomendadas de AWS para organizar su entorno. Para obtener más información, consulte Organización de su entorno de AWS con varias cuentas.

La siguiente sección proporciona orientación sobre cómo organizar la estructura de la cuenta para cada uno de los modelos operativos.

Estructura contable recomendada

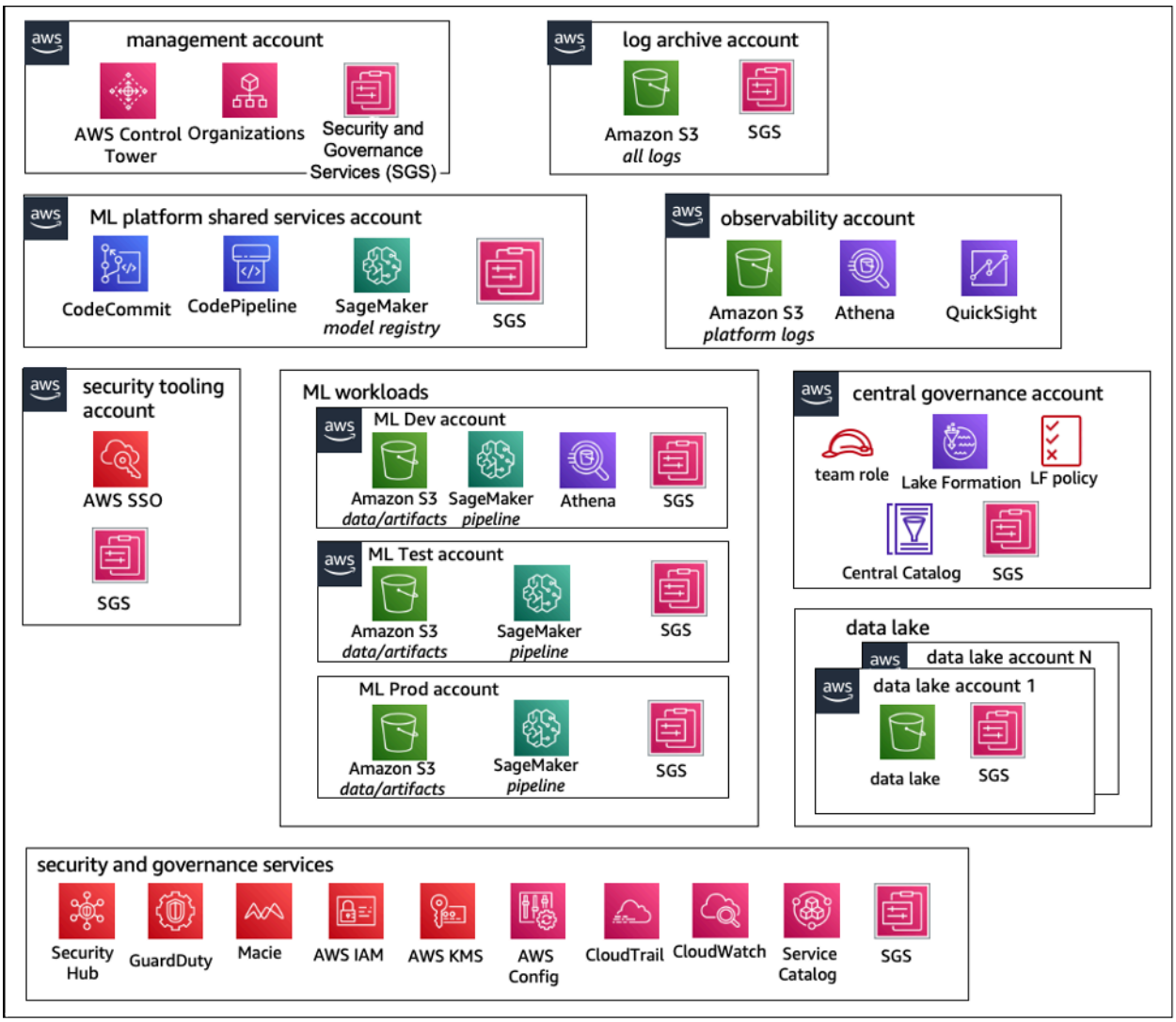
En esta sección, presentamos brevemente una estructura contable de modelo operativo con la que puede empezar y modificar de acuerdo con los requisitos operativos de su organización. Independientemente del modelo operativo que elija, le recomendamos implementar las siguientes prácticas recomendadas comunes:

- Utilice AWS Control Tower para configurar, administrar y gobernar sus cuentas.
- Centralice sus identidades con su proveedor de identidades (IdP) y AWS IAM Identity Center con una cuenta Securitiy Tooling de administrador delegado y permita el acceso seguro a las cargas de trabajo.
- Ejecute cargas de trabajo de machine learning con aislamiento a nivel de cuenta en todas las cargas de trabajo de desarrollo, prueba y producción.
- Transmita los registros de las cargas de trabajo de machine learning a una cuenta de archivo de registros y, a continuación, filtre y aplique el análisis de registros en una cuenta de observabilidad.
- Ejecute una cuenta de gobierno centralizada para aprovisionar, controlar y auditar el acceso a los datos.
- Integre los servicios de seguridad y gobierno (SGS) con las barreras de protección y detección adecuadas en cada cuenta para garantizar la seguridad y la conformidad, según los requisitos de su organización y su carga de trabajo.

Estructura de cuentas de modelo centralizado

En este modelo, el equipo de la plataforma de machine learning es responsable de proporcionar:

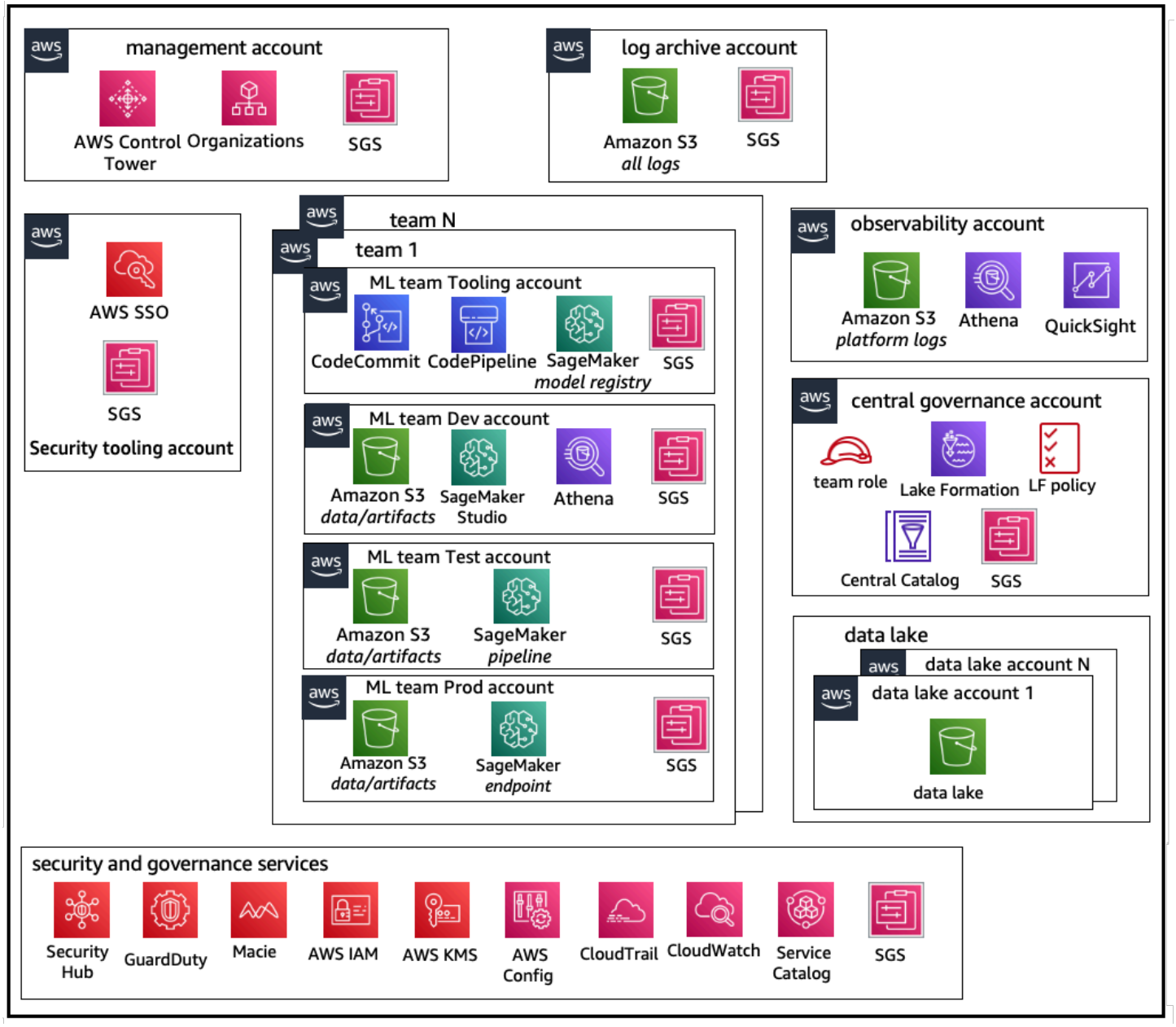
- Una cuenta de herramientas de servicios compartidos que aborda los requisitos de Machine Learning Operations (MLOp) de los equipos de ciencia de datos.
- Cuentas de desarrollo, prueba y producción de cargas de trabajo de machine learning que se comparten entre los equipos de ciencia de datos.
- Políticas de gobierno para garantizar que cada carga de trabajo de equipo de ciencia de datos se ejecute de forma aislada.
- Prácticas recomendadas comunes.



Estructura de cuentas de un modelo operativo centralizado

Estructura de cuentas de modelo descentralizado

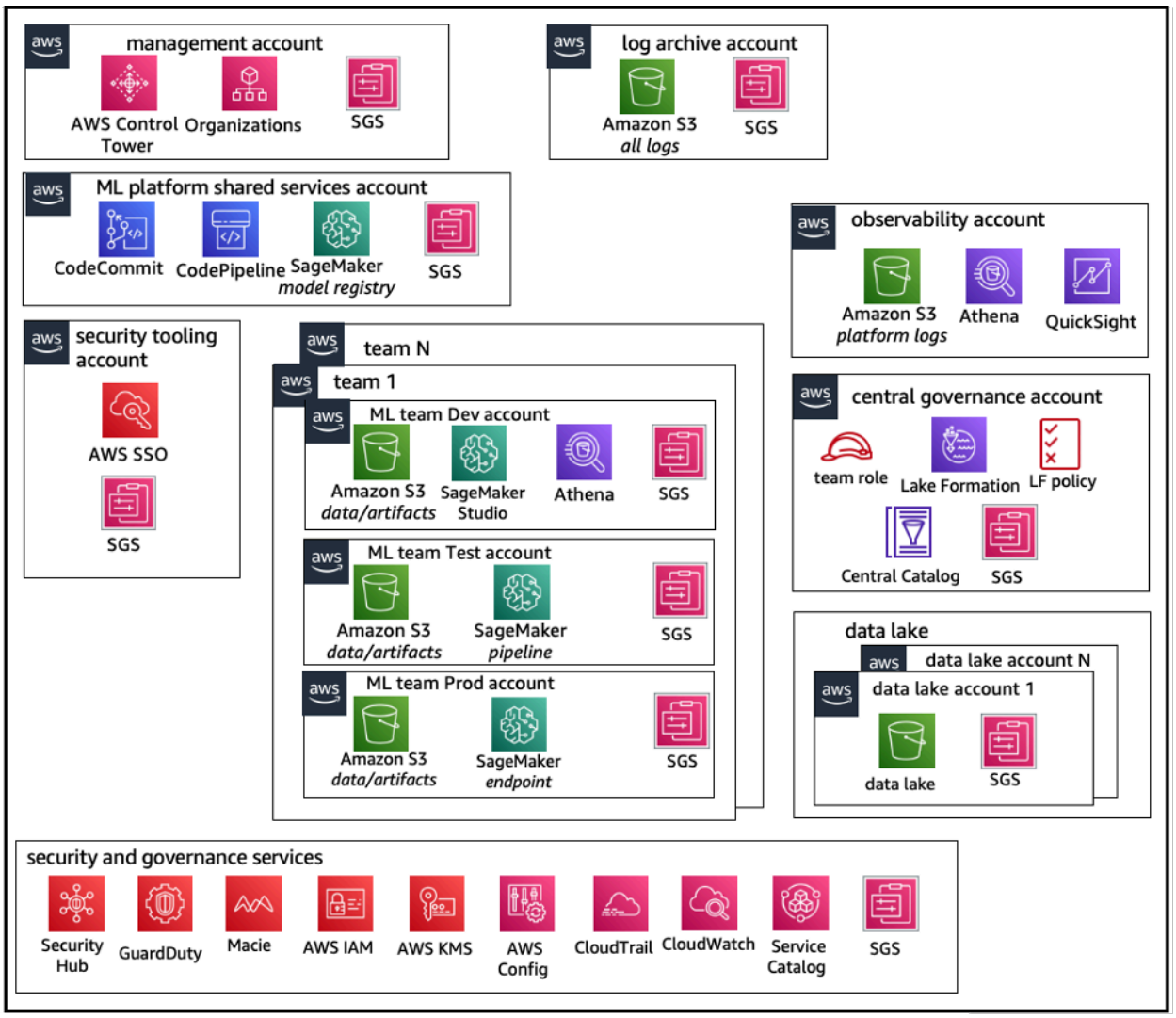
En este modelo, cada equipo de machine learning opera de forma independiente para aprovisionar, administrar y gobernar las cuentas y los recursos de machine learning. Sin embargo, recomendamos que los equipos de machine learning utilicen un enfoque centralizado de modelo de observabilidad y gobernanza de datos para simplificar la gobernanza de los datos y la administración de las auditorías.



Estructura de cuentas de modelo operativo descentralizado

Estructura de cuentas de modelo federado

Este modelo es similar al modelo centralizado; sin embargo, la diferencia clave es que cada equipo de ciencia de datos y machine learning tiene su propio conjunto de cuentas de carga de trabajo de desarrollo/prueba/producción, que permiten un aislamiento físico sólido de sus recursos de machine learning y, además, habilitan el escalado independiente de cada equipo sin afectar a los demás.



Estructura de cuentas de modelo operativo federado

Multitenencia de plataforma de ML

La multitenencia es una arquitectura de software donde una sola instancia de software puede atender a varios grupos de usuarios distintos. Un inquilino es un grupo de usuarios que comparten un acceso común con privilegios específicos a la instancia de software. Por ejemplo, si está creando varios productos de machine learning, cada equipo de producto con requisitos de acceso similares puede considerarse un inquilino o un equipo.

Aunque es posible implementar varios equipos dentro de una instancia de SageMaker Studio (por ejemplo, un Dominio de SageMaker), sopese las ventajas y desventajas como el radio de alcance, la atribución de costos y los límites a nivel de cuenta cuando agrupe varios equipos en un único

dominio de SageMaker Studio. Obtenga más información sobre las ventajas/desventajas y las prácticas recomendadas en las siguientes secciones.

Si necesita un aislamiento absoluto de los recursos, considere la posibilidad de implementar dominios de SageMaker Studio para cada inquilino en una cuenta diferente. En función de sus requisitos de aislamiento, puede implementar varias líneas de negocio (LOB) como varios dominios dentro de una sola cuenta y región. Utilice los espacios compartidos para una colaboración prácticamente en tiempo real entre los miembros del mismo equipo/LOB. Con varios dominios, seguirá utilizando los permisos y las políticas de Identity and Access Management (IAM) para garantizar el aislamiento de los recursos.

Los recursos de SageMaker creados a partir de un dominio se etiquetan automáticamente con el Nombre de recurso de Amazon (ARN) del dominio y el perfil de usuario o el ARN del espacio para facilitar el aislamiento de los recursos. Para ver ejemplos de políticas, consulte la documentación sobre el aislamiento de recursos del dominio. Aquí puede ver la referencia detallada sobre cuándo usar una estrategia de múltiples cuentas o múltiples dominios, junto con las comparaciones de características en la documentación, y ver ejemplos de scripts para reponer etiquetas para los dominios existentes en el repositorio de GitHub.

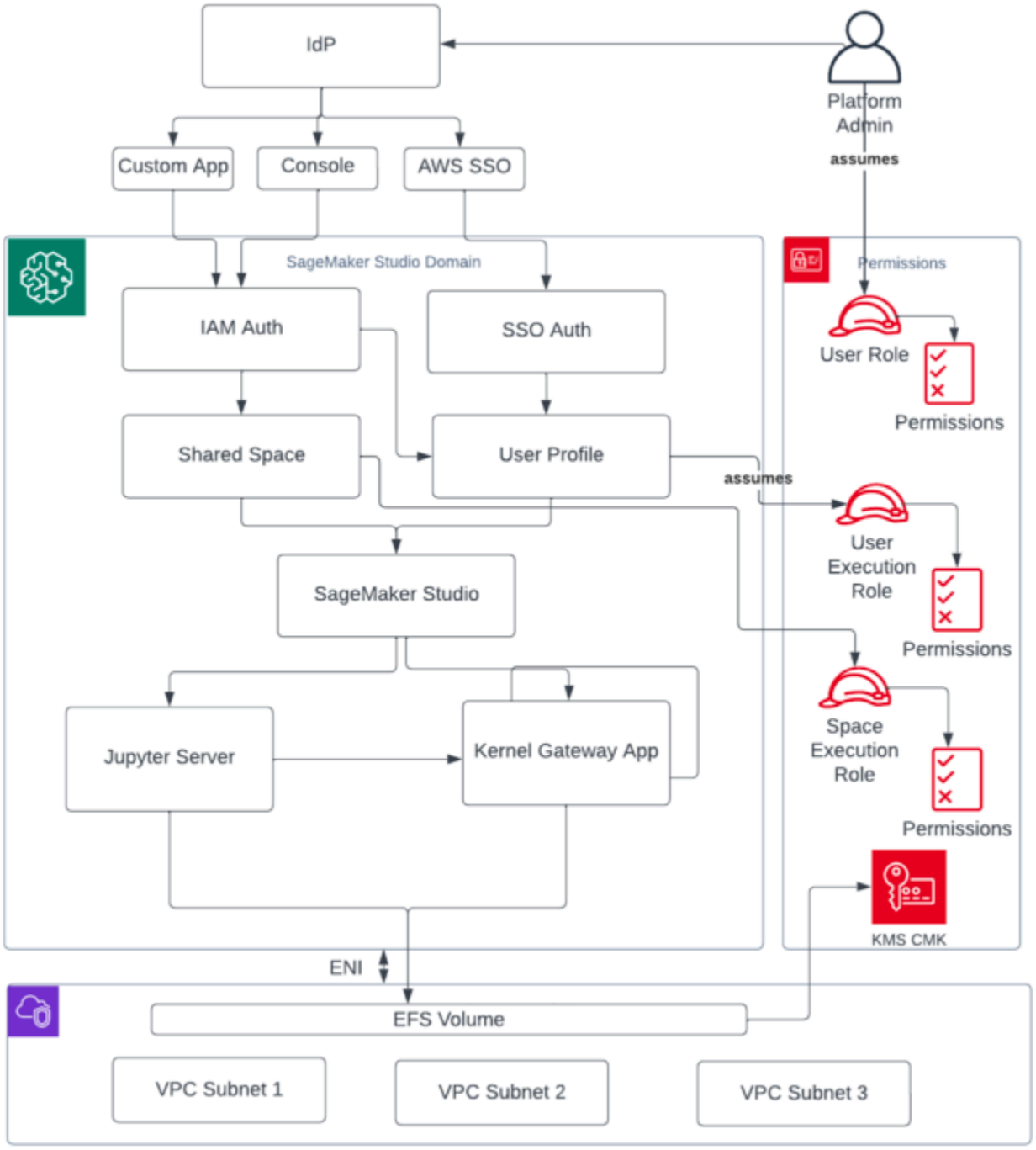
Por último, puede implementar una implementación de autoservicio de los recursos de SageMaker Studio en varias cuentas utilizando AWS Service Catalog. Para obtener más información, consulte Administrar productos de AWS Service Catalog en varias Cuentas de AWS y Regiones de AWS.

Administración de dominios

Un Dominio de Amazon SageMaker se compone de:

- Un volumen asociado de Amazon Elastic File System (Amazon EFS)
- Una lista de usuarios autorizados.
- Una amplia variedad de configuraciones de seguridad, aplicaciones, políticas y Amazon Virtual Private Cloud (Amazon VPC).

El siguiente diagrama proporciona una visión general sobre varios componentes que constituyen un dominio de SageMakerStudio:

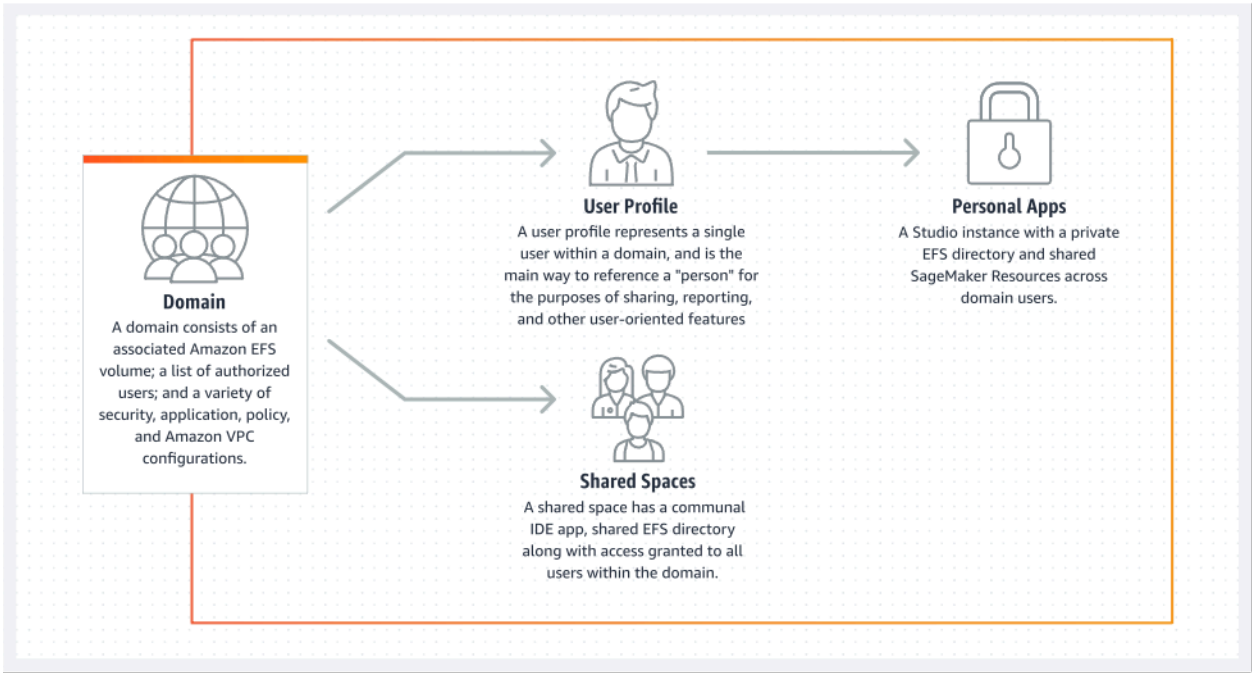


Visión general de varios componentes que constituyen un dominio de SageMaker Studio

Varios dominios y espacios compartidos

Amazon SageMaker ahora admite la creación de varios SageMaker dominios en uno solo Región de AWS para cada cuenta. Cada dominio puede tener su propia configuración de dominio, como el modo de autenticación, y una configuración de red, como la VPC y las subredes. Un perfil de usuario no se puede compartir entre varios dominios. Si un usuario humano forma parte de varios equipos separados por dominios, cree un perfil de usuario para el usuario en cada dominio. Consulte la Descripción general de varios dominios para obtener información sobre la reposición de etiquetas de los dominios existentes.

Cada dominio configurado en el modo de autenticación de IAM puede utilizar el espacio compartido para ofrecer una colaboración casi en tiempo real entre los usuarios. Con un espacio compartido, los usuarios tienen acceso a un directorio compartido de Amazon EFS y a una JupyterServeraplicación compartida para la interfaz de usuario, y pueden coeditar prácticamente en tiempo real. El etiquetado automático de los recursos creados por los espacios compartidos permite a los administradores realizar un seguimiento de los costos a nivel de proyecto. La JupyterServer interfaz de usuario compartida también filtra recursos como los experimentos y las entradas del registro de modelos, de modo que solo se muestren los elementos relevantes para la tarea de aprendizaje automático compartida. En el diagrama siguiente, se proporciona información general sobre las aplicaciones privadas y los espacios compartidos de cada dominio.



Descripción general de las aplicaciones privadas y los espacios compartidos dentro de un único dominio

Configura espacios compartidos en tu dominio

Por lo general, los espacios compartidos se crean para una actividad o proyecto de aprendizaje automático en particular, en el que los miembros de un único dominio requieren acceso casi en tiempo real al mismo almacenamiento de archivos y al mismo IDE subyacentes. El usuario puede acceder a sus libretas, leerlas, editarlas y compartirlas prácticamente en tiempo real, lo que le proporciona la forma más rápida de empezar a iterar con sus compañeros.

Para crear un espacio compartido, primero debe designar una función de ejecución predeterminada en el espacio que regirá los permisos de cualquier usuario que utilice el espacio. En el momento de escribir este artículo, todos los usuarios de un dominio tendrán acceso a todos los espacios compartidos de su dominio. Consulta Crear un espacio compartido para obtener la documentación más reciente sobre cómo añadir espacios compartidos a un dominio existente.

Configura tu dominio para la federación de IAM

Antes de configurar la federación AWS Identity and Access Management (IAM) para tu dominio de SageMaker Studio, debes configurar un rol de usuario de la federación de IAM (como un administrador de plataforma) en tu IdP, tal y como se explica en la sección Gestión de identidades.

Para obtener instrucciones detalladas sobre cómo configurar SageMaker Studio con la opción IAM, consulta Cómo integrar Amazon SageMaker Domain Using IAM Identity Center.

Configura tu dominio para la federación de inicio de sesión único (SSO)

Para usar la federación de inicio de sesión único (SSO), debes habilitarla AWS IAM Identity Center en tu cuenta de AWS Organizationsadministración en la misma región en la que necesitas ejecutar Studio. SageMaker Los pasos de configuración del dominio son similares a los pasos de la federación de IAM, con la salvedad de que se selecciona AWS IAM Identity Center(iDC) en la sección de autenticación.

Para obtener instrucciones detalladas, consulta Cómo incorporar un SageMaker dominio de Amazon mediante IAM Identity Center.

SageMaker Perfil de usuario de Studio

Un perfil de usuario representa a un único usuario dentro de un dominio y es la forma principal de hacer referencia a una "persona" con el propósito de compartir, generar informes y otras características orientadas al usuario. Esta entidad se crea cuando un usuario se incorpora a toSageMaker Studio. Si un administrador invita a una persona por correo electrónico o la importa desde IdC, se crea automáticamente un perfil de usuario. Un perfil de usuario es el principal titular de la configuración de un usuario individual y tiene una referencia al directorio particular privado de Amazon Elastic File System (Amazon EFS) del usuario. Recomendamos crear un perfil de usuario para cada usuario físico de la aplicación SageMaker Studio. Cada usuario tiene su propio directorio dedicado en Amazon EFS y los perfiles de usuario no se pueden compartir entre dominios de la misma cuenta.

Cada perfil de usuario que comparte el dominio de SageMaker Studio recibe recursos informáticos dedicados (como instancias de SageMaker Amazon Elastic Compute Cloud (Amazon EC2)) para ejecutar cuadernos. Las instancias informáticas asignadas al usuario uno están completamente aisladas de las asignadas al usuario dos. Del mismo modo, los recursos informáticos asignados a los usuarios de una AWS cuenta son completamente independientes de los asignados a los usuarios de otra cuenta. Cada usuario puede ejecutar hasta cuatro aplicaciones (aplicaciones) en contenedores Docker aislados o imágenes en el mismo tipo de instancia.

Aplicación Jupyter Server

Al lanzar un bloc de notas de Amazon SageMaker Studio para un usuario accediendo a la URL prefirmada o iniciando sesión con AWS IAM iDC, la aplicación Jupyter Server se lanza en la instancia de VPC gestionada por el servicio. SageMaker Cada usuario obtiene su propia aplicación dedicada de Jupyter Server en una aplicación privada. De forma predeterminada, la aplicación Jupyter Server para cuadernos SageMaker Studio se ejecuta en una *`ml.t3.medium`* instancia dedicada (reservada como tipo de instancia del sistema). El procesamiento de esta instancia no se factura al cliente.

La aplicación Jupyter Kernel Gateway

La aplicación Kernel Gateway se puede crear a través de la API o la interfaz de SageMaker Studio y se ejecuta en el tipo de instancia elegido. Esta aplicación se puede ejecutar con una de las imágenes

de SageMaker Studio integradas que están preconfiguradas con paquetes populares de ciencia de datos y aprendizaje profundo TensorFlow, como Apache MXNet y. PyTorch

Los usuarios pueden iniciar y ejecutar varios núcleos de cuadernos Jupyter, sesiones de terminal y consolas interactivas desde la misma SageMaker aplicación Studio Image/Kernel Gateway. Los usuarios también pueden ejecutar hasta cuatro aplicaciones o imágenes de Kernel Gateway en la misma instancia física, cada una aislada por su contenedor/imagen.

Para crear aplicaciones adicionales, debe usar un tipo de instancia diferente. Un perfil de usuario solo puede tener una instancia en ejecución, de cualquier tipo de instancia. Por ejemplo, un usuario puede ejecutar un bloc de notas simple con la imagen de ciencia de datos integrada de SageMaker Studio y otro bloc de notas con la TensorFlow imagen integrada, en la misma instancia. A los usuarios se les factura por el tiempo que la instancia esté en ejecución. Para evitar costes cuando el usuario no ejecuta SageMaker Studio de forma activa, debe cerrar la instancia. Para obtener más información, consulta Cómo cerrar y actualizar las aplicaciones de Studio.

Cada vez que cierra y vuelve a abrir una aplicación de Kernel Gateway desde la interfaz de SageMaker Studio, esa aplicación se inicia en una instancia nueva. Esto significa que la instalación del paquete no se prolonga hasta que se reinicie la misma aplicación. Del mismo modo, si un usuario cambia el tipo de instancia en un portátil, se pierden los paquetes instalados y las variables de sesión. Sin embargo, puede utilizar funciones como crear scripts de ciclo de vida e imagen propios para incorporar los paquetes del usuario a SageMaker Studio y conservarlos durante los cambios de instancia y el lanzamiento de nuevas instancias.

Volumen de Amazon Elastic File System

Cuando se crea un dominio, se crea un único volumen de Amazon Elastic File System (Amazon EFS) para ser utilizado por todos los usuarios del dominio. Cada perfil de usuario recibe un directorio principal privado dentro del volumen de Amazon EFS para almacenar las libretas, los GitHub repositorios y los archivos de datos del usuario. Cada espacio de un dominio recibe un directorio privado dentro del volumen de Amazon EFS al que pueden acceder varios perfiles de usuario. El acceso a las carpetas está segregado por usuario, mediante permisos del sistema de archivos. SageMaker Studio crea un ID de usuario global único para cada perfil o espacio de usuario y lo aplica como un ID de usuario/grupo de la Interfaz de Sistema Operativo Portátil (POSIX) para el directorio principal del usuario en EFS, lo que impide que otros usuarios/espacios accedan a sus datos.

Copia de seguridad y recuperación

No se puede adjuntar un volumen EFS existente a un SageMaker dominio nuevo. En un entorno de producción, asegúrese de que se haya realizado una copia de seguridad del volumen de Amazon EFS (en otro volumen de EFS o en Amazon Simple Storage Service (Amazon S3)). Si se elimina accidentalmente un volumen EFS, el administrador debe desmontar y volver a crear el dominio de SageMaker Studio. El proceso es el siguiente:

Realice una copia de seguridad de la lista de perfiles de usuario, espacios y los ID de usuario (UID) de EFS asociados mediante las llamadas `ListUserProfiles` `DescribeUserProfileList Spaces`,, y `DescribeSpace` API.

1. Cree un nuevo dominio de SageMaker Studio.
2. Crea los perfiles y espacios de usuario.
3. Para cada perfil de usuario, copie los archivos de la copia de seguridad en EFS/Amazon S3.
4. Si lo desea, elimine todas las aplicaciones y los perfiles de usuario del antiguo dominio de SageMaker Studio.

Para obtener instrucciones detalladas, consulte la sección del apéndice Copia de seguridad y recuperación de dominios de SageMaker Studio.

> **Note**
>
> Esto también se puede lograr haciendo una `LifecycleConfigurations` copia de seguridad de los datos desde y hacia S3 cada vez que un usuario inicia su aplicación.

Volumen de Amazon EBS

También se adjunta un volumen de almacenamiento de Amazon Elastic Block Store (Amazon EBS) a cada instancia de SageMaker Studio Notebook. Se utiliza como volumen raíz del contenedor o la imagen que se ejecuta en la instancia. Si bien el almacenamiento de Amazon EFS es persistente, el volumen de Amazon EBS adjunto al contenedor es temporal. Los datos almacenados localmente en el volumen de Amazon EBS no se conservarán si el cliente elimina la aplicación.

Asegurar el acceso a la URL prefirmada

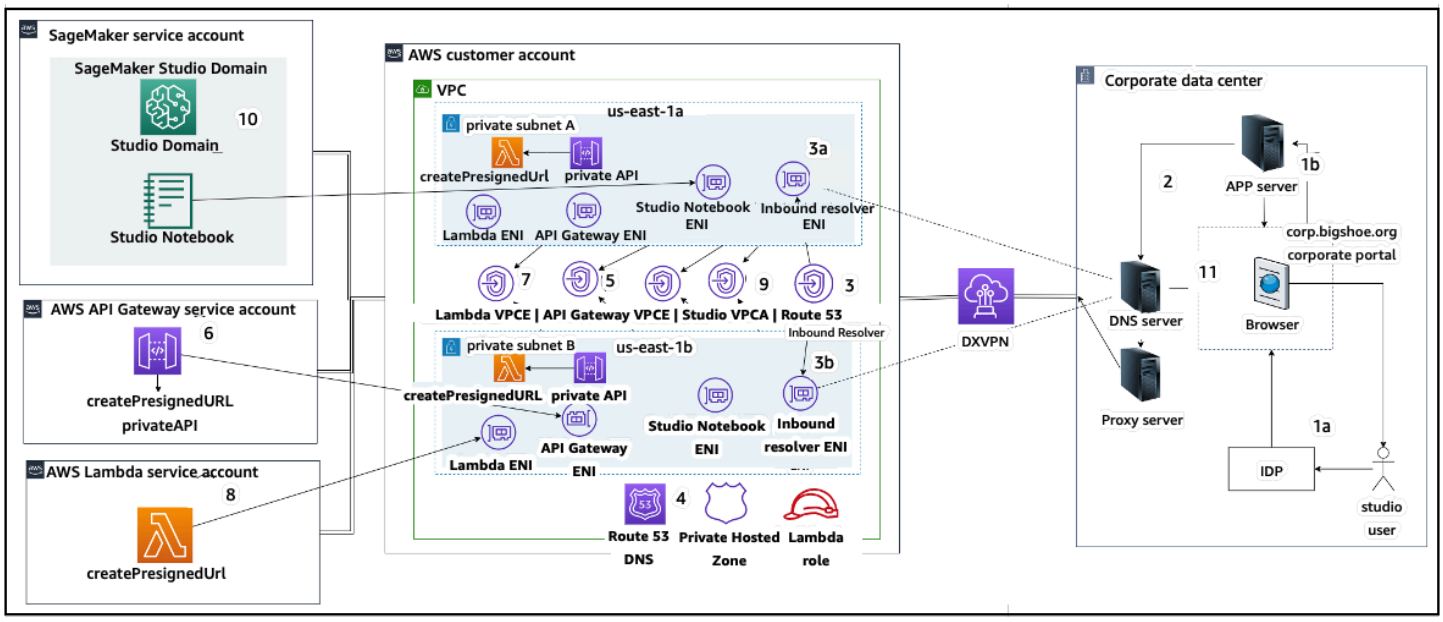
Cuando un usuario de SageMaker Studio abre el enlace del bloc de notas, SageMaker Studio valida la política de IAM del usuario federado para autorizar el acceso y genera y resuelve la URL prefirmada del usuario. Como la SageMaker consola se ejecuta en un dominio de Internet, esta URL generada y prefirmada es visible en la sesión del navegador. Esto representa un vector de amenaza no deseado para el robo de datos y el acceso a los datos de los clientes cuando no se aplican los controles de acceso adecuados.

Studio admite varios métodos para reforzar los controles de acceso contra el robo de datos mediante URL prefirmadas:

- Validación de la IP del cliente mediante la condición de política de IAM `aws:sourceIp`
- Validación de la VPC del cliente mediante la condición IAM `aws:sourceVpc`
- Validación del punto final de la VPC del cliente mediante la condición de política de IAM `aws:sourceVpce`

Al acceder a las libretas de SageMaker Studio desde la SageMaker consola, la única opción disponible es utilizar la validación de la IP del cliente con la condición de política de IAM. `aws:sourceIp` Sin embargo, puede utilizar productos de enrutamiento de tráfico para navegadores, como Zscaler, para garantizar la escalabilidad y el cumplimiento del acceso a Internet de sus empleados. Estos productos de enrutamiento de tráfico generan su propia IP de origen, cuyo rango de IP no está controlado por el cliente empresarial. Esto impide que estos clientes empresariales utilicen la `aws:sourceIp` condición.

Para utilizar la validación de puntos de enlace de la VPC del cliente mediante la condición de política de IAM`aws:sourceVpce`, la creación de una URL prefirmada debe originarse en la misma VPC del cliente en la que se ha implementado SageMaker Studio, y la resolución de la URL prefirmada debe realizarse a través de un punto de enlace de la VPC de Studio en la SageMaker VPC del cliente. Esta resolución de la URL prefirmada durante el tiempo de acceso para los usuarios de la red corporativa se puede lograr mediante reglas de reenvío de DNS (tanto en Zscaler como en el DNS corporativo) y, luego, en el punto final de la VPC del cliente mediante un solucionador de entradas Amazon Route 53, como se muestra en la siguiente arquitectura:



Acceso a la URL prefirmada de Studio con el punto final de VPC a través de la red corporativa

Para obtener step-by-step orientación sobre la configuración de la arquitectura anterior, consulte Secure Amazon SageMaker Studio presignadas, parte 1: Infraestructura fundamental.

SageMaker cuotas y límites de dominio

- SageMaker La federación de SSO de dominios de Studio solo se admite en la región, en todas las cuentas de los miembros de la AWS organización en la que se aprovisiona AWS Identity Center.
- Actualmente, los espacios compartidos no son compatibles con los dominios configurados con AWS Identity Center.
- La configuración de la VPC y la subred no se puede cambiar después de crear el dominio. Sin embargo, puede crear un dominio nuevo con una configuración de VPC y subred diferente.
- El acceso al dominio no se puede cambiar entre los modos IAM y SSO después de crear el dominio. Puede crear un dominio nuevo con un modo de autenticación diferente.
- Hay un límite de cuatro aplicaciones de gateway del núcleo por tipo de instancia lanzadas para cada usuario.
- Cada usuario puede lanzar solo una instancia de cada tipo de instancia.
- Hay límites en cuanto a los recursos que se consumen en un dominio, como el número de instancias lanzadas por tipo de instancia y el número de perfiles de usuario que se pueden crear. Consulta la página de cuotas de servicio para obtener una lista completa de los límites de servicio.

- Los clientes pueden presentar un caso de soporte empresarial con una justificación empresarial para aumentar los límites de recursos predeterminados, como el número de dominios o perfiles de usuario, sujetos a restricciones a nivel de cuenta.
- El límite máximo de aplicaciones simultáneas por cuenta es de 2500 aplicaciones. Los límites de dominios y perfiles de usuario dependen de este límite estricto. Por ejemplo, una cuenta puede tener un único dominio con 1000 perfiles de usuario o 20 dominios con 50 perfiles de usuario cada uno.

Administración de identidades

En esta sección se explica cómo los usuarios del personal de un directorio corporativo se federan en Studio Cuentas de AWS y acceden a SageMaker él. En primer lugar, describiremos brevemente cómo se asignan los usuarios, los grupos y los roles, y cómo funciona la federación de usuarios.

Usuarios, grupos y rol

En AWS, los permisos de los recursos se administran mediante usuarios, grupos y roles. Los clientes pueden administrar sus usuarios y grupos a través de IAM o en un directorio corporativo, como Active Directory (AD), habilitado a través de un IdP externo, como Okta, que les permite autenticar los usuarios en varias aplicaciones que se ejecutan en la nube y en las instalaciones.

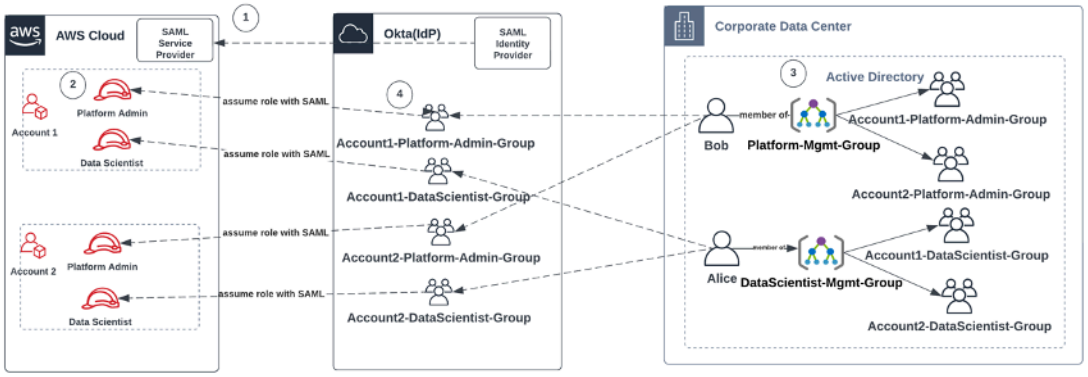
Como se explica en la sección Gestión de la identidad del pilar de la AWS seguridad, se recomienda gestionar las identidades de los usuarios en un IdP central, ya que esto ayuda a integrarse fácilmente con los procesos de recursos humanos internos y ayuda a gestionar el acceso a los usuarios de su fuerza laboral.

IdPs como Okta, permiten a los usuarios finales autenticarse en uno o varios roles Cuentas de AWS y acceder a funciones específicas mediante el inicio de sesión único con el lenguaje de marcado de aserciones de seguridad (SAML). Los administradores del IdP tienen la capacidad de descargar funciones desde el Cuentas de AWS IdP y asignarlas a los usuarios. Al iniciar sesión en AWS, a los usuarios finales se les presenta una AWS pantalla en la que se muestra una lista de los AWS roles que se les han asignado en uno o varios de ellos. Cuentas de AWS Pueden seleccionar el rol que deseen asumir para el inicio de sesión, que define sus permisos durante dicha sesión autenticada.

Debe existir un grupo en el IdP para cada combinación específica de cuentas y roles a la que desee proporcionar acceso. Puede pensar en estos grupos como grupos específicos de rol de AWS . A cualquier usuario que sea miembro de estos grupos específicos de rol se le concede un único derecho: el acceso a un rol específico en una Cuenta de AWS específica. Sin embargo, este proceso de concesión de un único derecho no se escala para administrar el acceso de los usuarios mediante la asignación de cada usuario a grupos de roles de AWS específicos. Para simplificar la administración, le recomendamos que también cree varios grupos para todos los distintos conjuntos de usuarios de su organización que requieren diferentes conjuntos de AWS derechos.

Para ilustrar la configuración del IdP central, considere una empresa con una configuración de AD donde los usuarios y los grupos estén sincronizados con el directorio del IdP. En AWS, estos grupos

de AD se asignan a funciones de IAM. A continuación, se muestran los principales pasos del flujo de trabajo:



Flujo de trabajo para incorporar usuarios de AD, grupos de AD y roles de IAM

1. En AWS, Configure la integración de SAML para cada uno de ustedes Cuentas de AWS con su IdP.
2. En AWS, configura los roles en cada uno Cuenta de AWS y sincronízalos con el IdP.
3. En el sistema AD corporativo:
   a. Crea un grupo de AD para cada rol de cuenta y sincronízalo con el IdP (por ejemplo, `Account1-Platform-Admin-Group` (también conocido como grupo de AWS roles)).
   b. Crea un grupo de administración en cada nivel de persona (por ejemplo`Platform-Mgmt-Group`) y asigna grupos de AWS roles como miembros.
   c. Asigne usuarios a ese grupo de administración para permitir el acceso a Cuenta de AWS los roles.
4. En IdP, asigne grupos de AWS roles (como`Account1-Platform-Admin-Group`) a Cuenta de AWS roles (como Administrador de plataforma en Account1).
5. Cuando la científica de datos Alice inicia sesión en Idp, se le presenta una interfaz de usuario de AWS Federation App con dos opciones entre las que elegir: «Cuenta 1 científica de datos» y «Cuenta 2 científica de datos».
6. Alice elige la opción «Científico de datos de la cuenta 1» y se conecta a su aplicación autorizada en la cuenta 1 (consola). AWS SageMaker

Para obtener instrucciones detalladas sobre cómo configurar la federación de cuentas SAML, consulta Cómo configurar SAML 2.0 para la federación de cuentas de Okta. AWS

Federación de usuarios

La autenticación de SageMaker Studio se puede realizar mediante IAM o IAM iDC. Si los usuarios se administran mediante IAM, pueden elegir el modo IAM. Si la empresa utiliza un IdP externo, puede federarse a través de IAM o IAM IdC. Tenga en cuenta que el modo de autenticación no se puede actualizar para un dominio de SageMaker Studio existente, por lo que es fundamental tomar la decisión antes de crear un dominio de Studio de producción SageMaker .

Si SageMaker Studio está configurado en modo IAM, los usuarios de SageMaker Studio acceden a la aplicación a través de una URL prefirmada que permite al usuario iniciar sesión automáticamente en la aplicación de SageMaker Studio cuando se accede a ella a través de un navegador.

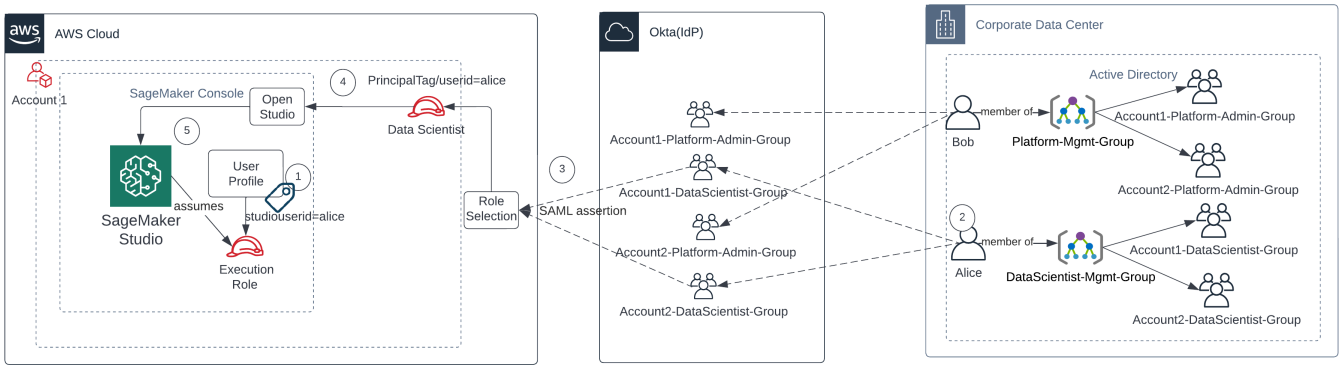
Usuarios de IAM

Para los usuarios de IAM, el administrador crea perfiles de usuario de SageMaker Studio para cada usuario y asocia el perfil de usuario a una función de IAM que permite realizar las acciones necesarias que el usuario debe realizar desde Studio. Para impedir que un AWS usuario acceda únicamente a su perfil de usuario de SageMaker Studio, el administrador debe etiquetar el perfil de usuario de SageMaker Studio y adjuntar una política de IAM al usuario que le permita acceder solo si el valor de la etiqueta es el mismo que el nombre de usuario. AWS La declaración de política es similar a la siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:username}"
                }
            }
        }
    ]
}
```

AWS IAM o federación de cuentas

El método de Cuenta de AWS federación permite a los clientes federarse en la SageMaker consola desde su IdP de SAML, como Okta. Para impedir que los usuarios accedan únicamente a su perfil de usuario, el administrador debe etiquetar el perfil de usuario de SageMaker Studio, añadir `PrincipalTags` el IdP y configurarlos como etiquetas transitivas. El siguiente diagrama muestra cómo el usuario federado (Alice, la científica de datos) está autorizado a acceder a su propio perfil de usuario de SageMaker Studio.



Acceder a SageMaker Studio en modo de federación de IAM

1. El perfil de usuario de Alice SageMaker Studio se etiqueta con su ID de usuario y se asocia a la función de ejecución.
2. Alice se autentica en el IdP (Okta).
3. El IdP autentica a Alice y publica una afirmación SAML con los dos roles (científico de datos para las cuentas 1 y 2) de los que Alice es miembro. Alice selecciona el rol Científico de datos para la cuenta 1.
4. Alice ha iniciado sesión en la SageMaker consola de Account 1 y ha asumido el rol de científica de datos. Alice abre su instancia de aplicación de Studio desde la lista de instancias de aplicaciones de Studio.
5. La etiqueta principal de Alice en la sesión de rol asumida se valida con la etiqueta de perfil de usuario de la instancia de aplicación de SageMaker Studio seleccionada. Si la etiqueta de perfil es válida, se lanza la instancia de la aplicación SageMaker Studio y se asume la función de ejecución.

Si quieres automatizar la creación de roles y políticas de SageMaker ejecución como parte de la incorporación de usuarios, puedes hacerlo de la siguiente manera:

1. Configure un grupo de AD, por ejemplo, `SageMaker-Account1-Group` en cada nivel de cuenta y dominio de Studio.
2. Agrega SageMaker -Account1-Group a la membresía del grupo del usuario cuando necesites incorporar a un usuario a Studio. SageMaker

Configura un proceso de automatización que escuche los eventos de `SageMaker-Account1-Group` membresía y usa las AWS API para crear el rol, las políticas, las etiquetas y el perfil de usuario de SageMaker Studio en función de sus grupos de AD. Asocie el rol con el perfil de usuario. Para ver un ejemplo de política, consulta. Impedir que los usuarios de SageMaker Studio accedan a otros perfiles de usuario

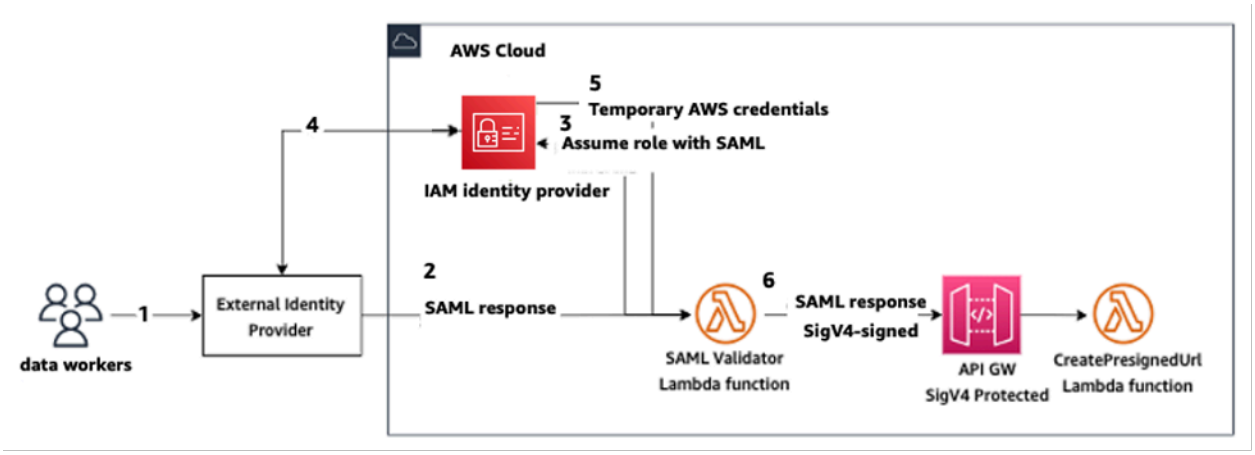
Autenticación SAML mediante AWS Lambda

En el modo IAM, los usuarios también se pueden autenticar en SageMaker Studio mediante aserciones SAML. En esta arquitectura, el cliente tiene un IdP existente, donde puede crear una aplicación SAML para que los usuarios accedan a Studio (en lugar de a la aplicación AWS Identity Federation). El IdP del cliente se añade a IAM. Una AWS Lambda función ayuda a validar la afirmación de SAML mediante IAM y STS y, a continuación, invoca directamente una puerta de enlace de API o una función Lambda para crear la URL de dominio prefirmada.

La ventaja de esta solución es que la función Lambda puede personalizar la lógica para acceder a SageMaker Studio. Por ejemplo:

- Cree automáticamente un perfil de usuario si no existe uno.
- Adjunte o elimine funciones o documentos de políticas a la función de ejecución de SageMaker Studio analizando los atributos de SAML.
- Para personalizar el perfil de usuario, añada la configuración del ciclo de vida (LCC) y añada etiquetas.

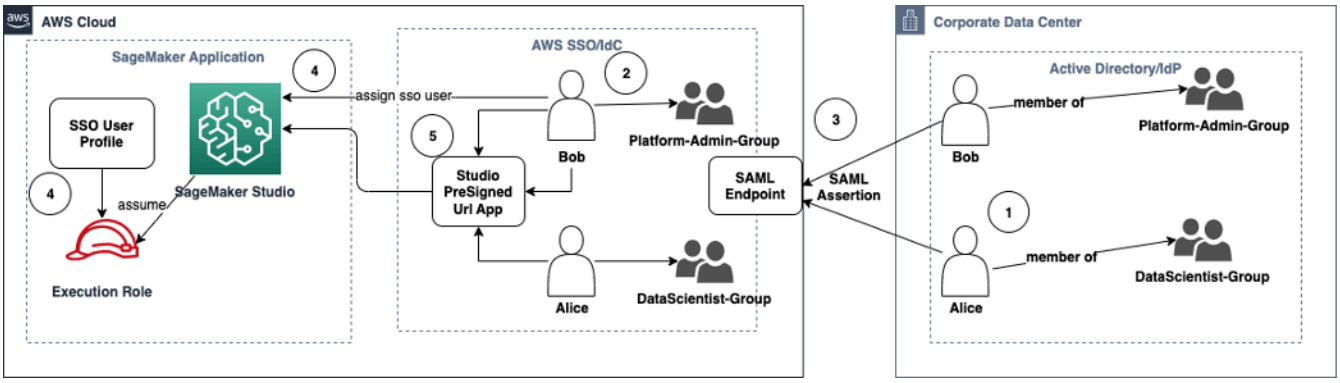
En resumen, esta solución mostrará a SageMaker Studio como una aplicación SAML2.0 con una lógica personalizada para la autenticación y la autorización. Consulte la sección del apéndice Acceso a SageMaker Studio mediante la aserción SAML para obtener detalles sobre la implementación.



Acceso a SageMaker Studio mediante una aplicación SAML personalizada

Federación de AWS IAM IdC

El método de federación de iDC permite a los clientes federarse directamente en una aplicación de SageMaker Studio desde su IdP de SAML (como Okta). En el siguiente diagrama, se muestra cómo el usuario federado está autorizado a acceder a su propia instancia de Studio. SageMaker



Acceso a SageMaker Studio en modo IAM iDC

1. En el AD corporativo, el usuario es miembro de grupos de AD como, por ejemplo, el grupo Administrador de plataforma y el grupo Científico de datos.
2. El usuario de AD y los grupos de AD del proveedor de identidad (IdP) se sincronizan con el Centro de identidad de AWS IAM y están disponibles como usuarios y grupos de inicio de sesión único para las asignaciones, respectivamente.
3. El IdP publica una afirmación de SAML en el punto final de SAML del AWS iDC.
4. En SageMaker Studio, el usuario de iDC está asignado a la aplicación Studio. SageMaker Esta tarea se puede realizar mediante iDC Group y SageMaker Studio se aplicará a cada nivel de

usuario de iDC. Cuando se crea esta asignación, SageMaker Studio crea el perfil de usuario de iDC y le asigna la función de ejecución del dominio.

5. El usuario accede a la aplicación SageMaker Studio mediante la URL prefirmada segura alojada como una aplicación en la nube desde el iDC. SageMaker Studio asume la función de ejecución asociada a su perfil de usuario de iDC.

Guía de autenticación de dominios

Estas son algunas consideraciones a tener en cuenta cuando se elige el modo de autenticación de un dominio:

1. Si quieres que tus usuarios no accedan a la AWS Management Console interfaz de usuario de SageMaker Studio ni la vean directamente, utiliza el modo de inicio de sesión único con AWS IAM iDC.
2. Si quieres que tus usuarios no accedan a la AWS Management Console interfaz de usuario de SageMaker Studio ni la vean directamente en el modo IAM, puedes hacerlo mediante una función de Lambda en el backend para generar una URL prefirmada para el perfil de usuario y redirigirlos a la interfaz de usuario de Studio. SageMaker
3. En el modo IdC, cada usuario se asigna a un único perfil de usuario.
4. A todos los perfiles de usuario se les asigna automáticamente el rol de ejecución predeterminado en modo IdC. Si quieres que a tus usuarios se les asignen diferentes funciones de ejecución, tendrás que actualizar los perfiles de usuario mediante la API. UpdateUserProfile
5. Si quieres restringir el acceso a la interfaz de usuario de SageMaker Studio en modo IAM (mediante la URL prefirmada generada) a un punto final de VPC, sin tener que atravesar Internet, puedes usar un solucionador de DNS personalizado. Consulte la entrada del blog Secure Amazon SageMaker Studio Presigned URL Part 1: Foundational infrastructure.

Administración de permisos

En esta sección, se analizan las prácticas recomendadas para configurar los roles de IAM, las políticas y barreras de protección que más se utilizan para aprovisionar y operar el dominio de SageMaker Studio.

Roles y políticas de IAM

Como práctica recomendada, tal vez desee identificar primero las personas y aplicaciones relevantes, conocidas como entidades principales que participan en el ciclo de vida del machine learning, y qué permisos de AWS necesita concederles. Como SageMaker es un servicio administrado, también debe tener en cuenta las entidades principales del servicio, que son servicios de AWS que pueden realizar llamadas a la API en nombre de un usuario. En el siguiente diagrama, se ilustran los distintos roles de IAM que puede crear, correspondientes a las distintas personas de la organización.

Roles de IAM de SageMaker

Estos roles se describen en detalle, junto con algunos ejemplos de permisos de IAM específicos que necesitarán.

- Rol de usuario de administrador de ML: es la entidad principal que aprovisiona el entorno de los científicos de datos mediante la creación de dominios de Studio y perfiles de usuario (`sagemaker:CreateDomain`, `sagemaker:CreateUserProfile`), la creación de claves de AWS Key Management Service (AWS KMS) para los usuarios, la creación de buckets de S3 para los científicos de datos y la creación de repositorios de Amazon ECR para alojar contenedores. También pueden establecer configuraciones y scripts de ciclo de vida predeterminados para los usuarios; crear imágenes personalizadas y asociarlas al dominio de SageMaker Studio; y proporcionar productos de Service Catalog como, por ejemplo, proyectos personalizados y plantillas de Amazon EMR.

Como esta entidad principal no ejecutará trabajos de entrenamiento, por ejemplo, no necesita permisos para lanzar los trabajos de entrenamiento o procesamiento de SageMaker. Si utilizan una infraestructura como plantillas de código, por ejemplo, CloudFormation o Terraform, para aprovisionar dominios y usuarios, el servicio de aprovisionamiento asumiría este rol para crear los recursos en nombre del administrador. Este rol puede tener acceso de solo lectura en SageMaker utilizando la AWS Management Console.

Este rol de usuario también necesitará determinados permisos de EC2 para lanzar el dominio dentro de una VPC privada, permisos de KMS para cifrar el volumen de EFS y permisos para crear un rol vinculado a un servicio para Studio (`iam:CreateServiceLinkedRole`). Describiremos esos permisos detallados más adelante en el documento.

- Rol de usuario del científico de datos: esta entidad principal es el usuario que inicia sesión en SageMaker Studio; explora los datos; y crea canalizaciones y trabajos de procesamiento y entrenamiento, etc. El permiso principal que necesita el usuario es el permiso para iniciar SageMaker Studio, y el resto de las políticas se pueden administrar mediante el rol de servicio de ejecución de SageMaker.
- Rol de servicio de ejecución de SageMaker: dado que SageMaker es un servicio administrado, lanza trabajos en nombre del usuario. Este rol suele ser el más amplio en términos de permisos permitidos, ya que muchos clientes optan por utilizar un solo rol de ejecución para ejecutar trabajos de entrenamiento, procesamiento o alojamiento de modelos. Aunque esta es una forma fácil de empezar, dado que los clientes maduran a medida que avanzan, suelen dividir el rol de ejecución de cuadernos en roles independientes para las distintas acciones de la API, especialmente cuando ejecutan estos trabajos en entornos implementados.

  Debe asociar un rol al dominio de SageMaker Studio cuando lo crea. Sin embargo, como los clientes pueden necesitar la flexibilidad de tener diferentes roles asociados a los distintos perfiles de usuario del dominio (por ejemplo, según su función de trabajo), también puede asociar un rol de IAM independiente a cada perfil de usuario. Se recomienda asignar un único usuario físico a un único perfil de usuario. Si no asigna un rol a un perfil de usuario al crearlo, el comportamiento predeterminado es asociar también el rol de ejecución del dominio de SageMakerStudio al perfil de usuario.

  En los casos en los que varios científicos de datos e ingenieros de machine learning trabajen juntos en un proyecto y necesiten un modelo de permisos compartido para acceder a los recursos, le recomendamos que cree un rol de ejecución de servicios de SageMaker a nivel de equipo para compartir los permisos de IAM entre los miembros de su equipo. En los casos donde necesite

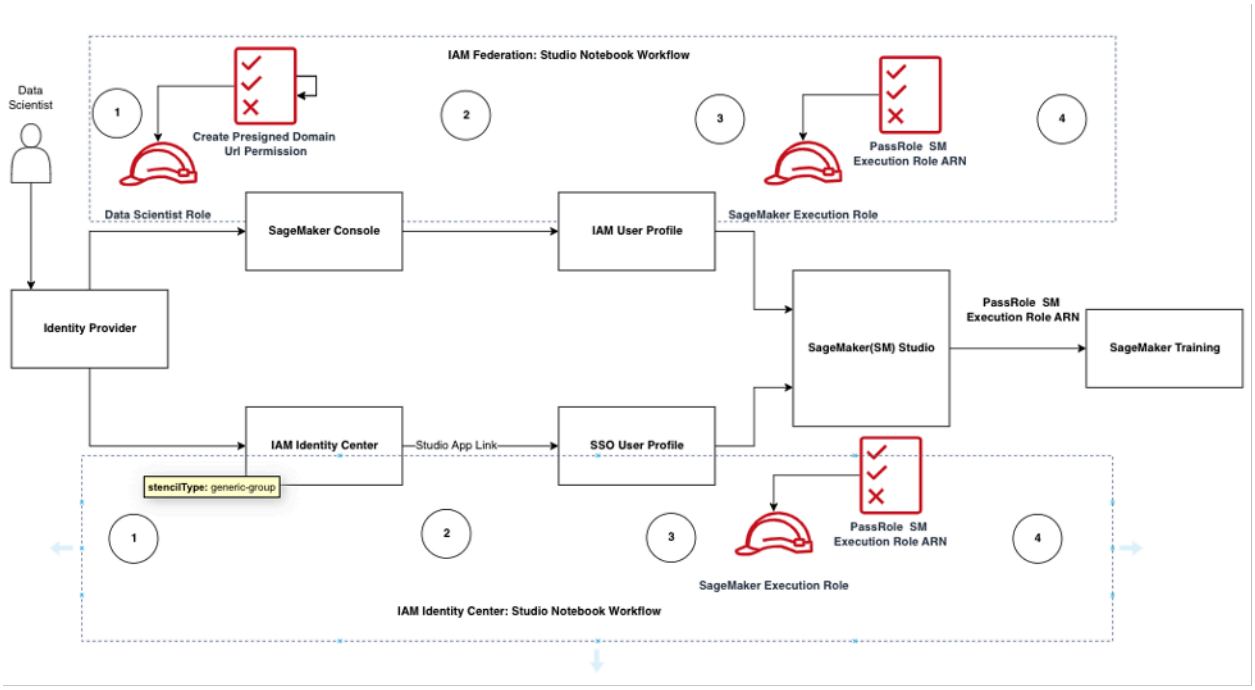
bloquear los permisos en cada nivel de usuario, puede crear un rol de ejecución del servicio de SageMaker individual a nivel de usuario; sin embargo, debe tener en cuenta los límites del servicio.

Flujo de trabajo de autorización de cuaderno de SageMaker Studio

En esta sección, se explica cómo funciona la autorización de Cuaderno de SageMaker Studio para diversas actividades que el científico de datos debe realizar para crear y entrenar el modelo directamente desde el cuaderno de SageMaker Studio. El dominio de SageMaker admite dos modos de autorización:

- Federación de IAM
- IAM Identity Center

En este documento, se explica el flujo de trabajo de autorización de Científico de datos para cada uno de esos modos.



Flujo de trabajo de autenticación y autorización para los usuarios de Studio

Federación de IAM: flujos de trabajo de cuaderno de SageMaker Studio

1. Un científico de datos se autentica en su proveedor de identidad corporativa y asume el rol de usuario de científico de datos (el rol de federación de usuario) en la consola de SageMaker. Este

rol de federación tiene el permiso de API `iam:PassRole` en el rol de ejecución de SageMaker para transferir el rol Nombre de recurso de Amazon (ARN) a SageMaker Studio.

2. El científico de datos selecciona el enlace de Open Studio de su perfil de usuario de IAM de Studio que está asociado con el rol de ejecución de SageMaker.
3. Se lanza el servicio IDE de SageMaker Studio, suponiendo los permisos del rol de ejecución de SageMaker del perfil de usuario. Este rol tiene permiso de `iam:PassRole` API en el rol de ejecución de SageMaker para transferir el ARN de rol al servicio de entrenamiento de SageMaker.
4. Cuando el científico de datos lanza el trabajo de entrenamiento en los nodos de cómputo remoto, el ARN de rol de ejecución de SageMaker se transfiere al servicio de entrenamiento de SageMaker. Esto crea una nueva sesión de rol con este ARN y ejecuta el trabajo de entrenamiento. Si necesita reducir aún más el permiso para un trabajo de entrenamiento, puede crear un rol específico de entrenamiento y pasarle el ARN de ese rol al llamar a la API de entrenamiento.

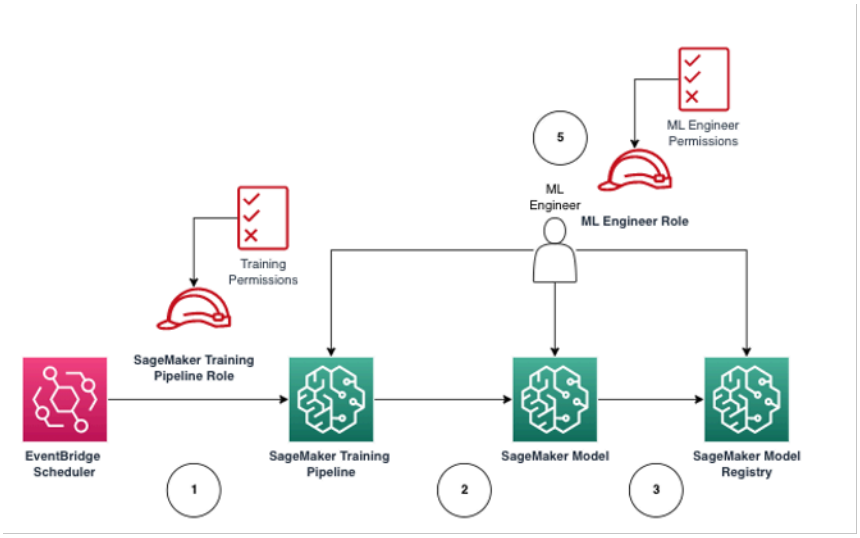
IAM Identity Center: flujo de trabajo de cuaderno de SageMaker Studio

1. El científico de datos se autentica en su proveedor de identidad corporativa y hace clic en AWS IAM Identity Center. El científico de datos recibe el portal de Identity Center para el usuario.
2. El científico de datos hace clic en el enlace de la aplicación SageMaker Studio que se ha creado a partir de su perfil de usuario de IdC, que está asociado con el rol de ejecución de SageMaker.
3. Se lanza el servicio de IDE de SageMaker Studio, suponiendo los permisos del rol de ejecución de SageMaker del perfil de usuario. Este rol tiene permiso de `iam:PassRole` API en el rol de ejecución de SageMaker para transferir el ARN de rol al servicio de entrenamiento de SageMaker.
4. Cuando el científico de datos lanza el trabajo de entrenamiento en los nodos de cómputo remoto, el ARN del rol de ejecución de SageMaker se transfiere al servicio de entrenamiento de SageMaker. El ARN del rol de ejecución crea una nueva sesión de rol con este ARN y ejecuta el trabajo de entrenamiento. Si necesita reducir aún más el permiso para los trabajos de entrenamiento, puede crear un rol específico del entrenamiento y transferir el ARN del rol al llamar a la API de entrenamiento.

Entorno implementado: flujo de trabajo de entrenamiento de SageMaker

En los entornos implementados como, por ejemplo, las pruebas de sistemas y la producción, los trabajos se ejecutan mediante un programador automático y desencadenadores de eventos, y el

acceso humano a estos entornos se restringe en los cuadernos de SageMaker Studio. En esta sección, se analiza cómo funcionan los roles de IAM con la canalización de entrenamiento de SageMaker en el entorno desplegado.



Flujo de trabajo de entrenamiento de SageMaker en un entorno de producción administrado

1. El programador de Amazon EventBridge activa el trabajo de canalización de entrenamiento de SageMaker.
2. El trabajo de canalización de entrenamiento de SageMaker asume el rol de canalización de entrenamiento de SageMaker para entrenar el modelo.
3. El modelo de SageMaker entrenado está registrado en el Registro de modelos de SageMaker.
4. Un ingeniero de machine learning asume el rol de usuario de ingeniero de machine learning para administrar la canalización de entrenamiento y el modelo de SageMaker.

Permisos para los datos

La capacidad de los usuarios de SageMaker Studio de acceder a cualquier fuente de datos se rige por los permisos asociados a su rol de ejecución de IAM de SageMaker. Las políticas asociadas pueden autorizarles a leer, escribir o eliminar en determinados prefijos o buckets de Amazon S3, y a conectarse a las bases de datos de Amazon RDS.

Acceso a datos de AWS Lake Formation

Muchas empresas han empezado a utilizar lagos de datos gobernados por AWS Lake Formation para habilitar el acceso a datos detallado para sus usuarios. Como ejemplo de este tipo de datos

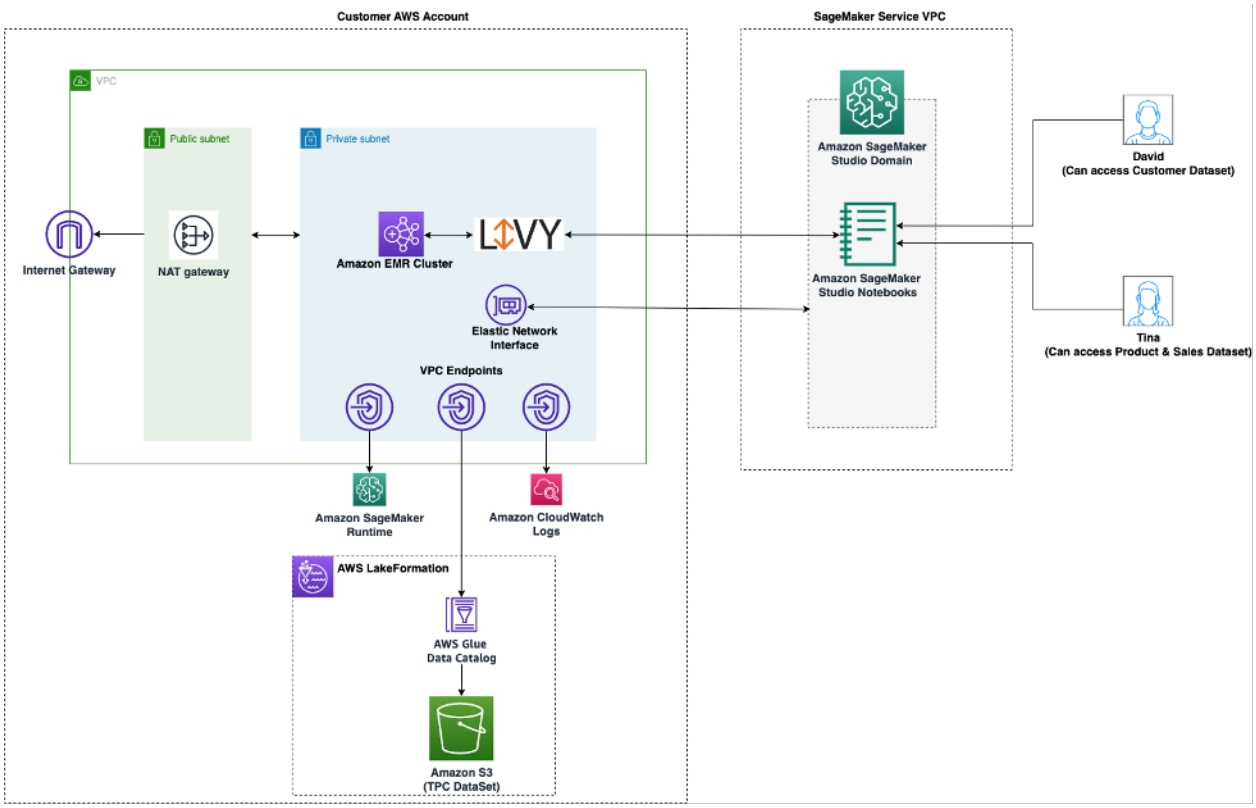
gobernados, los administradores pueden ocultar columnas confidenciales para algunos usuarios y, al mismo tiempo, habilitar las consultas de la misma tabla subyacente.

Para utilizar Lake Formation de SageMaker Studio, los administradores pueden registrar los roles de ejecución de IAM de SageMaker como `DataLakePrincipals`. Para obtener más información, consulte Referencia de permisos de Lake Formation. Una vez autorizados, hay tres métodos principales para acceder a los datos gobernados y escribirlos en SageMaker Studio:

1. En un cuaderno de SageMaker Studio, los usuarios pueden utilizar motores de consulta como Amazon Athena o bibliotecas basadas en boto3 para extraer datos directamente en el cuaderno. El SDK de AWS para Pandas (anteriormente conocido como awswrangler) es una biblioteca muy conocida. El siguiente ejemplo de código muestra lo sencillo que puede ser:

```
transaction_id = wr.lakeformation.start_transaction(read_only=True)
df = wr.lakeformation.read_sql_query(
    sql=f"SELECT * FROM {table};",
    database=database,
    transaction_id=transaction_id
)
```

2. Utilice la conectividad nativa de SageMaker Studio con Amazon EMR para leer y escribir datos a escala. Mediante el uso de los roles de ejecución de Apache Livy y Amazon EMR, SageMaker Studio ha creado una conectividad nativa que permite transferir su rol de IAM de ejecución de SageMaker (u otro rol autorizado) a un clúster de Amazon EMR para acceder a los datos y procesarlos. Consulte Conectarse a un clúster de Amazon EMR desde Studio para obtener instrucciones actualizadas.



Arquitectura para acceder a los datos administrados por Lake Formation en SageMaker Studio

3. Utilice la conectividad nativa de SageMaker Studio con las sesiones interactivas de AWS Glue para leer y escribir datos a escala. Los cuadernos de SageMaker Studio tienen kernels integrados que permiten a los usuarios ejecutar comandos de forma interactiva en AWS Glue. Esto permite el uso escalable de los backends de Python, Spark o Ray, que pueden leer y escribir datos a escala sin problemas en fuentes de datos gobernadas. Los kernels permiten a los usuarios transferir sus roles de ejecución de SageMaker u otros roles de IAM autorizados. Consulte Preparación de datos mediante sesiones interactivas de AWS Glue para obtener más información.

Barreras de protección comunes

En esta sección, se analizan las barreras de protección que se utilizan con más frecuencia para aplicar la gobernanza a los recursos de ML utilizando políticas de IAM, políticas de recursos, políticas de puntos de conexión de VPC y políticas de control de servicio (SCP).

Limitar el acceso del cuaderno a instancias específicas

Esta política de control de servicios se puede utilizar para limitar los tipos de instancias a los que tienen acceso los científicos de datos al crear cuadernos de Studio. Tenga en cuenta que cualquier

usuario necesitará que la instancia “system” esté permitida para crear la aplicación de servidor de Jupyter predeterminada que aloja SageMaker Studio.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "LimitInstanceTypesforNotebooks",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateApp"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringNotLike": {
                     "sagemaker:InstanceTypes": [
                         "ml.c5.large",
                         "ml.m5.large",
                         "ml.t3.medium",
                         "system"
                     ]
                 }
             }
         }
     ]
 }
```

Limitar los dominios de SageMaker Studio no conformes

En el caso de los dominios de SageMaker Studio, se puede utilizar la siguiente política de control de servicios para obligar al tráfico a acceder a los recursos del cliente, para que no pase por el Internet público, sino a través de la VPC del cliente:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {   "Sid": "LockDownStudioDomain",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateDomain"
             ],
             "Resource": "*",
```

```
            "Condition": {
                        "StringNotEquals": {"sagemaker:AppNetworkAccessType":
"VpcOnly"
                },
                "Null": {
                        "sagemaker:VpcSubnets": "true",
                        "sagemaker:VpcSecurityGroupIds": "true"
                }
            }
        }
    ]
}
```

Limitar el lanzamiento de imágenes de SageMaker no autorizadas

La siguiente política impide que un usuario lance una imagen de SageMaker no autorizada dentro de su dominio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:CreateApp"
             ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringNotLike": {
                    "sagemaker:ImageArns":
                        [
                        "arn:aws:sagemaker:*:*:image/{ImageName}"
                        ]
                }
            }
        }
    ]
}
```

Iniciar cuadernos solo a través de puntos de conexión de VPC de SageMaker

Además de los puntos de conexión de VPC para el plano de control de SageMaker, SageMaker admite puntos de conexión de VPC para que los usuarios se conecten a cuadernos de SageMaker Studio o instancias de cuadernos de SageMaker. Si ya ha configurado un punto de conexión de VPC para una instancia de SageMaker Studio/cuaderno, la siguiente clave de condición de IAM solo permitirá las conexiones a los cuadernos de SageMaker Studio si se realizan mediante el punto de conexión de VPC de SageMaker Studio o mediante el punto de conexión de la API de SageMaker.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EnableSageMakerStudioAccessviaVPCEndpoint",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreatePresignedDomainUrl",
                 "sagemaker:DescribeUserProfile"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "aws:sourceVpce": [
                         "vpce-111bbccc",
                         "vpce-111bbddd"
                     ]
                 }
             }
         }
     ]
 }
```

Limitar el acceso del cuaderno de SageMaker Studio a un rango de IP limitado

Las empresas suelen limitar el acceso de SageMaker Studio a determinados rangos de IP corporativos permitidos. La siguiente política de IAM con la clave de condición `SourceIP` puede limitar el acceso.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EnableSageMakerStudioAccess",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreatePresignedDomainUrl",
                 "sagemaker:DescribeUserProfile"
             ],
             "Resource": "*",
             "Condition": {
                 "IpAddress": {
                     "aws:SourceIp": [
                         "192.0.2.0/24",
                         "203.0.113.0/24"
                     ]
                 }
             }
         }
     ]
 }
```

Impedir que los usuarios de SageMaker Studio accedan a otros perfiles de usuario

Como administrador, al crear el perfil de usuario, asegúrese de que el perfil esté etiquetado con el nombre de usuario de SageMaker Studio con la clave de etiqueta `studiouserid`. La entidad principal (usuario o rol asociado al usuario) también debe tener una etiqueta con la clave `studiouserid` (esta etiqueta puede tener cualquier nombre y no está restringida a `studiouserid`).

A continuación, asocie la siguiente política al rol que asumirá el usuario al lanzar SageMaker Studio.

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

```
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:PrincipalTag/
studiouserid}"
                }
            }
        }
    ]
}
```

Imponer el etiquetado

Los científicos de datos necesitan usar los cuadernos de SageMaker Studio para explorar los datos, y crear y entrenar modelos. La aplicación de etiquetas a los cuadernos ayuda a supervisar el uso y controlar los costos, además de garantizar la propiedad y la capacidad de auditoría.

En el caso de las aplicaciones de SageMaker Studio, asegúrese de que el perfil de usuario esté etiquetado. Las etiquetas se propagan automáticamente a las aplicaciones desde el perfil de usuario. Para imponer la creación de perfiles de usuario con etiquetas (compatibles con CLI y SDK), se recomienda añadir esta política al rol de administrador:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceUserProfileTags",
            "Effect": "Allow",
            "Action": "sagemaker:CreateUserProfile",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Para otros recursos, como los trabajos de entrenamiento y los trabajos de procesamiento, puede hacer que las etiquetas sean obligatorias utilizando la siguiente política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceTagsForJobs",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateProcessingJob",
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Acceso raíz en SageMaker Studio

En SageMaker Studio, el cuaderno se ejecuta en un contenedor de Docker que, de forma predeterminada, no tiene acceso raíz a la instancia de host. Del mismo modo, excepto el usuario Ejecutar como predeterminado, los demás rangos de ID de usuario del contenedor se reasignan como ID de usuario sin privilegios en la propia instancia de host. Como resultado, la amenaza de una escalada de privilegios se limita al propio contenedor del cuaderno.

Al crear imágenes personalizadas, es posible que desee proporcionar al usuario permisos no raíz para aplicar controles más estrictos; por ejemplo, evitar ejecutar procesos no deseados como raíz o instalar paquetes disponibles públicamente. En esos casos, puede crear la imagen para que se ejecute como un usuario no raíz en el Dockerfile. Tanto si crea el usuario como raíz como si lo crea como no raíz, debe asegurarse de que el UID/GID del usuario sea idéntico al UID/GID de AppImageConfig de la aplicación personalizada, que crea la configuración para que SageMaker ejecute una aplicación con la imagen personalizada. Por ejemplo, si el Dockerfile se ha creado para un usuario no raíz como el siguiente:

```
ARG NB_UID="1000"
ARG NB_GID="100"
...
USER $NB_UID
```

El archivo `AppImageConfig` debe mencionar el mismo UID y GID en `KernelGatewayConfig`:

```
{
    "KernelGatewayImageConfig": {
        "FileSystemConfig": {
            "DefaultUid": 1000,
            "DefaultGid": 100
        }
    }
}
```

Los valores de UID/GID aceptables para las imágenes personalizadas son 0/0 y 1000/100 para las imágenes de Studio. Para ver ejemplos de creación de imágenes personalizadas y la configuración de `AppImageConfig` asociada, consulte este repositorio de Github.

Para evitar la manipulación indebida de los usuarios, no conceda los permisos `CreateAppImageConfig`, `UpdateAppImageConfig` o `DeleteAppImageConfig` a los usuarios de cuadernos de SageMaker Studio.

Administración de red

Para configurar el dominio de SageMaker Studio, debes especificar la red, las subredes y los grupos de seguridad de la VPC. Al especificar la VPC y las subredes, asegúrese de asignar las IP teniendo en cuenta el volumen de uso y el crecimiento esperado, que se describen en las siguientes secciones.

Planificación de redes de VPC

Las subredes de VPC del cliente asociadas al dominio de SageMaker Studio se deben crear con el rango de enrutamiento entre dominios sin clase (CIDR) adecuado, en función de los siguientes factores:

- Número de usuarios.
- Número de aplicaciones por usuario.
- Número de tipos de instancias únicos por usuario.
- Número medio de instancias de formación por usuario.
- Porcentaje de crecimiento esperado.

SageMaker y AWS los servicios participantes inyectan interfaces de red elásticas (ENI) en la subred de VPC del cliente para los siguientes casos de uso:

- Amazon EFS inyecta un ENI para un destino de montaje de EFS para el SageMaker dominio (una IP por subred/zona de disponibilidad asociada al SageMaker dominio).
- SageMaker Studio inyecta un ENI para cada instancia única utilizada por un perfil de usuario o un espacio compartido. Por ejemplo:
  - Si un perfil de usuario ejecuta una aplicación de servidor Jupyter predeterminada (una instancia de «sistema»), una aplicación de ciencia de datos y una aplicación Python base (ambas ejecutadas en una `ml.t3.medium` instancia), Studio inyecta dos direcciones IP.
  - Si un perfil de usuario ejecuta una aplicación de servidor Jupyter predeterminada (una instancia de «sistema»), una aplicación de GPU de Tensorflow (en una `ml.g4dn.xlarge` instancia) y una aplicación de almacenamiento de datos (en una `ml.m5.4xlarge` instancia), Studio inyecta tres direcciones IP.
- Se inyecta un ENI para cada punto de enlace de VPC en las subredes o zonas de disponibilidad de la VPC del dominio (cuatro IP para los puntos de enlace de VPC; aproximadamente seis IP

para los SageMaker puntos de enlace de VPC de los servicios participantes, como S3, ECR y.) CloudWatch

- Si los trabajos de SageMaker formación y procesamiento se lanzan con la misma configuración de VPC, cada trabajo necesita dos direcciones IP por instancia.

> **Note**
>
> La configuración de VPC para SageMaker Studio, como las subredes y el tráfico exclusivo de VPC, no se transfiere automáticamente a los trabajos de formación o procesamiento creados desde Studio. SageMaker El usuario debe configurar la configuración de la VPC y el aislamiento de la red según sea necesario al llamar a las API Create*Job. Consulte Ejecutar los contenedores de entrenamiento e inferencia en modo con acceso a Internet para obtener más información.

Escenario: un científico de datos realiza experimentos en dos tipos de instancias diferentes

En este escenario, supongamos que un SageMaker dominio está configurado en el modo de tráfico solo de VPC. Hay puntos de enlace de VPC configurados, como la SageMaker API, el tiempo de SageMaker ejecución, Amazon S3 y Amazon ECR.

Un científico de datos realiza experimentos en cuadernos de Studio, los ejecuta en dos tipos de instancias diferentes (por ejemplo, `ml.t3.medium` y`ml.m5.large`) y lanza dos aplicaciones en cada tipo de instancia.

Suponga que el científico de datos también ejecuta simultáneamente un trabajo de formación con la misma configuración de VPC en una `ml.m5.4xlarge` instancia.

En este escenario, el servicio SageMaker Studio inyectará los ENI de la siguiente manera:

Tabla 1: Se inyectan ENI en la VPC del cliente para un escenario de experimentación

Entidad	Destino	ENI inyectado	Notas	Nivel
Objetivo de montaje EFS	Subredes de la VPC	Tres	Tres AZS/subredes	Dominio

Entidad	Destino	ENI inyectado	Notas	Nivel
Puntos de conexión de VPC	Subredes de la VPC	30	Tres subredes AZS con 10 VPCE cada una	Dominio
Servidor Jupyter	Subred de VPC	Uno	Una IP por instancia	Usuario
KernelGateway aplicación	Subred de VPC	Dos	Una IP por tipo de instancia	Usuario
Formación	Subred de VPC	Dos	Dos IP por instancia de entrenamiento Cinco IP por instancia de entrenamiento si se usa EFA	Usuario

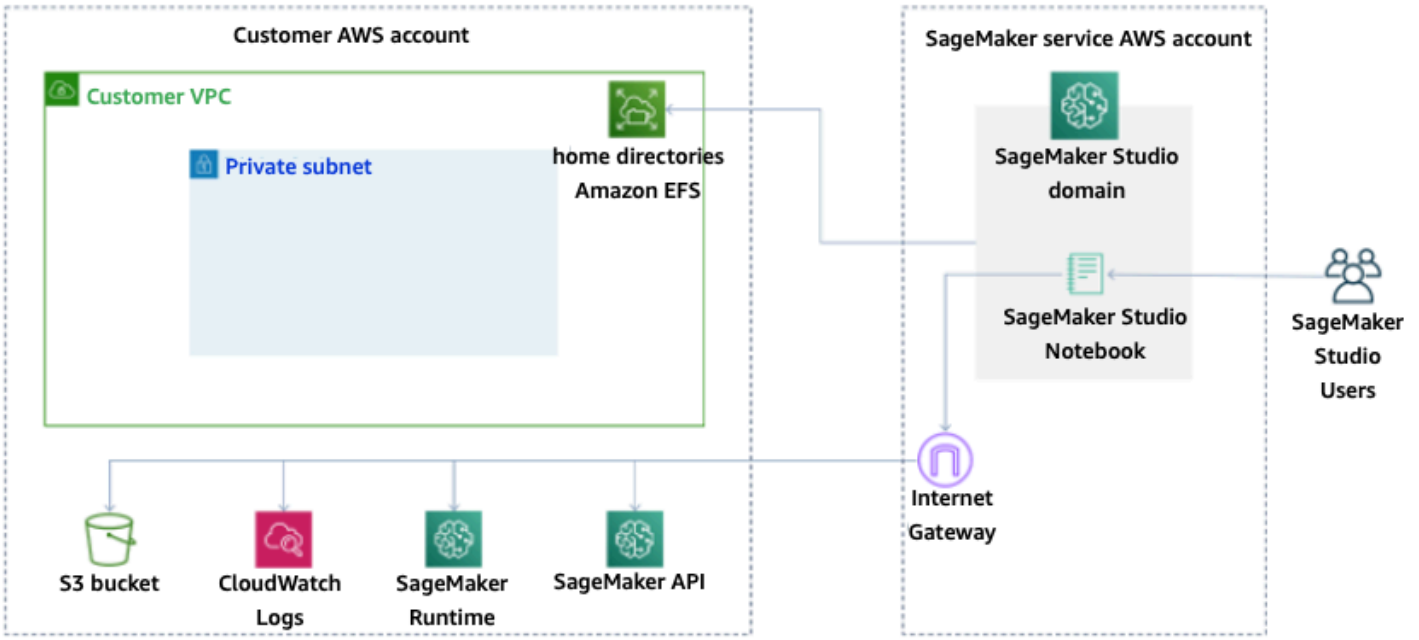
Para este escenario, hay un total de 38 IP consumidas en la VPC del cliente, de las que 33 IP se comparten entre los usuarios a nivel de dominio y cinco IP se consumen a nivel de usuario. Si tiene 100 usuarios con perfiles de usuario similares en este dominio que realizan estas actividades de forma simultánea, consumirá cinco x 100 = 500 IP a nivel de usuario, además del consumo de IP a nivel de dominio, que es de 11 IP por subred, para un total de 511 IP. Para este escenario, debe crear el CIDR de subred de VPC con /22 que asignará 1024 direcciones IP, con espacio para crecer.

Opciones de red de VPC

Un dominio de SageMaker Studio admite la configuración de la red de VPC con una de las siguientes opciones:

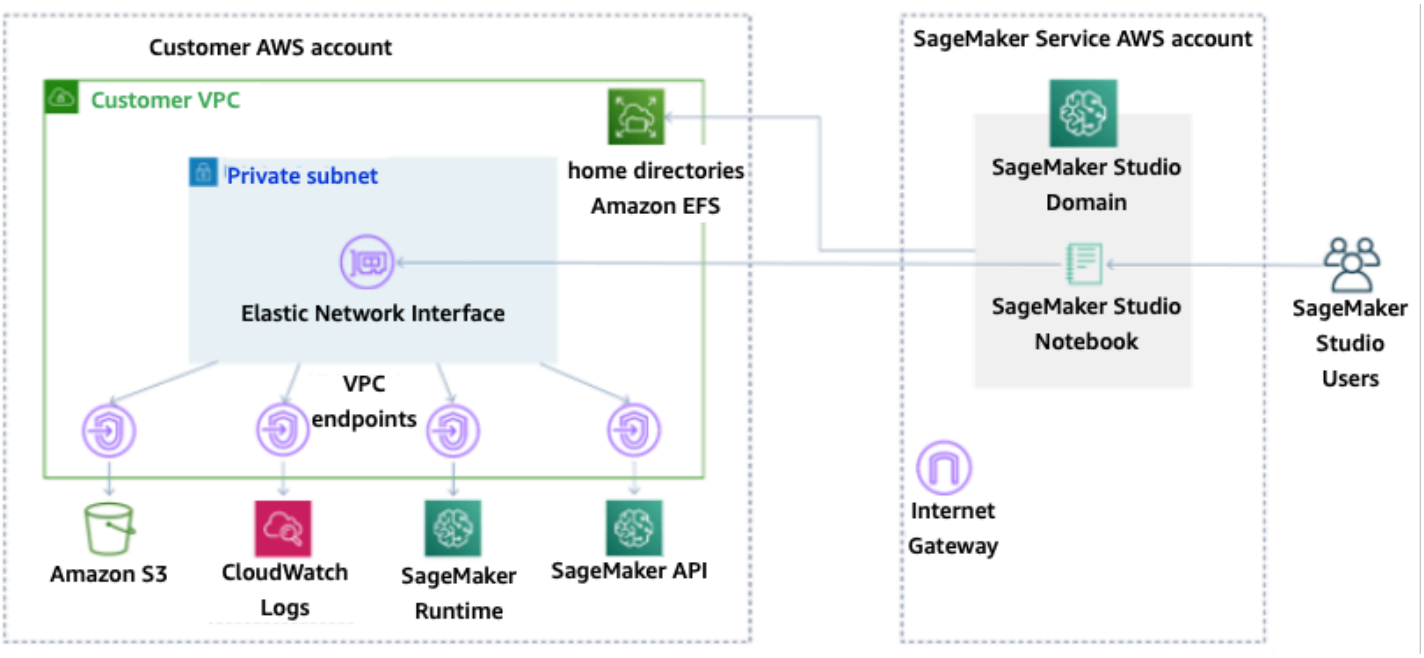
- Solo Internet público
- VPC solo

La opción solo para Internet pública permite que los servicios de SageMaker API usen Internet pública a través de la puerta de enlace de Internet aprovisionada en la VPC, administrada por SageMaker la cuenta de servicio, como se muestra en el siguiente diagrama:



Modo predeterminado: acceso a Internet a través de una cuenta SageMaker de servicio

La opción solo para VPC deshabilita el enrutamiento de Internet desde la VPC administrada por la cuenta de SageMaker servicio y permite al cliente configurar el tráfico para que se enrute a través de los puntos finales de la VPC, como se muestra en el siguiente diagrama:



Modo solo VPC: sin acceso a Internet a través SageMaker de la cuenta de servicio

Para un dominio configurado solo en modo VPC, configure un grupo de seguridad por perfil de usuario para garantizar el aislamiento completo de las instancias subyacentes. Cada dominio de una AWS cuenta puede tener su propia configuración de VPC y modo de Internet. Para obtener más información sobre la configuración de la red de la VPC, consulte Connect SageMaker Studio Notebooks in a External Resources.

Limitaciones

- Una vez creado un dominio de SageMaker Studio, no puedes asociar nuevas subredes al dominio.
- No se puede cambiar el tipo de red de la VPC (solo Internet pública o solo VPC).

Protección de los datos

Antes de diseñar una carga de trabajo de machine learning, se deben implementar las prácticas fundamentales que influyen en la seguridad. Por ejemplo, la clasificación de datos proporciona una forma de categorizar los datos en función de los niveles de confidencialidad, y el cifrado protege los datos al hacerlos ininteligibles para el acceso no autorizado. Estos métodos son importantes porque respaldan objetivos como evitar una administración incorrecta o cumplir las obligaciones reglamentarias.

SageMaker Studio ofrece varias funciones para proteger los datos en reposo y en tránsito. Sin embargo, como se describe en el Modelo de responsabilidad compartida de AWS, los clientes son responsables de mantener el control sobre el contenido que se aloja en la infraestructura global de AWS. En esta sección, se describe cómo los clientes pueden usar esas funciones para proteger sus datos.

Proteger los datos en reposo

Para proteger sus cuadernos de SageMaker Studio junto con sus datos de creación de modelos y artefactos de modelos, SageMaker cifra los cuadernos, así como el resultado de los trabajos de entrenamiento y transformación por lotes. SageMaker los cifra de forma predeterminada utilizando la clave administrada de AWS para Amazon S3. Esta clave administrada de AWS para Amazon S3 no se puede compartir para el acceso entre cuentas. Para el acceso entre cuentas, especifique la clave administrada por el cliente al crear los recursos de SageMaker para que pueda compartirla para el acceso entre cuentas.

Con SageMaker Studio, los datos se pueden almacenar en las siguientes ubicaciones:

- Bucket de S3: cuando se habilita un cuaderno compartible, SageMaker Studio comparte las instantáneas y los metadatos del cuaderno en un bucket de S3.
- Volumen de EFS: SageMaker Studio asocia un volumen de EFS a su dominio para almacenar cuadernos y archivos de datos. Este volumen de EFS persiste incluso después de eliminar el dominio.
- Volumen de EBS: EBS se asocia a la instancia en la que se ejecuta el cuaderno. Este volumen se conserva mientras dure la instancia.

Cifrado en reposo con AWS KMS

- Puede pasar su clave de AWS KMS para cifrar un volumen de EBS asociado con cuadernos, entrenamientos, ajustes, trabajos de transformación por lotes y puntos de conexión.
- Si no especifica una clave de KMS, SageMaker cifra los volúmenes del sistema operativo (SO) y los volúmenes de datos de ML con una clave de KMS administrada por el sistema.
- La información confidencial que por razones de conformidad tenga que cifrarse con una clave de KMS debe almacenarse en el volumen de almacenamiento de ML o en Amazon S3, ya que ambos permiten especificar una clave de KMS para el cifrado.

Protección de los datos en tránsito

SageMaker Studio garantiza que los artefactos del modelo de ML y otros artefactos del sistema estén cifrados en tránsito y en reposo. Las solicitudes a la API de SageMaker se efectúan a través de una conexión segura (SSL). Algunos datos dentro de la red en tránsito (dentro de la plataforma de servicios) no están cifrados. Esto incluye:

- Comando y control de las comunicaciones entre el plano de control de servicio y las instancias de trabajo de capacitación (no los datos del cliente).
- Comunicaciones entre nodos en trabajos de entrenamiento y procesamiento distribuido (dentro de la red).

Sin embargo, puede optar por cifrar la comunicación entre los nodos de un clúster de entrenamiento. La habilitación del cifrado de tráfico entre contenedores puede aumentar el tiempo de capacitación, especialmente si se utilizan algoritmos de aprendizaje profundo distribuidos.

De forma predeterminada, Amazon SageMaker ejecuta trabajos de entrenamiento en una Amazon VPC para ayudar a mantener sus datos seguros. Puede añadir otro nivel de seguridad para proteger los contenedores de capacitación y los datos mediante la configuración de una VPC privada. Además, puede configurar su dominio de SageMaker Studio para que se ejecute solo en modo VPC y configurar los puntos de conexión de VPC para enrutar el tráfico a través de una red privada sin que el tráfico de salida pase por Internet.

Barreras de protección de datos

Cifrar los volúmenes de alojamiento de SageMaker en reposo

Utilice la siguiente política para aplicar el cifrado durante el alojamiento de un punto de conexión de SageMaker para realizar inferencias en línea:

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateEndpointConfig"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false"
             }
         }
     }
   ]
 }
```

Cifrar los buckets de S3 utilizados durante la supervisión de modelos

La Supervisión de modelos captura los datos enviados a su punto de conexión de SageMaker y los almacena en un bucket de S3. Al realizar la configuración de captura de datos, debe cifrar el bucket de S3. Actualmente, no existe ningún control compensatorio para ello.

Además de recopilar los resultados de los puntos de conexión, el servicio de supervisión de modelos comprueba si hay desviaciones respecto a una línea base previamente especificada. Debe cifrar las salidas y los volúmenes de almacenamiento intermedios utilizados para supervisar la desviación.

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
```

```
        "Sid": "Encryption",
        "Effect": "Allow",
        "Action": [
            "sagemaker:CreateMonitoringSchedule",
            "sagemaker:UpdateMonitoringSchedule"
        ],
        "Resource": "*",
        "Condition": {
            "Null": {
                "sagemaker:VolumeKmsKey": "false",
                "sagemaker:OutputKmsKey": "false"
            }
        }
    }
  ]
}
```

Cifrar un volumen de almacenamiento de dominio de SageMaker Studio

Aplique el cifrado al volumen de almacenamiento asociado con el dominio de Studio. Esta política requiere que el usuario proporcione una CMK para cifrar los volúmenes de almacenamiento asociados con los dominios de Studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EncryptDomainStorage",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:VolumeKmsKey": "false"
                }
            }
        }
    ]
}
```

Cifrar los datos almacenados en S3 que se utilizan para compartir cuadernos

Esta es la política para cifrar cualquier dato almacenado en el bucket que se utiliza para compartir cuadernos entre los usuarios de un dominio de SageMaker Studio:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EncryptDomainSharingS3Bucket",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreateDomain",
                 "sagemaker:UpdateDomain"
             ],
             "Resource": "*",
             "Condition": {
                 "Null": {
                     "sagemaker:DomainSharingOutputKmsKey": "false"
                 }
             }
         }
     ]
 }
```

Limitaciones

- Una vez creado un dominio, no puede actualizar el volumen de almacenamiento de EFS asociado con una clave de AWS KMS personalizada.
- No puede actualizar los trabajos de entrenamiento/procesamiento ni las configuraciones de los puntos de conexión con claves de KMS una vez que se hayan creado.

Registro y monitoreo

Para ayudarle a depurar los trabajos de compilación, los trabajos de procesamiento, los trabajos de entrenamiento, los puntos de conexión, los trabajos de transformación, las instancias de cuaderno y las configuraciones del ciclo de vida de las instancias de cuaderno, todo lo que un contenedor de algoritmos, un contenedor de modelos o una configuración del ciclo de vida de una instancia de cuaderno envíe a stdout o stderr también se envía a los Registros de Amazon CloudWatch. Puede supervisar SageMaker Studio mediante Amazon CloudWatch, que recopila y procesa los datos sin procesar y los convierte en métricas legibles y casi en tiempo real. Estas estadísticas se mantienen durante 15 meses, para que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio.

Registro con CloudWatch

Como el proceso de ciencia de datos es intrínsecamente experimental e iterativo, es esencial registrar la actividad como el uso del cuaderno, el tiempo de ejecución de las tareas de entrenamiento/procesamiento, las métricas de entrenamiento y las métricas de servicio de puntos de conexión como, por ejemplo, la latencia de invocación. De forma predeterminada, SageMaker publica las métricas en los Registros de CloudWatch, y estos registros se pueden cifrar con claves administradas por el cliente utilizando AWS KMS.

También puede usar puntos de conexión de VPC para enviar registros a CloudWatch sin usar la Internet pública. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

SageMaker crea un único grupo de registro para Studio, en `/aws/sagemaker/studio`. Cada perfil de usuario y cada aplicación tiene su propio flujo de registro en este grupo de registro, y los scripts de configuración del ciclo de vida también tienen su propio flujo de registro. Por ejemplo, un perfil de usuario denominado “studio-user” con una aplicación de servidor de Jupyter y con un script de ciclo de vida asociado, y una aplicación de puerta de enlace del kernel de Ciencia de datos tiene los siguientes flujos de registro:

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default
```

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default/
LifecycleConfigOnStart
```

`/aws/sagemaker/studio/<domain-id>/studio-user/KernelGateway/datascience-app`

Para que SageMaker envíe registros a CloudWatch en su nombre, el intermediario de las API de trabajo de Entrenamiento /Procesamiento /Transformación necesitará los siguientes permisos:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "logs:CreateLogDelivery",
                 "logs:CreateLogGroup",
                 "logs:CreateLogStream",
                 "logs:DeleteLogDelivery",
                 "logs:Describe*",
                 "logs:GetLogEvents",
                 "logs:GetLogDelivery",
                 "logs:ListLogDeliveries",
                 "logs:PutLogEvents",
                 "logs:PutResourcePolicy",
                 "logs:UpdateLogDelivery"
             ],
             "Resource": "*",
             "Effect": "Allow"
         }
     ]
 }
```

Para cifrar esos registros con una clave de AWS KMS personalizada, primero tendrá que modificar la política de claves para permitir que el servicio CloudWatch cifre y descifre la clave. Una vez que haya creado una clave de AWS KMS de cifrado de registros, modifique la política de claves para incluir lo siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
```

```
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
    ]
}
```

Tenga en cuenta que siempre puede usar `ArnEquals` y proporcionar un Nombre de recurso de Amazon (ARN) específico para el registro de CloudWatch que desee cifrar. Aquí se muestra cómo puede usar esta clave para cifrar todos los registros de una cuenta a efectos de simplicidad. Además, los puntos de conexión de entrenamiento, procesamiento y modelo publican métricas sobre el uso de la CPU y la memoria de la instancia, la latencia de invocación del alojamiento, etc. También puede configurar Amazon SNS para que avise a los administradores de los eventos cuando se superen determinados umbrales. El consumidor de las API de entrenamiento y procesamiento debe tener los siguientes permisos:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "cloudwatch:DeleteAlarms",
                 "cloudwatch:DescribeAlarms",
                 "cloudwatch:GetMetricData",
                 "cloudwatch:GetMetricStatistics",
                 "cloudwatch:ListMetrics",
                 "cloudwatch:PutMetricAlarm",
                 "cloudwatch:PutMetricData",
                 "sns:ListTopics"
             ],
             "Resource": "*",
             "Effect": "Allow",
```

```
            "Condition": {
                "StringLike": {
                    "cloudwatch:namespace": "aws/sagemaker/*"
                }
            }

        },
        {
            "Action": [
                "sns:Subscribe",
                "sns:CreateTopic"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*SageMaker*",
                "arn:aws:sns:*:*:*Sagemaker*",
                "arn:aws:sns:*:*:*sagemaker*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Auditoría con AWS CloudTrail

Para mejorar su postura de conformidad, audite todas sus API conAWS CloudTrail. De forma predeterminada, todas las API de SageMaker se registran con AWS CloudTrail. No necesita permisos de IAM adicionales para activar CloudTrail.

Todas las acciones de SageMaker, con la excepción de `InvokeEndpoint` y `InvokeEndpointAsync`, están registradas por CloudTrail y se documentan en las operaciones. Por ejemplo, las llamadas a las acciones `CreateTrainingJob`, `CreateEndpoint` y `CreateNotebookInstance` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de evento de CloudTrail contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM de AWS.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS. Para ver un ejemplo de evento, consulte la documentación de Registrar llamadas a la API de SageMaker con CloudTrail.

De forma predeterminada, CloudTrail registra el nombre del rol de ejecución de Studio del perfil de usuario como el identificador de cada evento. Esto funciona si cada usuario tiene su propio rol de ejecución. Si varios usuarios comparten el mismo rol de ejecución, puede usar la configuración de `sourceIdentity` para propagar el nombre del perfil de usuario de Studio a CloudTrail. Consulte Supervisión del acceso a los recursos de usuario desde Amazon SageMaker Studio para activar la característica `sourceIdentity`. En un espacio compartido, todas las acciones hacen referencia al ARN del espacio como la fuente y no puede realizar la auditoría utilizando `sourceIdentity`.

Atribución de costos

SageMaker Studio ha incorporado funciones para ayudar a los administradores a realizar un seguimiento del gasto de sus dominios individuales, espacios compartidos y usuarios.

Etiquetado automatizado

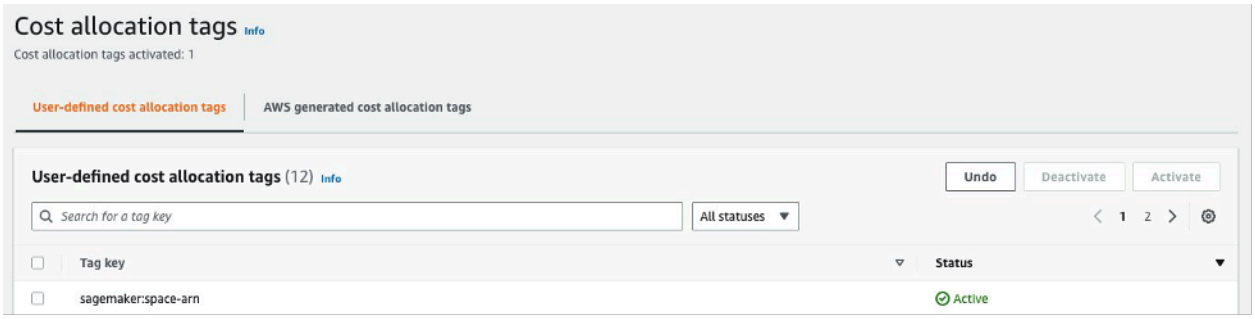
SageMaker Studio ahora etiqueta automáticamente los nuevos recursos de SageMaker como, por ejemplo, los trabajos de entrenamiento, los trabajos de procesamiento y las aplicaciones de kernel con su respectivo `sagemaker:domain-arn`. A un nivel más detallado, SageMaker también etiqueta el recurso con `sagemaker:user-profile-arn` o `sagemaker:space-arn` para designar al creador principal del recurso.

Los volúmenes EFS del dominio de SageMaker se etiquetan con una clave denominada `ManagedByAmazonSageMakerResource` con el valor del ARN del dominio. No tienen etiquetas granulares para comprender el uso del espacio a nivel de usuario. Sin embargo, los administradores pueden asociar el volumen de EFS a una instancia de EC2 para garantizar una supervisión personalizada.

Supervisión de costos

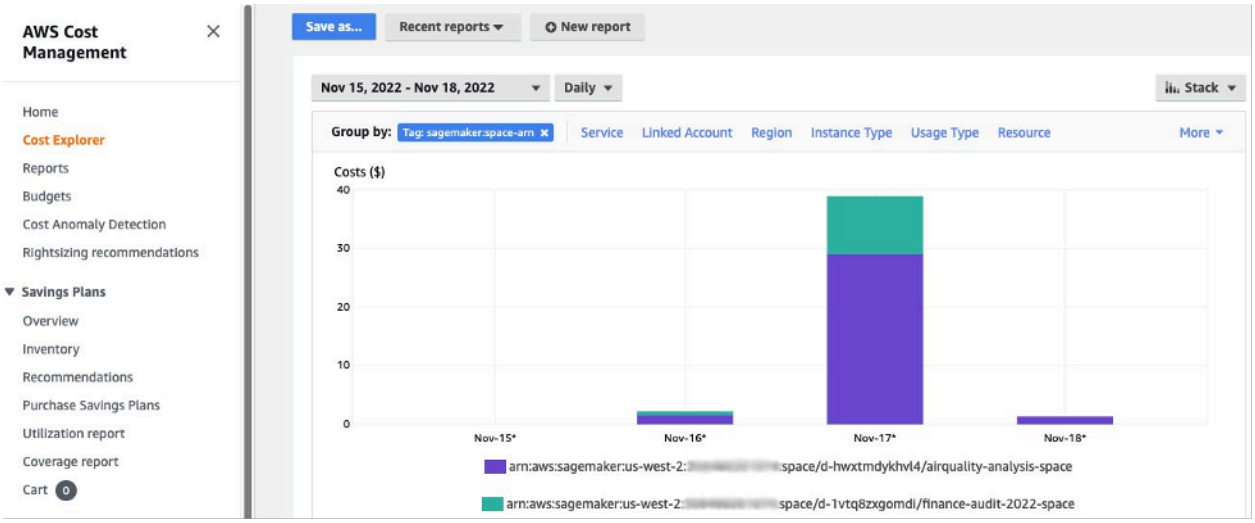
Las etiquetas automatizadas permiten a los administradores realizar un seguimiento, elaborar informes y supervisar su gasto en machine learning mediante soluciones listas para usar como, por ejemplo, AWS Cost Explorer y AWS Budgets, así como soluciones personalizadas basadas en los datos de los informes de costos y uso de AWS (CUR).

Para utilizar las etiquetas adjuntas para el análisis de costos, primero hay que activarlas en la sección Etiquetas de asignación de costos de la consola de AWS Billing. Las etiquetas pueden tardar hasta 24 horas en aparecer en el panel de etiquetas de asignación de costos, por lo que deberá crear un recurso de SageMaker antes de habilitarlas.



El ARN de espacio está habilitado como etiquetas de asignación de costos en el Explorador de costos

Una vez que haya activado una etiqueta de asignación de costos, AWS empezará a rastrear los recursos etiquetados y, después de 24-48 horas, las etiquetas aparecerán como filtros seleccionables en el explorador de costos.



Los costos se agrupan por espacio compartido para un dominio de muestra

Control de costos

Cuando se incorpora el primer usuario de SageMaker Studio, SageMaker crea un volumen de EFS para el dominio. Este volumen de EFS implica costos de almacenamiento, ya que los cuadernos y los archivos de datos se almacenan en el directorio principal del usuario. Cuando el usuario lanza cuadernos de Studio, los lanza para las instancias de procesamiento que ejecutan los cuadernos. Consulte los Precios de Amazon SageMaker para obtener un desglose detallado de los costos.

Los administradores pueden controlar los costos de procesamiento especificando la lista de instancias que un usuario puede poner en marcha, utilizando las políticas de IAM, tal como se describe en la sección Barreras de protección más comunes. Además, recomendamos a los clientes que utilicen la Extensión de apagado automático de SageMaker Studio para ahorrar costos al cerrar automáticamente las aplicaciones inactivas. Esta extensión de servidor sondea periódicamente si hay aplicaciones en ejecución por perfil de usuario, y cierra las aplicaciones inactivas en función del tiempo de espera establecido por el administrador.

Para configurar esta extensión para todos los usuarios de su dominio, puede usar una configuración de ciclo de vida tal como se describe en la sección Personalización. Además, también puede usar

el comprobador de extensiones para asegurarse de que todos los usuarios de su dominio tengan la extensión instalada.

Personalización

Configuración del ciclo de vida

Las configuraciones del ciclo de vida son scripts de intérpretes de comandos iniciados por eventos del ciclo de vida de SageMaker Studio como, por ejemplo, iniciar un nuevo cuaderno de SageMaker Studio. Puede utilizar estos scripts de intérpretes de comandos para automatizar la personalización de sus entornos de SageMaker Studio como, por ejemplo, la instalación de paquetes personalizados, la extensión de Jupyter para el cierre automático de las aplicaciones de cuadernos inactivas y la configuración de Git. Para obtener instrucciones detalladas sobre cómo crear configuraciones de ciclo de vida, consulte este blog: Personalización de Amazon SageMaker Studio mediante configuraciones de ciclo de vida.

Imágenes personalizadas para cuadernos de SageMaker Studio

Los cuadernos de Studio incluyen un conjunto de imágenes prediseñadas, que se componen del SDK de Python de Amazon SageMaker y la última versión del kernel o el tiempo de ejecución de iPython. Con esta función, puede llevar sus propias imágenes personalizadas a los cuadernos de Amazon SageMaker. Estas imágenes estarán disponibles para todos los usuarios autenticados en el dominio.

Los desarrolladores y los científicos de datos pueden necesitar imágenes personalizadas para varios casos de uso diferentes:

- Acceso a versiones específicas o más recientes de marcos de machine learning populares, como TensorFlow, MXNet, PyTorch u otros.
- Incorpore código personalizado o algoritmos desarrollados localmente en los cuadernos de SageMaker Studio para garantizar una iteración rápida y el entrenamiento de modelos.
- Acceda a lagos de datos o almacenes de datos en las instalaciones utilizando API. Los administradores deben incluir los controladores correspondientes en la imagen.
- Acceso a un tiempo de ejecución de backend (también denominado kernel) distinto de IPython (por ejemplo, R, Julia u otros). También puede utilizar el enfoque que se describe para instalar un kernel personalizado.

Para obtener instrucciones detalladas sobre cómo crear una imagen personalizada, consulte Crear una imagen de SageMaker personalizada.

Extensiones de JupyterLab

Con SageMaker Studio JuypterLab 3 Notebook, puede aprovechar la creciente comunidad de extensiones de código abierto de JupyterLab. En esta sección, se destacan algunas que se adaptan perfectamente al flujo de trabajo de los desarrolladores de SageMaker, aunque le recomendamos explorar las extensiones disponibles o incluso crear las suyas propias.

JupyterLab 3 ahora facilita considerablemente el proceso de empaquetado e instalación de extensiones. Puede instalar las extensiones anteriores utilizando scripts bash. Por ejemplo, en SageMaker Studio, abra el terminal del sistema desde el lanzador de Studio y ejecute los siguientes comandos. Además, puede automatizar la instalación de estas extensiones utilizando configuraciones de ciclo de vida para que persistan entre los reinicios de Studio. Puede configurarlo para todos los usuarios del dominio o a nivel de usuario individual.

Por ejemplo, para instalar una extensión para un navegador de archivos Amazon S3, ejecute los siguientes comandos en el terminal del sistema y asegúrese de actualizar el navegador:

```
conda init
conda activate studio
pip install jupyterlab_s3_browser
jupyter serverextension enable --py jupyterlab_s3_browser
conda deactivate
restart-jupyter-server
```

Para obtener más información sobre la administración de extensiones, incluido cómo escribir configuraciones del ciclo de vida que funcionen para las versiones 1 y 3 de los cuadernos de JupyterLab para garantizar la compatibilidad con versiones anteriores, consulte Instalación de extensiones de JupyterLab y servidor de Jupyter.

Repositorios de Git

SageMaker Studio viene preinstalado con una extensión Git de Jupyter para que los usuarios puedan introducir una URL personalizada de un repositorio de Git, clonarla en su directorio EFS, enviar los cambios y consultar el historial de confirmaciones. Los administradores pueden configurar los repositorios de Git recomendados a nivel de dominio para que aparezcan como selecciones desplegables para los usuarios finales. Consulte Asociación de los repositorios de Git sugeridos a Studio para obtener instrucciones actualizadas.

Si un repositorio es privado, la extensión le pedirá al usuario que introduzca sus credenciales en el terminal mediante la instalación estándar de Git. Como alternativa, el usuario puede almacenar las credenciales SSH en su directorio EFS individual para facilitar la administración.

Entorno Conda

Los cuadernos de SageMaker Studio utilizan Amazon EFS como capa de almacenamiento persistente. Los científicos de datos pueden utilizar el almacenamiento persistente para crear entornos conda personalizados y utilizar estos entornos para crear kernels. Estos kernels están respaldados por EFS y son persistentes entre los reinicios de kernel, aplicación o Studio. Studio selecciona automáticamente todos los entornos válidos como kernels de KernelGateway.

El proceso de creación de un entorno conda es sencillo para un científico de datos, pero los kernels tardan aproximadamente un minuto en rellenarse en el selector de kernels. Para crear un entorno, ejecute lo siguiente en una terminal del sistema:

```
mkdir -p ~/.conda/envs
conda create --yes -p ~/.conda/envs/custom
conda activate ~/.conda/envs/custom
conda install -y ipykernel
conda config --add envs_dirs ~/.conda/envs
```

Para ver instrucciones detalladas, consulte la sección Mantener los entornos de Conda en el volumen de EFS de Studio en Cuatro enfoques para administrar paquetes de Python en los cuadernos de Amazon SageMaker Studio.

Conclusión

En este documento técnico, hemos revisado varias prácticas recomendadas en áreas como el modelo operativo, la administración de dominios, la administración de identidades, la administración de permisos, la administración de redes, el registro, la supervisión y la personalización para permitir a los administradores de la plataforma configurar y administrar la plataforma SageMaker Studio.

Apéndice

Comparación de varios arrendatarios

Tabla 2: Comparación de varios arrendatarios

Multidominio	Cuenta múltiple	Control de acceso basado en atributos (ABAC) dentro de un único dominio
El aislamiento de los recursos se logra mediante etiquetas . SageMaker Studio etiqueta automáticamente todos los recursos con el ARN del dominio y el ARN del espacio o perfil de usuario.	Cada inquilino está en su propia cuenta, por lo que hay un aislamiento absoluto de los recursos.	El aislamiento de los recursos se logra mediante etiquetas. Los usuarios deben gestionar el etiquetado de los recursos creados para ABAC.
Las API de listas no se pueden restringir mediante etiquetas. El filtrado de los recursos a través de la interfaz de usuario se realiza en espacios compartidos; sin embargo, las llamadas a la API de listas realizadas a través del SDK de Boto3 AWS CLI o del SDK de Boto3 mostrarán los recursos de la región.	También es posible aislar las API de listas, ya que los inquilinos están en sus cuentas dedicadas.	Las API de listas no se pueden restringir mediante etiquetas. Las llamadas a la API de lista realizadas a través del SDK de Boto3 AWS CLI o del SDK mostrarán los recursos de la región.
SageMaker Los costos de procesamiento y almacenam iento de Studio por inquilino se pueden monitorear fácilmente mediante el ARN de dominio	SageMaker Los costes informáticos y de almacenam iento de Studio por inquilino son fáciles de supervisar con una cuenta dedicada.	SageMaker Los costes de Studio Compute por inquilino deben calcularse mediante etiquetas personalizadas.

Multidominio	Cuenta múltiple	Control de acceso basado en atributos (ABAC) dentro de un único dominio
como etiqueta de asignación de costos.		SageMaker Los costos de almacenamiento de Studio no se pueden monitorear por dominio, ya que todos los inquilinos comparten el mismo volumen de EFS.
Las cuotas de servicio se establecen a nivel de cuenta, por lo que un solo inquilino podría seguir consumiendo todos los recursos.	Las cuotas de servicio se pueden establecer a nivel de cuenta para cada inquilino.	Las cuotas de servicio se establecen a nivel de cuenta, por lo que un solo inquilino podría seguir consumiendo todos los recursos.
El escalamiento a varios inquilinos se puede lograr mediante la infraestructura como código (IaC) o Service Catalog.	La ampliación a varios inquilinos implica Organizat ions y la venta de varias cuentas.	Scaling necesita un rol de inquilino específico para cada nuevo inquilino, y los perfiles de usuario deben etiquetarse manualmente con los nombres de los inquilinos.
La colaboración entre los usuarios de un inquilino es posible a través de los espacios compartidos.	La colaboración entre un usuario y un inquilino es posible a través de espacios compartidos.	Todos los inquilinos tendrán acceso al mismo espacio compartido para la colaborac ión.

SageMaker Respaldo y recuperación de dominios de Studio

En caso de que se elimine accidentalmente el EFS o cuando sea necesario volver a crear un dominio debido a cambios en la red o la autenticación, siga estas instrucciones.

Opción 1: realizar copias de seguridad de los EFS existentes mediante EC2

SageMaker Respaldo de dominios de Studio

1. Enumere los perfiles de usuario y los espacios en SageMaker Studio (CLI, SDK).
2. Asigne perfiles y espacios de usuario a UID en EFS.
   a. Para cada usuario de la lista de usuarios/espacios, describa el perfil/espacio de usuario (CLI, SDK).
   b. Asigne el perfil/espacio de usuario a. `HomeEfsFileSystemUid`
   c. Asigne el perfil de usuario a `UserSettings['ExecutionRole']` si los usuarios tienen funciones de ejecución distintas.
   d. Identifique el rol de ejecución predeterminado de Space.
3. Cree un nuevo dominio y especifique la función de ejecución de Space predeterminada.
4. Cree perfiles de usuario y espacios.
   - Para cada usuario de la lista de usuarios, cree un perfil de usuario (CLI, SDK) mediante la asignación de funciones de ejecución.
5. Cree un mapeo para los nuevos EFS y UID.
   a. Para cada usuario de la lista de usuarios, describa el perfil de usuario (CLI, SDK).
   b. Asigne el perfil de usuario a`HomeEfsFileSystemUid`.
6. Si lo desea, elimine todas las aplicaciones, los perfiles de usuario y los espacios y, a continuación, elimine el dominio.

Copia de seguridad de EFS

Para hacer una copia de seguridad de EFS, siga las instrucciones siguientes:

1. Inicie la instancia EC2 y adjunte los grupos de seguridad entrantes y salientes del antiguo dominio de SageMaker Studio a la nueva instancia EC2 (permita el tráfico NFS a través de TCP en el puerto 2049). Consulte Conectar los cuadernos de SageMaker Studio de una VPC a recursos externos.
2. Monte el volumen SageMaker Studio EFS en la nueva instancia EC2. Consulte Montaje de sistemas de archivos de EFS.
3. Copie los archivos al almacenamiento local de EBS: `>sudo cp -rp /efs /studio-backup:`
   a. Adjunte los nuevos grupos de seguridad de dominio a la instancia EC2.

b. Monte el nuevo volumen EFS en la instancia EC2.

c. Copie los archivos al nuevo volumen EFS.

d. Para cada usuario de la colección de usuarios:

i. Cree el directorio: `mkdir new_uid`.

ii. Copie los archivos del antiguo directorio de UID al nuevo directorio de UID.

iii. Cambie la propiedad de todos los archivos: de todos `chown <new_UID>` los archivos.

Opción 2: realizar copias de seguridad de los EFS existentes mediante S3 y la configuración del ciclo de vida

1. Consulte Migrar su trabajo a una instancia de Amazon SageMaker Notebook con Amazon Linux 2.
2. Cree un bucket de S3 para la copia de seguridad (por ejemplo `>studio-backup`.
3. Enumere todos los perfiles de usuario con funciones de ejecución.
4. En el dominio de SageMaker Studio actual, defina un script de LCC predeterminado a nivel de dominio.
   - En la LCC, copia todo en `/home/sagemaker-user` el prefijo del perfil de usuario en S3 (por ejemplo,). `s3://studio-backup/studio-user1`
5. Reinicie todas las aplicaciones predeterminadas de Jupyter Server (para que se ejecute la LCC).
6. Elimine todas las aplicaciones, perfiles de usuario y dominios.
7. Crea un nuevo dominio de SageMaker Studio.
8. Crea nuevos perfiles de usuario a partir de la lista de perfiles de usuario y funciones de ejecución.
9. Configure una LCC a nivel de dominio:
   - En la LCC, copie todo el prefijo del perfil de usuario en S3 para `/home/sagemaker-user`
10. Cree aplicaciones predeterminadas de Jupyter Server para todos los usuarios con la configuración de LCC (CLI, SDK).

SageMaker Acceso a Studio mediante la aserción SAML

Configuración de la solución:

1. Cree una aplicación SAML en su IdP externo.
2. Configure el IdP externo como proveedor de identidad en IAM.

3. Cree una función `SAMLValidator` Lambda a la que pueda acceder el IdP (a través de una URL de función o API Gateway).
4. Cree una función `GeneratePresignedUrl` Lambda y una API Gateway para acceder a la función.
5. Cree una función de IAM que los usuarios puedan asumir para invocar la API Gateway. Esta función debe transferirse a la aserción SAML como un atributo con el siguiente formato:
   - Nombre de atributo: https://aws.amazon.com/SAML/Attributes/Role
   - Valor de atributo: `<IdentityProviderARN>`, `<RoleARN>`
6. Actualice el punto final del SAML Assertion Consumer Service (ACS) a la URL de invocación. `SAMLValidator`

Código de ejemplo del validador de SAML:

```
import requests
import os
import boto3
from urllib.parse import urlparse, parse_qs
import base64
import requests
from aws_requests_auth.aws_auth import AWSRequestsAuth
import json


# Config for calling AssumeRoleWithSAML
idp_arn = "arn:aws:iam::0123456789:saml-provider/MyIdentityProvider"
api_gw_role_arn = 'arn:aws:iam:: 0123456789:role/APIGWAccessRole'
studio_api_url = "abcdef.execute-api.us-east-1.amazonaws.com"
studio_api_gw_path = "https://" + studio_api_url + "/Prod "

# Every customer will need to get SAML Response from the POST call
def get_saml_response(event):
    saml_response_uri = base64.b64decode(event['body']).decode('ascii')
    request_body = parse_qs(saml_response_uri)
    print(f"b64 saml response: {request_body['SAMLResponse'][0]}")
    return request_body['SAMLResponse'][0]


def lambda_handler(event, context):
    sts = boto3.client('sts')
```

```
    # get temporary credentials
    response = sts.assume_role_with_saml(
                    RoleArn=api_gw_role_arn,
                    PrincipalArn=durga_idp_arn,
                    SAMLAssertion=get_saml_response(event)
                )
    auth = AWSRequestsAuth(aws_access_key=response['Credentials']['AccessKeyId'],
                      aws_secret_access_key=response['Credentials']['SecretAccessKey'],
                      aws_host=studio_api_url,
                      aws_region='us-west-2',
                      aws_service='execute-api',
                      aws_token=response['Credentials']['SessionToken'])

    presigned_response = requests.post(
        studio_api_gw_path,
        data=saml_response_data,
        auth=auth)

    return presigned_response
```

Documentación adicional

- Configuración de entornos de machine learning seguros y bien gobernados en AWS (blog de AWS)
- Configuración de Amazon SageMaker Studio para equipos y grupos con aislamiento total de recursos (blog de AWS)
- Incorporación de Amazon SageMaker Studio con AWS SSO y Okta Universal Directory (blog de AWS)
- Cómo configurar SAML 2.0 para la federación de cuentas de AWS (documentación de Okta)
- Creación de una plataforma de Machine Learning empresarial segura en AWS (guía técnica de AWS)
- Personalización de Amazon SageMaker Studio mediante configuraciones de ciclo de vida (blog de AWS)
- Incorporación de su propia imagen de contenedor personalizada en los cuadernos de Amazon SageMaker Studio (blog de AWS)
- Creación de plantillas de proyectos de SageMaker personalizadas: prácticas recomendadas (blog de AWS)
- Implementación de un modelo multicuenta con Canalizaciones de Amazon SageMaker (blog de AWS)
- Parte 1: Cómo NatWest Group creó una plataforma MLOps escalable, segura y sostenible (blog de AWS)
- Protección de las URL prefirmadas de Amazon SageMaker Studio, parte 1: Infraestructura básica (blog de AWS)

Colaboradores

Los colaboradores de este documento son:

- Ram Vittal, arquitecto de soluciones ML, Amazon Web Services
- Sean Morgan, arquitecto de soluciones ML, Amazon Web Services
- Durga Sury, arquitecto de soluciones ML, Amazon Web Services

Un agradecimiento especial a las siguientes personas que aportaron ideas, revisiones y perspectivas:

- Alessandro Cerè, arquitecto de soluciones de inteligencia artificial y machine learning, Amazon Web Services
- Sumit Thakur, líder de productos de SageMaker, Amazon Web Services
- Han Zhang, ingeniero sénior de desarrollo de software, Amazon Web Services
- Bhadrinath Pani, ingeniero de desarrollo de software, Amazon Web Services, Amazon Web Services

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Documento técnico actualizado	Se han corregido los enlaces rotos y numerosos cambios editoriales.	25 de abril de 2023
Publicación inicial	Documento técnico publicado.	19 de octubre de 2022

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.