aws

Guía del usuario

CodeWhisperer

CodeWhisperer: Guía del usuario

Table of Contents

..... vii
Pasar a Amazon Q Developer 1
Pasar a Amazon Q Developer 1
Probando las funciones de Amazon Q en su interior CodeWhisperer 1
¿Qué es CodeWhisperer? 3
CodeWhisperer en acción 5
Configuración 13
Elección del IDE 13
Instalación o actualización del IDE 14
Instalación del AWS kit de herramientas 15
Elección del método de autenticación 15
Configuración del método de autenticación 15
Obtenga una Cuenta de AWS y las credenciales de usuario raíz 15
CodeWhisperer Profesional 16
Con Organizaciones 17
Con la administración del IAM Identity Center 21
Administración de usuarios finales 28
CodeWhisperer perfiles 34
Introducción 38
Con la línea de comando 39
Instalación 39
Finalizaciones de CLI 41
Traducción 43
Debugging 45
Modificar 46
Con VS Code y JetBrains 46
Autenticación 48
Con Visual Studio (versión preliminar) 50
Con Amazon SageMaker Studio 52
Con JupyterLab 55
JupyterLab Instalándose solo 55
Con JupyterLab 4 55
Con JupyterLab 3 56
BID 56

Con Amazon EMR Studio 57
Con AWS Glue Studio 58
Con AWS Lambda 59
Habilitar los permisos de IAM para CodeWhisperer 60
Activación de Amazon CodeWhisperer con Lambda 60
Con AWS Cloud9 61
Habilitar los permisos de IAM para CodeWhisperer 61
Activar Amazon CodeWhisperer con AWS Cloud9 61
Con otros servicios de 62
Habilitar los permisos de IAM para CodeWhisperer 62
Características 63
Personalizaciones 63
Preparación 64
Creación 68
Eliminar 72
Evaluación 72
Solución de problemas 74
Activación 79
Actualizar 80
Agregación de usuarios y grupos 82
Utilización 83
Panel de control 84
Actividad de los usuarios 85
Impacto del código 85
Análisis de seguridad 85
Acciones del usuario 86
Lenguajes 91
Lenguajes 91
Pausa de sugerencias 92
Análisis de seguridad 99
idiomas admitidos 100
Ejecución de análisis de seguridad 101
Límites de datos de análisis de seguridad 105
Referencias de código 106
Visualización de las referencias de código 107
Conmutación de las referencias de código 112

Desactivación ... 117
Tipos de usuarios ... 120
Usuario raíz ... 120
Administrador del IAM Identity Center ... 120
CodeWhisperer administrador ... 120
Desarrollador de nivel profesional ... 121
Desarrollador de nivel individual ... 121
Desarrollador integrado en la consola ... 121
Ejemplos de código ... 122
Finalización de código de línea única ... 122
Generación de funciones completas ... 125
Finalización de bloques ... 133
Finalización de Docstring, JSDoc y Javadoc ... 135
L: recomendaciones ine-by-line ... 138
Facturación ... 141
Nivel personal ... 141
Nivel profesional ... 141
Dentro de la AWS consola ... 142
Facturación de las personalizaciones ... 143
Supervisión ... 144
Monitorización con CloudWatch ... 144
En toda la organización ... 146
Uso compartido de datos ... 147
Desactivación del envío de la telemetría del cliente ... 147
Cancelación del uso compartido del contenido ... 154
Cuotas ... 159
Seguridad ... 160
Resiliencia ... 161
Análisis y administración de vulnerabilidades ... 161
Seguridad administrativa ... 161
Protección de datos ... 162
AWS CloudTrail y CodeWhisperer las API ... 163
Cifrado de datos en Amazon CodeWhisperer ... 164
Protección y personalizaciones de datos ... 164
Validación de conformidad ... 165
Prácticas recomendadas de seguridad ... 166

Seguridad de la infraestructura 166
Identity and Access Management 167
Público 167
Autenticación con identidades 168
Administración de acceso mediante políticas 172
Cómo CodeWhisperer funciona Amazon con IAM 174
Ejemplos de políticas basadas en identidades 182
AWS políticas gestionadas 185
Resolución de problemas 190
Uso de roles vinculados a servicios 192
Puntos de conexión de VPC (AWS PrivateLink) 196
Consideraciones sobre los puntos CodeWhisperer finales de VPC 196
Requisitos previos 197
Creación de un punto de conexión de VPC de interfaz para CodeWhisperer 197
Utilizar un ordenador local para conectarse a un punto final CodeWhisperer 197
Uso de un IDE integrado en la consola para conectarse a un punto final CodeWhisperer 198
Conexión CodeWhisperer mediante un IDE AWS PrivateLink de terceros en una instancia de Amazon EC2 198
Historial de documentos 200

CodeWhispererLas funciones de Amazon Q están pasando a formar parte de Amazon Q Developer. Más información

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.

CodeWhisperer pasa a formar parte de Amazon Q Developer

El propósito de esta sección es explicar la relación entre CodeWhisperer un desarrollador de Amazon Q.

Amazon Q Developer es un asistente conversacional basado en inteligencia artificial (IA) generativa que puede ayudarlo a comprender, crear, ampliar y operar AWS aplicaciones. Para obtener más información, consulte la Guía del usuario para desarrolladores de Amazon Q.

Todas las funciones de CodeWhisperer se trasladarán a Amazon Q Developer.

Los administradores de CodeWhisperer Professional pueden activar la funcionalidad de desarrollo de funciones y transformación de código de Amazon Q Developer con solo pulsar un botón en la CodeWhisperer consola.

- Con Amazon Q Developer, puedes autenticarte con una identidad personal a través del Centro de identidades de IAM cuando chateas con Amazon Q en la AWS consola o en las páginas de documentación o marketing.
- Amazon Q Developer forma parte de una familia integrada de servicios que incluye Amazon Q Business y Amazon QuickSight.

Cómo cambiarse a Amazon Q Developer

Para cambiar de CodeWhisperer Professional a Amazon Q Developer Pro, utilice el siguiente procedimiento.

1. Elimine cualquier personalización existente.
2. Elimina tu CodeWhisperer perfil.
3. Suscríbase a Amazon Q Developer Pro.

Probando las funciones de Amazon Q en su interior CodeWhisperer

Puedes probar algunas funciones de Amazon Q en el IDE a través de CodeWhisperer.

Para ello, selecciona Activar las funciones de Amazon Q Developer en tu CodeWhisperer configuración.

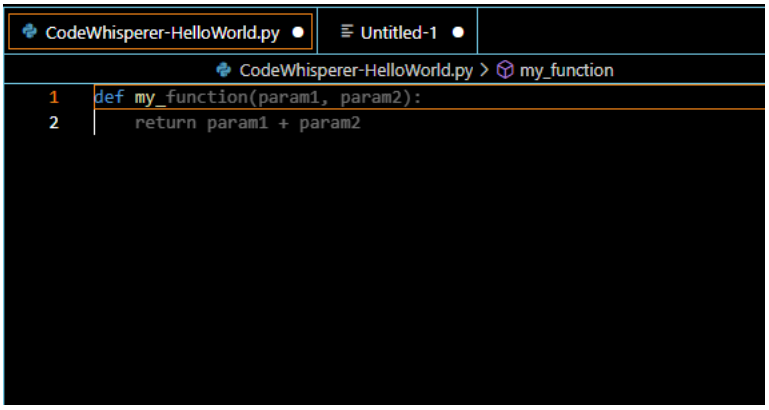
¿Qué es CodeWhisperer?

> **Note**
>
> La forma más rápida de empezar a usarlo CodeWhisperer es autenticarse ID de creador de AWS como desarrollador individual. No necesitas una AWS cuenta para hacer esto.

Amazon CodeWhisperer es un generador de código de uso general basado en el aprendizaje automático que te proporciona recomendaciones de código en tiempo real. A medida que escribes código, genera CodeWhisperer automáticamente sugerencias basadas en el código y los comentarios existentes. Las recomendaciones personalizadas pueden variar en tamaño y alcance, desde un comentario de una sola línea hasta funciones completamente formadas.

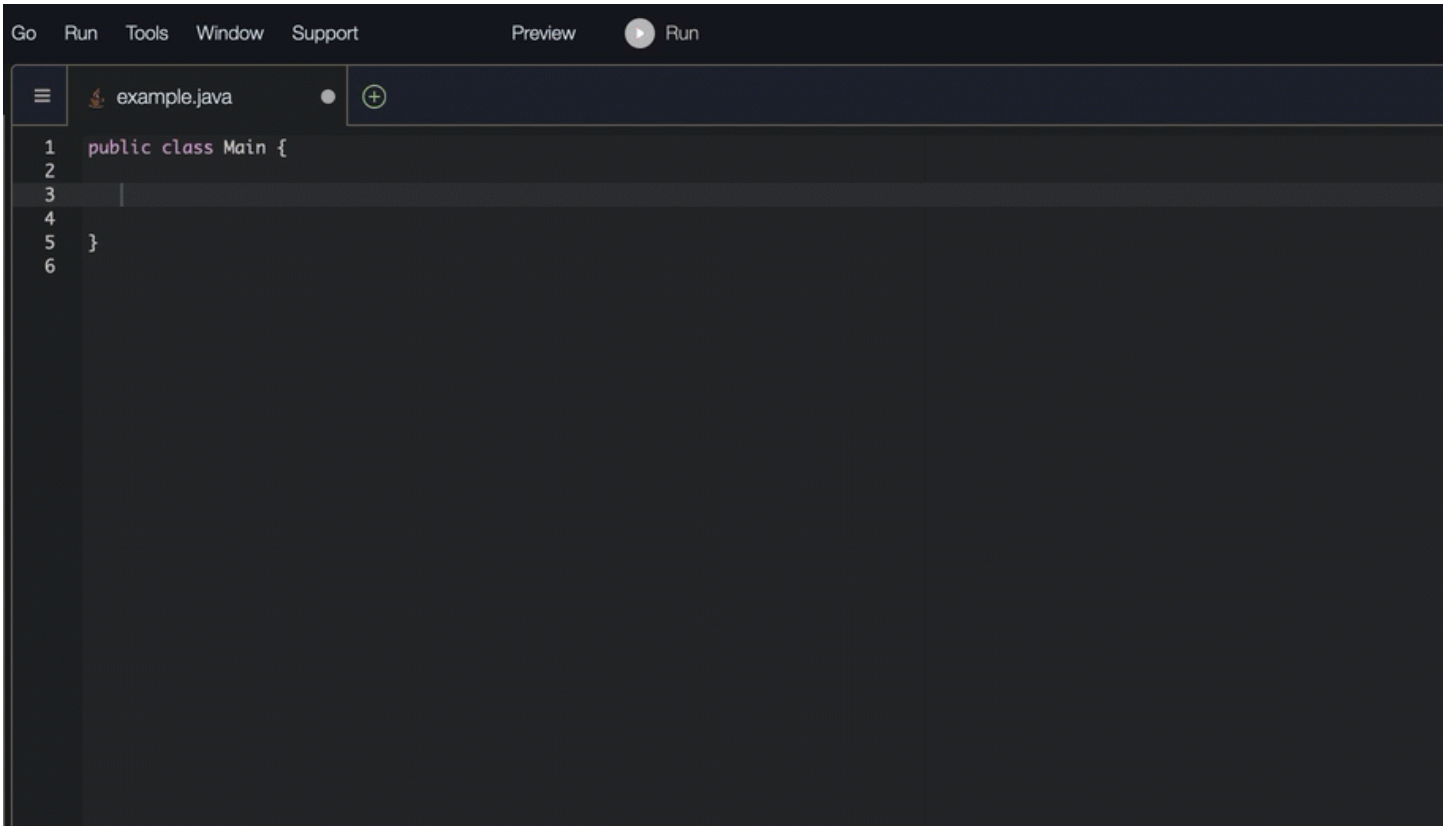
Cuando empieces a escribir líneas individuales de código o comentarios, CodeWhisperer hace sugerencias en función de tus entradas actuales y anteriores.

En la imagen de abajo, un usuario ha empezado a escribir una línea de código. En función de la entrada, CodeWhisperer ha generado sugerencias para completar la línea. El usuario puede recorrer las sugerencias con las teclas de flecha.



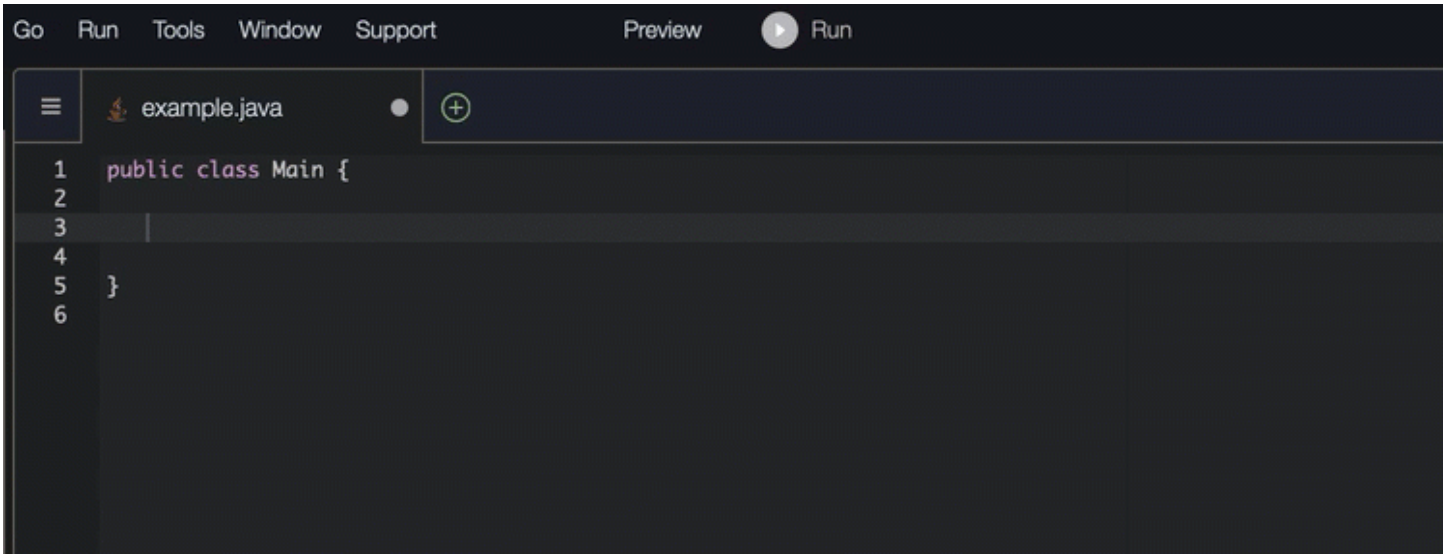
En el siguiente ejemplo, en Java, un usuario introduce un comentario. CodeWhisperer sugiere una firma de función.

Una vez que el usuario acepta esa sugerencia, CodeWhisperer sugiere el cuerpo de una función.



La finalización de bloques se utiliza para completar su bloques de código de `if/for/while/try`.

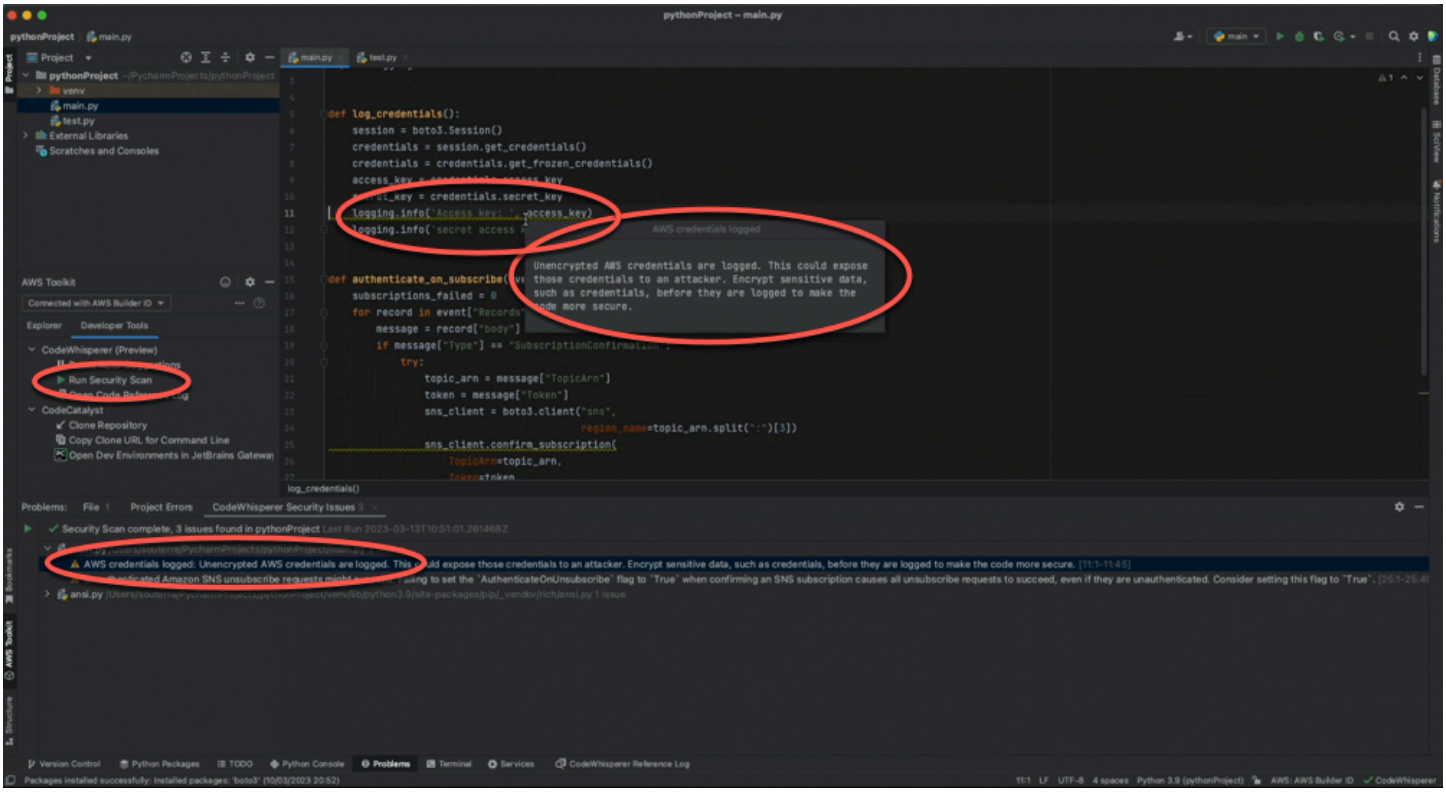
En el siguiente ejemplo, en Java, un usuario introduce la firma de una instrucción de `if`. El cuerpo de la declaración es una sugerencia de CodeWhisperer.



CodeWhisperer también puede escanear el código para resaltar y definir los problemas de seguridad.

En este ejemplo, se utiliza Python y JetBrains, el usuario ha escrito un código que escribiría AWS credenciales sin cifrar en un registro; una mala práctica de seguridad.

Afortunadamente, el usuario también ha realizado un análisis de seguridad. CodeWhisperer identificó el problema y emitió una alerta.

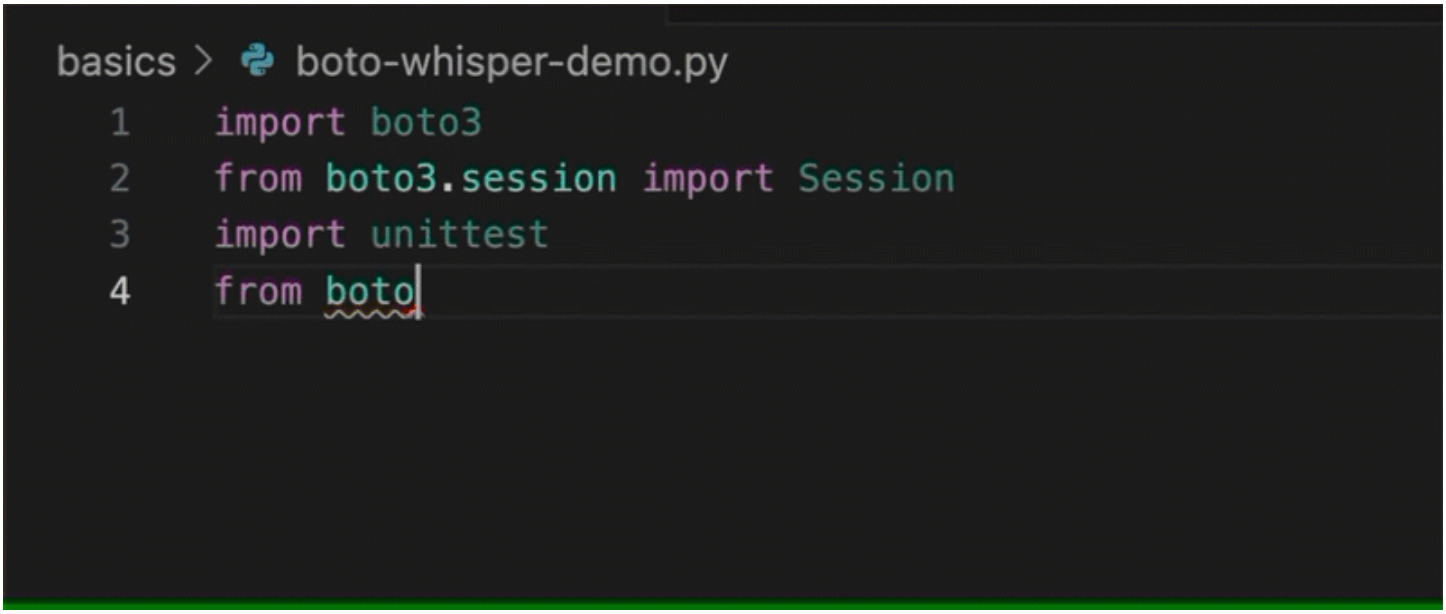


Para obtener información sobre los lenguajes de programación CodeWhisperer compatibles, consulte Compatibilidad con idiomas.

CodeWhisperer en acción

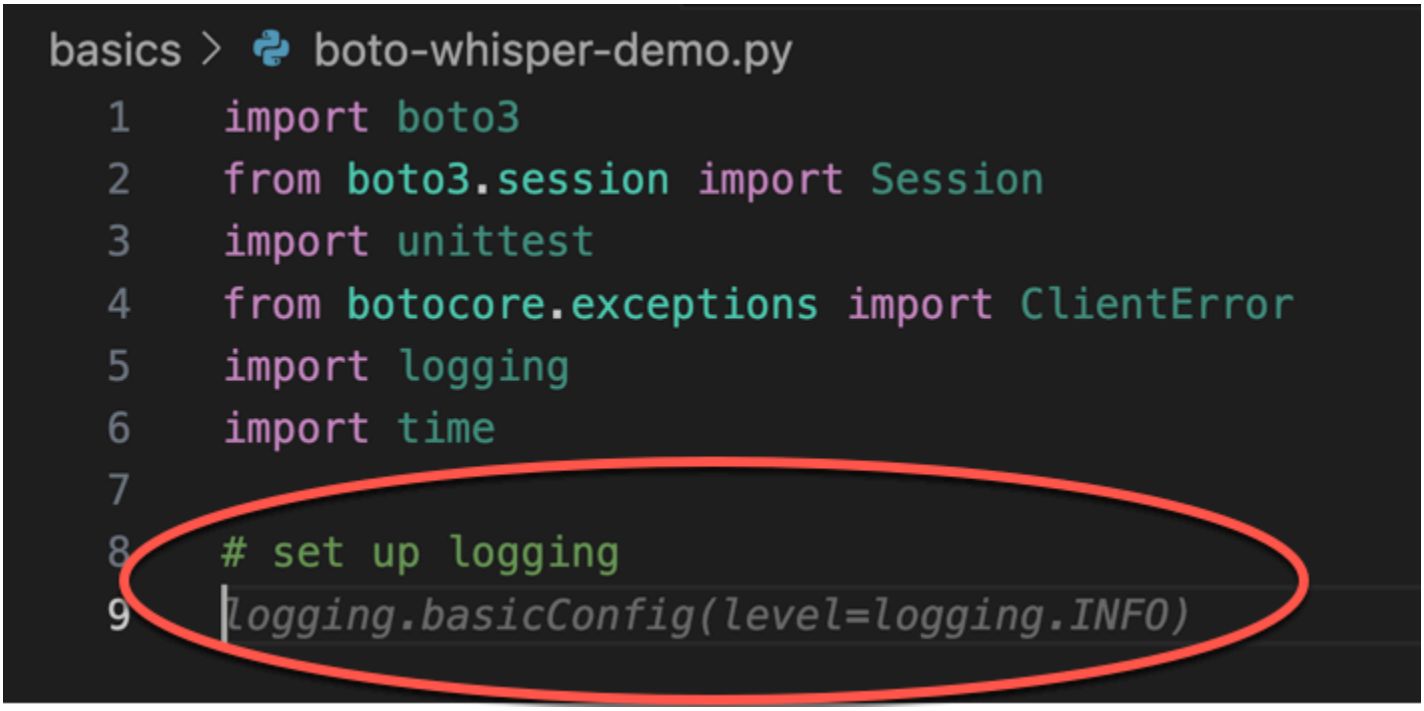
En esta sección se muestra cómo CodeWhisperer puede ayudarle a redactar una solicitud completa. Esta aplicación crea un bucket de Amazon S3 y una tabla de Amazon DynamoDB, además de una prueba unitaria que valida ambas tareas.

Aquí, CodeWhisperer ayuda al desarrollador a elegir qué bibliotecas importar. Con las teclas de flecha, el desarrollador cambia entre varias sugerencias.



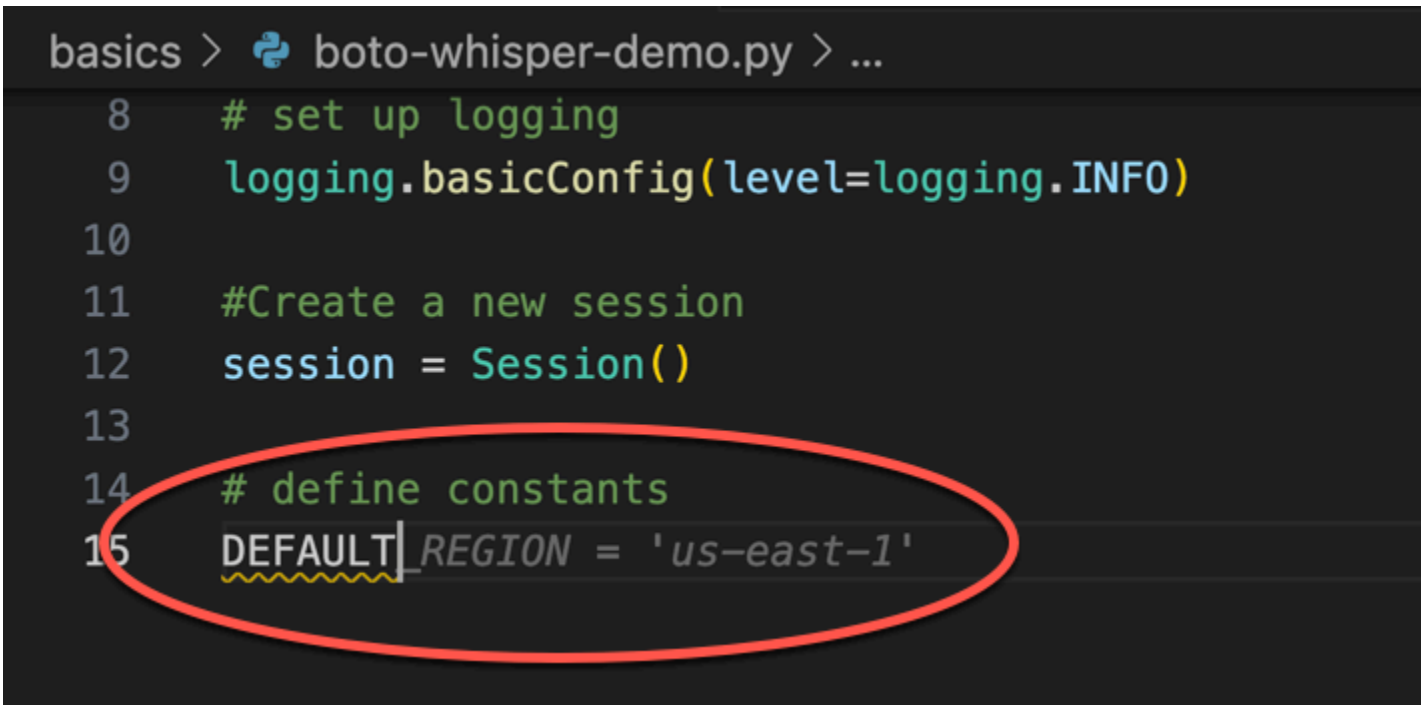
Aquí, el desarrollador ingresa un comentario, que describe el código que pretende escribir en la siguiente línea.

CodeWhisperer anticipa correctamente el método que se va a llamar. El desarrollador puede aceptar la sugerencia con la tecla de tabulación.



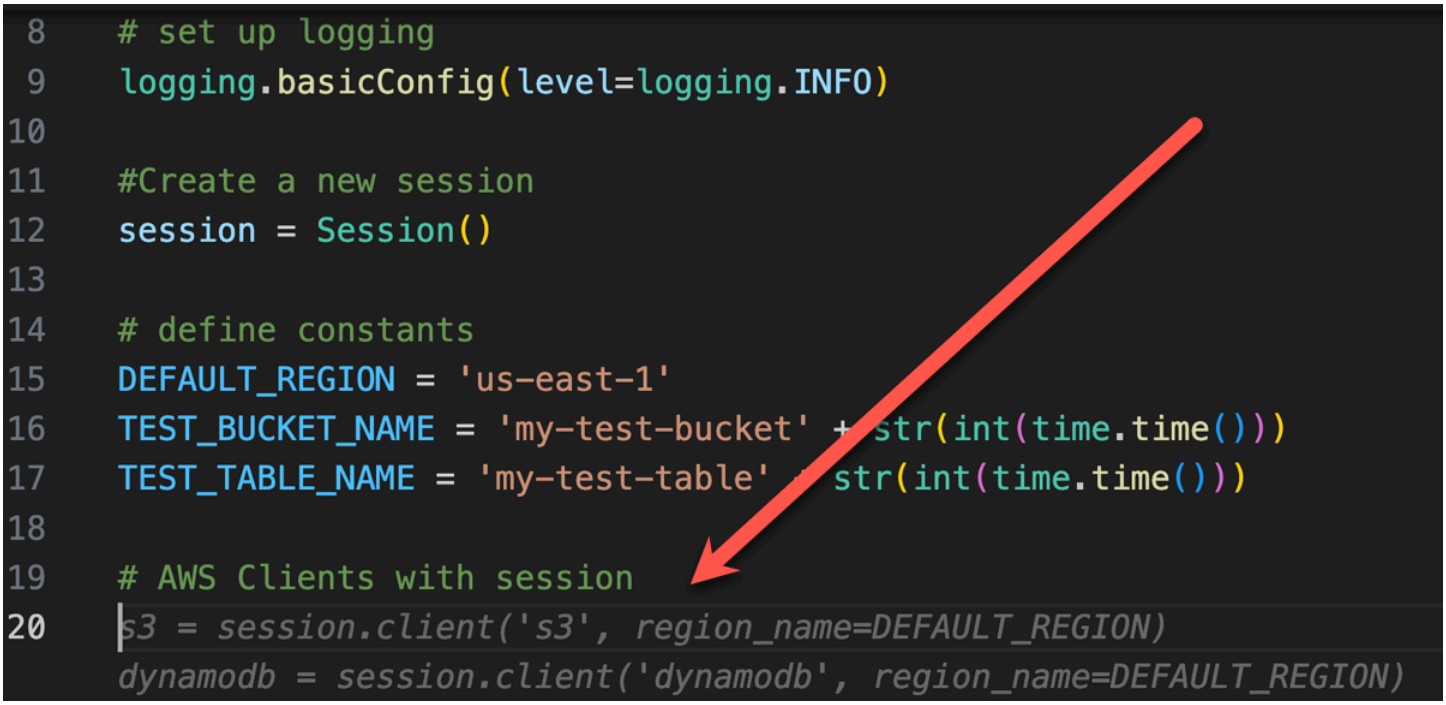
Aquí, el desarrollador se prepara para definir las constantes.

CodeWhisperer anticipa correctamente que la primera constante será `REGION` y que su valor seráus-east-1, que es el valor predeterminado.



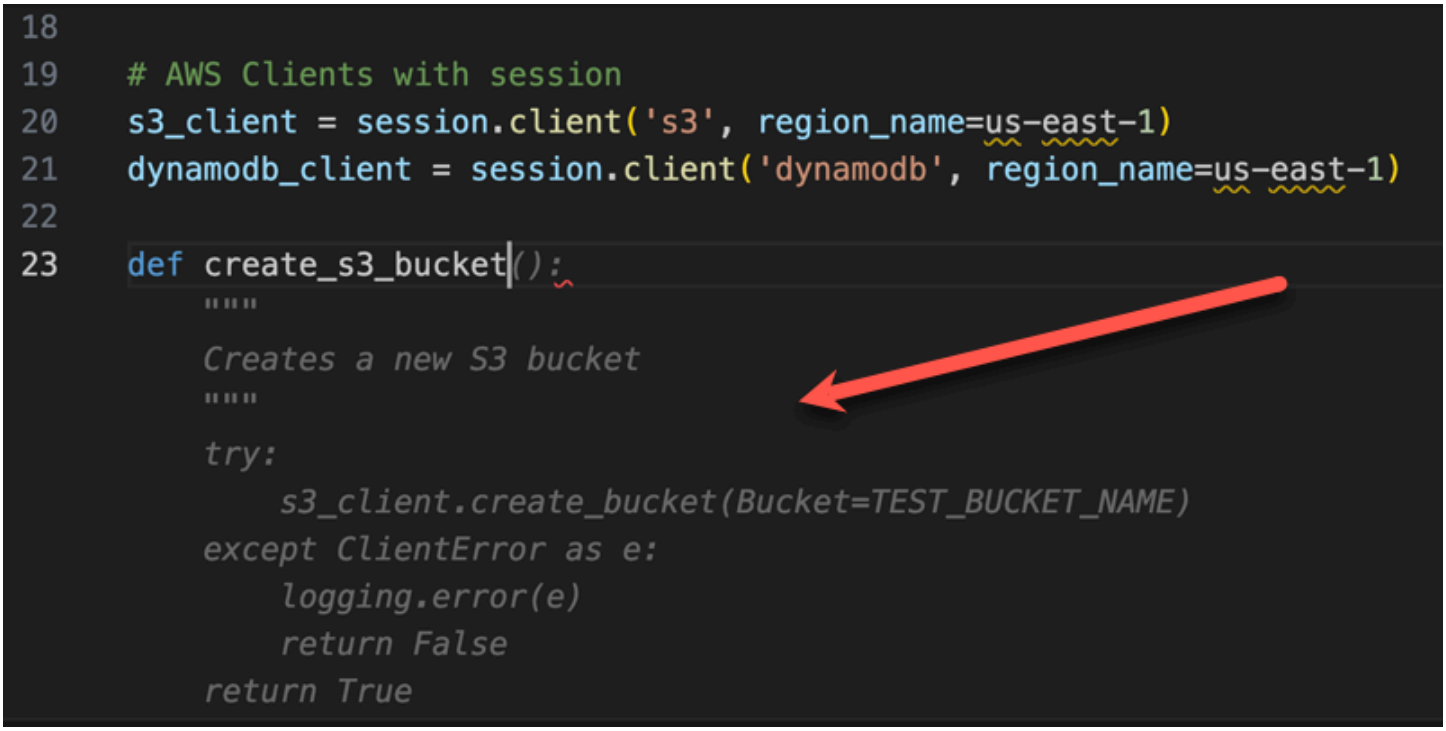
Aquí, el desarrollador se prepara para escribir código que abrirá sesiones entre el usuario y Amazon S3 y DynamoDB.

CodeWhisperer, familiarizado con AWS las API y los SDK, sugiere el formato correcto.



El desarrollador se ha limitado a escribir el nombre de la función que creará el bucket. Pero en función de eso (y del contexto), CodeWhisperer ofrece una función completa, con cláusulas de prueba/excepción.

Observación del uso de `TEST_BUCKET_NAME, which is a constant declared earlier in the same file.`



El desarrollador acaba de empezar a escribir el nombre de la función que creará una tabla de DynamoDB. Pero CodeWhisperer puedo decir a dónde va esto.

Observe que la sugerencia corresponde a la sesión de DynamoDB creada anteriormente e incluso la menciona en un comentario.

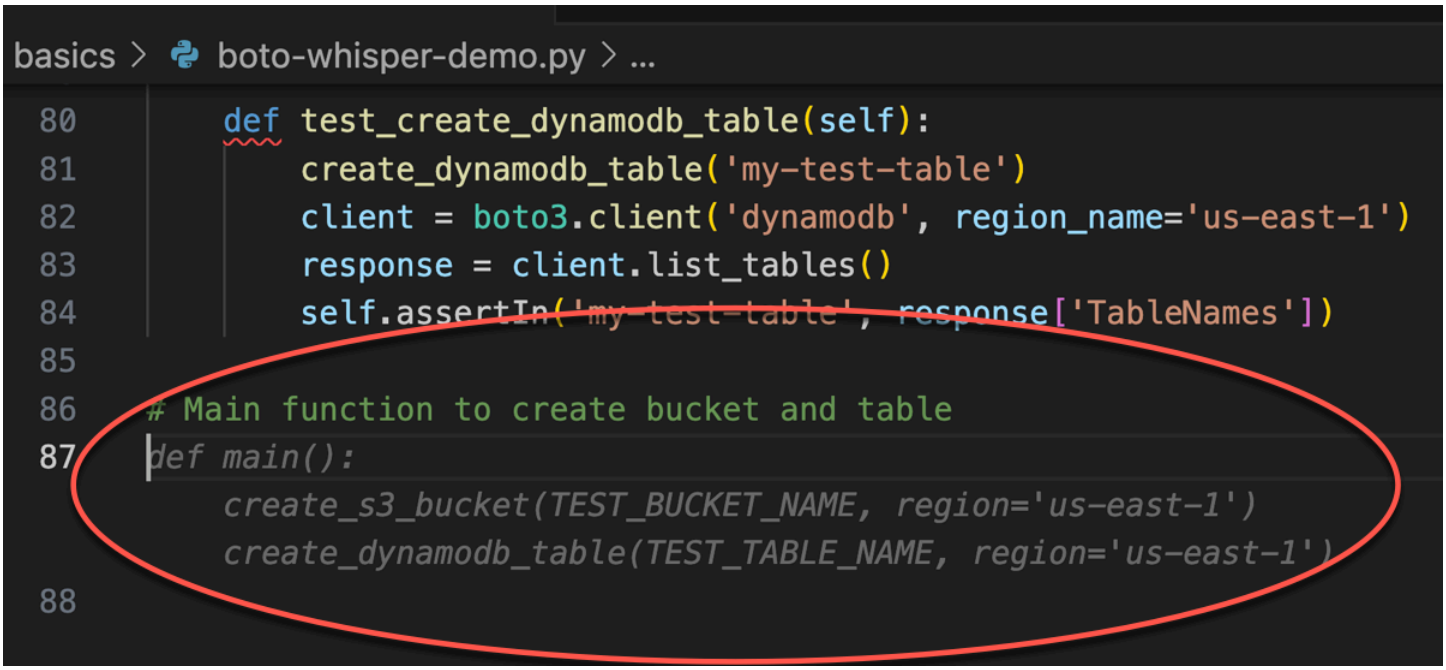
El desarrollador ha hecho poco más que escribir el nombre de la clase de prueba unitaria cuando se CodeWhisperer ofrece a completarla.

Tenga en cuenta las referencias integradas en las dos funciones creadas anteriormente en el mismo archivo.

El desarrollador acaba de empezar a escribir el nombre de la función que creará una tabla de DynamoDB. Pero CodeWhisperer puedo decir a dónde va esto.

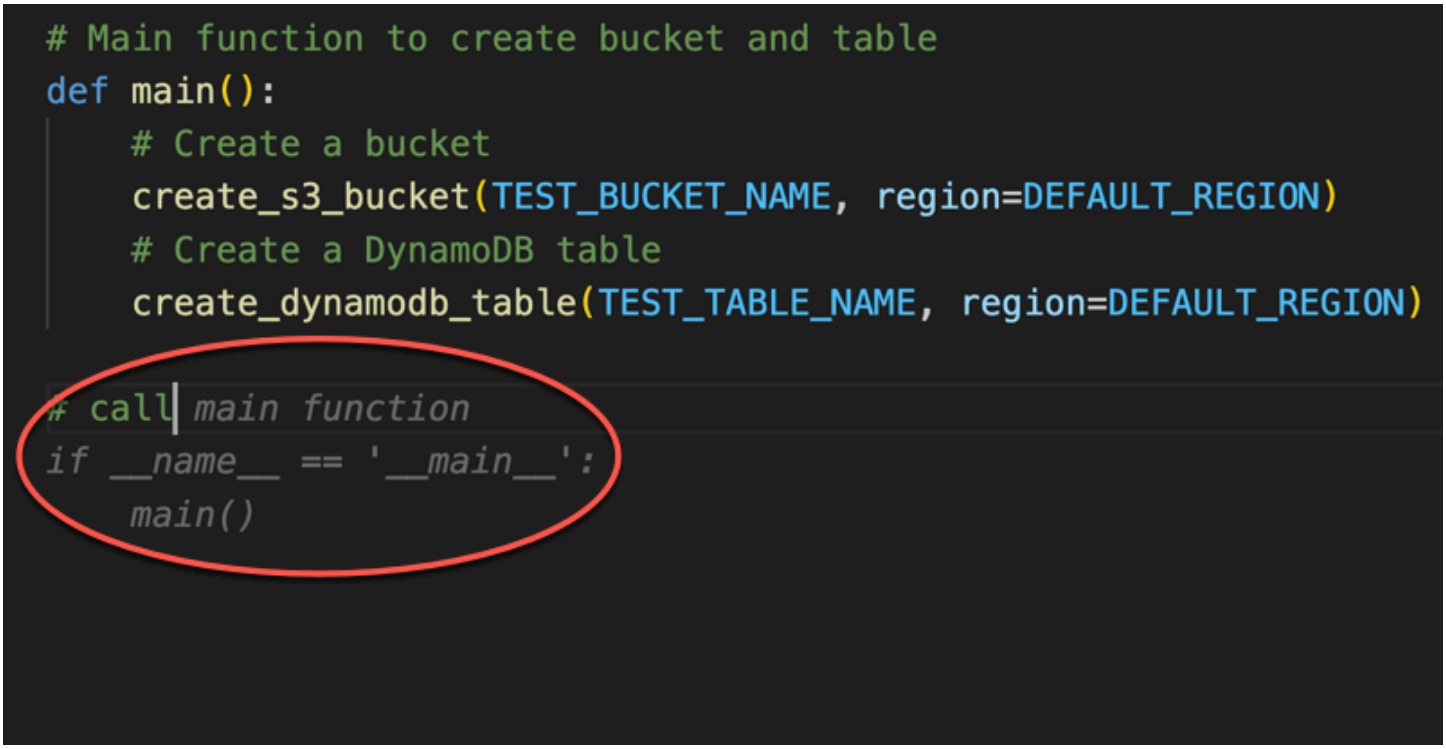
Observe que la sugerencia corresponde a la sesión de DynamoDB creada anteriormente e incluso la menciona en un comentario.

Basado solo en un comentario y el contexto, CodeWhisperer proporciona toda la función principal.

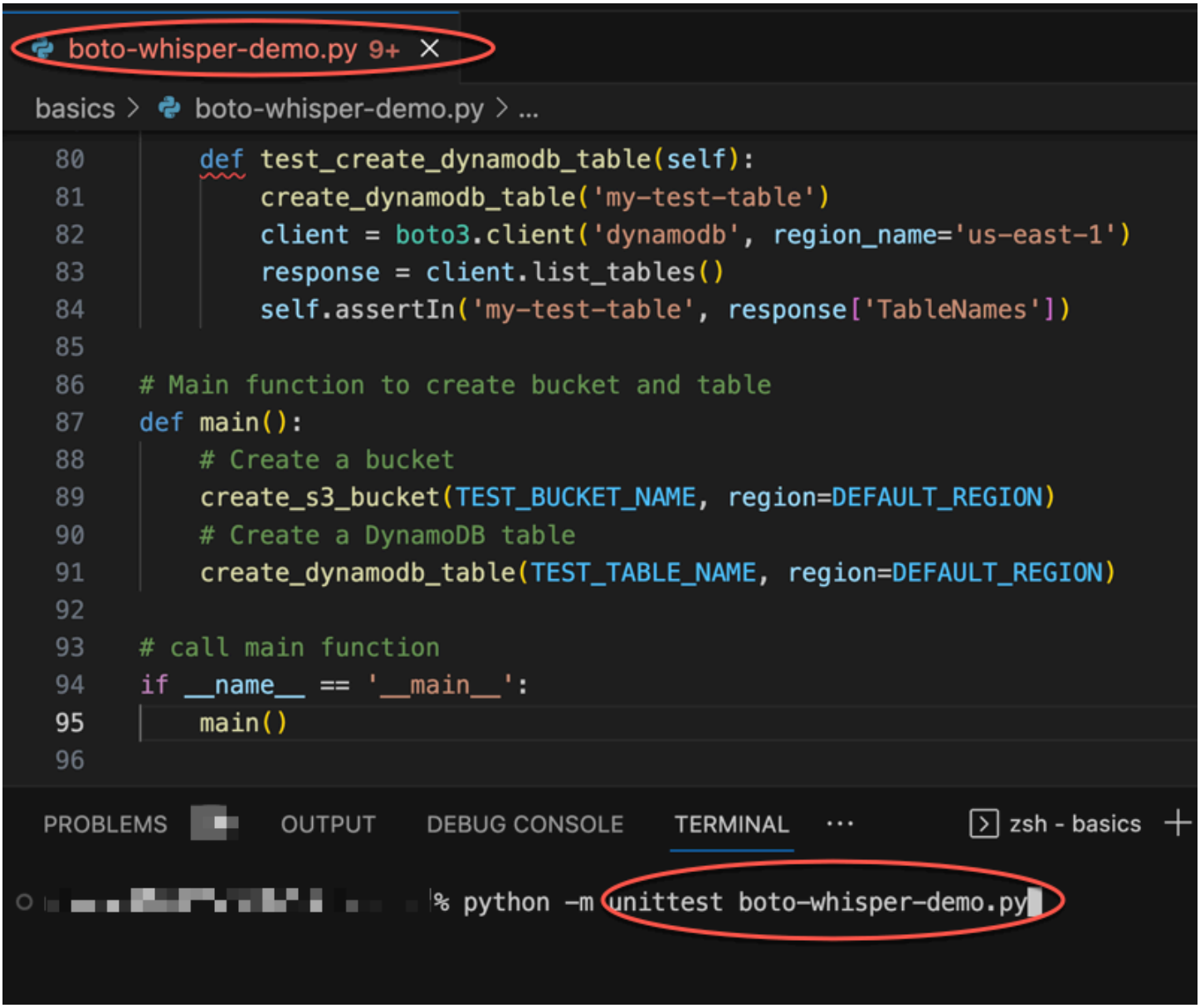


Lo único que queda es el guardia principal y CodeWhisperer lo sabe.

Basado únicamente en un comentario y en el contexto, CodeWhisperer cumple toda la función principal.



Por último, el desarrollador ejecuta la prueba unitaria desde el terminal del mismo IDE donde se realizó la codificación.


boto-whisper-demo.py 9+
basics > boto-whisper-demo.py > ...
80 def test_create_dynamodb_table(self):
81 create_dynamodb_table('my-test-table')
82 client = boto3.client('dynamodb', region_name='us-east-1')
83 response = client.list_tables()
84 self.assertIn('my-test-table', response['TableNames'])
85
86 # Main function to create bucket and table
87 def main():
88 # Create a bucket
89 create_s3_bucket(TEST_BUCKET_NAME, region=DEFAULT_REGION)
90 # Create a DynamoDB table
91 create_dynamodb_table(TEST_TABLE_NAME, region=DEFAULT_REGION)
92
93 # call main function
94 if __name__ == '__main__':
95 main()
96
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL ··· zsh - basics
% python -m unittest boto-whisper-demo.py

Configuración

En las siguientes secciones se describen los pasos que debe seguir antes de usarlo CodeWhisperer como desarrollador por primera vez.

Si es un administrador que está configurando CodeWhisperer Professional para su organización, consulteConfiguración de Amazon CodeWhisperer para administradores.

Antes de usarlo CodeWhisperer por primera vez, debe seguir los siguientes pasos:

1. Elija el IDE.
2. Instale o actualice el IDE (si corresponde).
3. Instale o actualice el AWS kit de herramientas (si corresponde).
4. Elija un método de autenticación.
5. Configure el ID de creador, el IAM Identity Center o las credenciales de IAM.

Elección del IDE

CodeWhisperer actúa como una mejora de ciertos entornos de desarrollo integrados (IDE). Puede utilizarlo en cualquiera de los siguientes servicios.

- Las SageMakerlibretas Amazon son un componente esencial del entorno de desarrollo interactivo de SageMaker Studio, ya que ofrecen un JupyterLab entorno gestionado para crear, compartir y colaborar en las libretas de Jupyter. Diseñados para respaldar los flujos de trabajo de machine learning en AWS, los cuadernos de Studio ofrecen funciones integradas de colaboración y control de versiones. Facilitan la integración con otros AWS servicios SageMaker y permiten a los usuarios crear, entrenar e implementar modelos directamente desde sus cuadernos. Además, las libretas SageMaker Studio escalan automáticamente los recursos subyacentes en función de los requisitos de la carga de trabajo, lo que garantiza una utilización eficiente de los recursos.
- JupyterLab es un IDE que permite trabajar con datos y código en una plataforma flexible de código abierto. Con JupyterLab él, puede crear y editar cuadernos de Jupyter, ejecutar código en varios lenguajes de programación y visualizar y manipular datos mediante una variedad de bibliotecas y herramientas. JupyterLab se utiliza ampliamente en la ciencia de datos, el aprendizaje automático y la investigación científica, y cuenta con el respaldo de una comunidad dinámica de colaboradores y usuarios.

- AWS Toolkit for Visual Studio Code es un complemento de código abierto para Visual Studio Code que facilita crear, depurar e implementar aplicaciones mediante Amazon Web Services. Con él AWS Toolkit for Visual Studio Code, podrá empezar más rápido y ser más productivo a la hora de crear aplicaciones con Visual Studio Code activado AWS. El kit de herramientas proporciona una experiencia integrada para desarrollar aplicaciones sin servidor, que incluye asistencia para empezar, recomendaciones de código basadas en ML, depuración gradual e implementación desde el IDE.
- AWS Toolkit for JetBrainsSe trata de un complemento de código abierto para los IDE JetBrains que facilita a los desarrolladores el desarrollo, la depuración y el despliegue de aplicaciones sin servidor que utilizan Amazon Web Services. Incluye funciones como la administración de credenciales y AWS la administración de regiones que simplifican la redacción de aplicaciones para Amazon Web Services.
- AWS Cloud9 es un IDE basado en la nube que le permite escribir, ejecutar y depurar el código con solo un navegador. Incluye un editor de código, un depurador y un terminal. AWS Cloud9 viene preempaquetado con herramientas esenciales para los lenguajes de programación populares JavaScript, incluidos Python y PHP.
- AWS Lambda es un servicio de computación controlado por eventos sin servidor que permite ejecutar código para virtualmente cualquier tipo de aplicación o servicio de backend, sin aprovisionar ni administrar servidores. Puede activar Lambda desde más de 200 AWS servicios y aplicaciones de software como servicio (SaaS) y pagar solo por lo que utilice.

Instalación o actualización del IDE

Para instalar VS Code por primera vez, use la página de descargas de VS Code.

Si ya tiene VS Code instalado, actualice a la versión más reciente de la siguiente manera:

- En MacOS, elija Código -> Buscar actualizaciones.
- En Windows y Linux, elija Ayuda -> Buscar actualizaciones.

Para instalarlo JetBrains por primera vez, utilice la página de JetBrains descargas.

Si ya lo ha JetBrains instalado, actualice a la última versión de la siguiente manera:

- En MacOS, en el menú desplegable principal del IDE, elija Buscar actualizaciones.
- En Windows y Linux, elija Ayuda -> Buscar actualizaciones.

Instalación del AWS kit de herramientas

Para usarlo CodeWhisperer con VS Code o JetBrains, primero debe descargar e instalar el AWS kit de herramientas.

Para obtener información sobre la instalación del AWS kit de herramientas para VS Code, consulte Configuración AWS del kit de herramientas para Visual Studio Code AWS en la guía del usuario del kit de herramientas para Visual Studio Code.

Para obtener información sobre cómo instalar el AWS kit de herramientas JetBrains, consulte Configuración del kit de herramientas JetBrains en la AWS guía del usuario del kit de herramientas para.AWS JetBrains

Elección del método de autenticación

Si planea usarlo CodeWhisperer con VS Code (a través de AWS Toolkit) o JetBrains (a través de AWS Toolkit), tendrá que autenticarse mediante AWS Builder ID o IAM Identity Center.

Si planea usarlo CodeWhisperer con Studio o SageMaker AWS Glue Studio AWS Cloud9 AWS Lambda JupyterLab, tendrá que autenticarse mediante IAM.

Para obtener información sobre la autenticación con CodeWhisperer, consulte. Autenticarse con un kit de CodeWhisperer herramientas AWS

Configuración del método de autenticación

El Builder ID (usado con AWS Toolkit y VS Code o JetBrains) solo requiere una dirección de correo electrónico. Para usarlo, ni siquiera necesitas una AWS cuenta.

El IAM Identity Center requiere que el administrador de la empresa lo configure.

Las credenciales de IAM se utilizan en su AWS cuenta para regular el acceso a varios AWS servicios y entre ellos.

Obtenga una Cuenta de AWS y las credenciales de usuario raíz

Para acceder AWS, debe registrarse para obtener un Cuenta de AWS.

Para inscribirse en un Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Configuración de Amazon CodeWhisperer para administradores

En esta sección se describen los procedimientos de configuración necesarios para que un desarrollador pueda utilizar CodeWhisperer Professional.

En este contexto, un desarrollador profesional es un desarrollador que trabaja para una empresa (empresa) que tiene una AWS cuenta.

Este es un resumen de los procedimientos descritos en esta página. Si es un AWS usuario habitual, es posible que ya haya completado uno o más de estos procedimientos en relación con otro AWS servicio.

- El usuario root viene integrado en su AWS cuenta.
- El usuario root crea el conjunto de permisos para el AWS Organizations administrador.
- El usuario raíz agrega ese conjunto de permisos al administrador de Organizaciones.
- El administrador de Organizaciones agrega usuarios.
- El administrador de Organizations autoriza al CodeWhisperer administrador a administrar CodeWhisperer.
- El CodeWhisperer administrador autoriza a los desarrolladores empresariales a utilizarla. CodeWhisperer

Para obtener más información sobre las diferentes personas que pueden utilizar, CodeWhisperer consulteTipos de usuarios para CodeWhisperer.

Configuración de CodeWhisperer Professional con AWS Organizations administración

El usuario raíz viene integrado con la cuenta de AWS

El usuario raíz es el usuario que viene con la cuenta. El usuario raíz tiene acceso a todos los servicios y configuraciones de la cuenta.

Como el usuario raíz es tan poderoso, se recomienda usarlo lo menos posible. Sin embargo, una función útil del usuario raíz es crear un usuario administrativo potente.

En este caso, utilizaremos al usuario raíz para crear el administrador de Organizaciones.

El usuario raíz crea al administrador de Organizaciones

Los conjuntos de permisos se guardan en el IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta Cuenta de AWS. Realice los siguientes pasos para crear un conjunto de permisos que conceda permisos administrativos.

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando Usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
2. Abra la consola del IAM Identity Center
3. Si es la primera vez que utiliza el IAM Identity Center, elija Habilitar. A continuación, elija Creación de organización de AWS . Si ha habilitado anteriormente el IAM Identity Center, puede omitir este paso.
4. En el panel de navegación del IAM Identity Center, en Permisos multicuenta, seleccione Conjuntos de permisos.
5. Elija Crear conjunto de permisos.
6. En la página Seleccionar el tipo de conjunto de permisos, mantenga la configuración predeterminada y elija Siguiente. La configuración predeterminada otorga acceso total a AWS los servicios y recursos mediante el conjunto de permisos AdministratorAccesspredefinido.

> **Note**
>
> El conjunto de AdministratorAccesspermisos predefinido usa la política AdministratorAccess AWS administrada.

7. En la página Especificar detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente. La configuración predeterminada limita la sesión a una hora.
8. En la página Revisar y crear, haga lo siguiente:
    1. Revise el tipo de conjunto de permisos y confirme que es AdministratorAccess.
    2. Revise la política AWS administrada y confirme que lo es AdministratorAccess.
    3. Seleccione Crear.

El usuario root asigna al administrador de la Organización permisos especiales relacionados con CodeWhisperer

En esta sección, agregará una política insertada al conjunto de permisos que acaba de crear. Esta política permitirá al administrador del Centro de Identidad de IAM crear y eliminar instancias de la CodeWhisperer aplicación.

1. En el IAM Identity Center, en Permisos multicuenta, elija Conjuntos de permisos.
2. Elija el conjunto de AdministratorAccesspermisos que creó en la sección anterior.
3. En Política insertada, elija Editar.
4. Elimine el código de la ventana de códigos y péguelo en:

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
  "Sid": "Statement1",
  "Effect": "Allow",
  "Action": [
   "sso:CreateManagedApplicationInstance",
   "sso:DeleteManagedApplicationInstance",
   "codewhisperer:CreateProfile",
   "codewhisperer:DeleteProfile"
```

```
  ],
  "Resource": [
   "*"
  ]
     }
 ]
}
```

5. Elija Save changes (Guardar cambios) en la parte inferior de la página.

El usuario raíz asigna el conjunto de permisos de administrador de Organizaciones a un usuario

En la última sección, creó el conjunto de AdministratorAccesspermisos. Ahora debe asignar ese conjunto de permisos a un usuario.

1. En la consola del IAM Identity Center, en la página Cuentas de AWS, aparece una lista de la organización en forma de árbol. Seleccione la casilla de verificación situada junto a la Cuenta de AWS a la que desea asignar el acceso administrativo. Si tiene varias cuentas en su organización, active la casilla de verificación situada junto a la cuenta de administración.
2. Seleccione Asignar usuarios o grupos.
3. Si es necesario, seleccione la pestaña Usuarios.
4. Elija Creación de usuarios. Se abrirá una nueva pestaña del navegador con la página de usuarios.
5. Elija Añadir usuario.
6. En la página Especificar los detalles del usuario, rellene los campos con información sobre el usuario que será el administrador de la cuenta. Un ejemplo de nombre de usuario podría ser *account_admin*.

   A continuación, elija Next.
7. En la página Agregar el usuario a los grupos, agregue este usuario a un grupo si quiere y, a continuación, elija Siguiente.
8. En la página Revisar y agregar usuario, compruebe la información que ha ingresado y seleccione Agregar usuario.
9. Si eligió utilizar una contraseña de un solo uso, una ventana emergente mostrará la contraseña de un solo uso.

Copie esta contraseña en una ubicación segura del equipo local.

Elija Close.

10. Regrese a la pestaña anterior del navegador con la opción Asignar usuarios y grupos a “***AWS-account-name***” en la parte superior de la página.
11. Elija el botón de actualización o actualice la pestaña del navegador. El usuario que acaba de crear debería aparecer en la lista.
12. Seleccione la casilla de verificación que hay junto al nombre del usuario que se convertirá en el administrador de la cuenta.
13. Elija Siguiente.
14. En la página Asignar conjuntos de permisos a «***AWS-account-name***», en Conjuntos de permisos, seleccione el AdministratorAccessconjunto de permisos.
15. Elija Siguiente.
16. En la página Revisar y enviar asignaciones a “***AWS-account-name***”, elija Enviar.

> **Important**
>
> El proceso de asignación de usuarios puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

17. Mientras aún se encuentre en el IAM Identity Center, en la barra de navegación de la izquierda, elija Panel.
18. En el resumen de configuración de la parte derecha de la página, copia la URL del portal de AWS acceso.

    El administrador de la cuenta y el administrador utilizarán esta URL cuando inicien sesión en el CodeWhisperer IAM Identity Center.

    El desarrollador CodeWhisperer profesional también la utilizará cuando se autentique a través de VS Code o. JetBrains En ese contexto, se denomina URL de inicio, como se explica en Primeros pasos CodeWhisperer en VS Code y JetBrains.

Configuración de CodeWhisperer Professional con IAM Identity Center

Delegación de la administración de IAM Identity Center a una cuenta que no sea de administración

Como práctica recomendada, no debe administrar el IAM Identity Center desde la cuenta de administración.

Por lo tanto, debe usar la administración delegada para designar una cuenta que no sea de administración para administrar el IAM Identity Center.

Si solo tiene una cuenta en su AWS organización, esa es la cuenta de administración. Debe crear cuentas adicionales para usarlas en la administración del IAM Identity Center y CodeWhisperer. Puede obtener información sobre las prácticas recomendadas para crear y mantener varias AWS cuentas en la Guía de referencia sobre la administración de AWS cuentas.

Tras elegir la cuenta que se convertirá en la cuenta de administración delegada, siga los pasos que se indican en Registro de una cuenta de miembro en la Guía del usuario de IAM Identity Center.

No es necesario que administre CodeWhisperer desde la misma cuenta que utilizó para administrar el Centro de Identidad de IAM.

La administración CodeWhisperer se lleva a cabo account-by-account dentro de su organización.

> **Warning**
>
> Por motivos de compatibilidad CodeWhisperer, no puede configurar el Centro de Identidad de IAM en una región de suscripción voluntaria.

Asignación de derechos de administración CodeWhisperer

> **Warning**
>
> En este procedimiento, actúa como administrador de Organizaciones y ha iniciado sesión en la cuenta de administrador del delegado. En función de cómo haya iniciado sesión en los procedimientos anteriores, es posible que tenga que cambiar de usuario, cuenta o rol antes de continuar.

El administrador de su CodeWhisperer perfil es un usuario especial con derecho a cambiar la configuración del CodeWhisperer perfil y a gestionar el acceso de usuarios y grupos o a los que pueden añadirlos CodeWhisperer.

Para ascender a un usuario a CodeWhisperer administrador, el administrador de la cuenta utiliza los siguientes procedimientos.

> **Note**
>
> En este procedimiento se presupone que ya tiene un usuario al que desea ascender a CodeWhisperer administrador. Si no lo tiene, cree uno mediante los procedimientos descritos en Asignación de usuarios y grupos a IAM Identity Center.

Configuración de las políticas para un CodeWhisperer administrador

1. Abra una pestaña del navegador con la URL del portal de acceso que le proporcionó el usuario raíz e inicie sesión como administrador de la cuenta.
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija Crear conjunto de permisos.
4. En Tipo de conjunto de permisos, seleccione Conjunto de permisos personalizado.
5. Elija Siguiente.
6. Amplíe la ventana de política insertada.
7. Borre los corchetes de la casilla.
8. Pegue el texto siguiente en la casilla:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",
                "sso-directory:GetUserPoolInfo",
                "sso-directory:DescribeDirectory",
                "sso:ListApplicationInstances",
                "sso-directory:ListMembersInGroup",
                "sso:CreateManagedApplicationInstance"
```

```
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "pricing:GetProducts"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:GetSharedSsoConfiguration",
                "sso:ListDirectoryAssociations",
                "sso:DescribeRegisteredRegions",
                "sso:GetSsoConfiguration",
                "sso:GetApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",
                "sso:GetProfile",
                "sso:GetSSOStatus"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "identitystore:ListUsers",
                "identitystore:ListGroups"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases",
                "kms:CreateGrant",
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey*",
                "kms:RetireGrant",
                "kms:DescribeKey"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codeguru-security:UpdateAccountConfiguration"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/codewhisperer.amazonaws.com/
AWSServiceRoleForCodeWhisperer"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codewhisperer:UpdateProfile",
                "codewhisperer:ListProfiles",
                "codewhisperer:TagResource",
                "codewhisperer:UnTagResource",
                "codewhisperer:ListTagsForResource",
                "codewhisperer:CreateProfile"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

> **Note**
>
> Si utiliza CodeWhisperer personalizaciones, el CodeWhisperer administrador necesitará permisos adicionales. Consulte Requisitos previos para CodeWhisperer las personalizaciones.

9. Elija Siguiente.
10. En Nombre del conjunto de permisos, escriba CodeWhisperer_administrator.
11. Elija Siguiente.
12. En la página Review and create (Revisar y crear), elija Create (Crear).

Adjuntar las políticas de un CodeWhisperer administrador a un usuario

> **Warning**
>
> En este procedimiento, actúa como administrador de Organizaciones y ha iniciado sesión en la cuenta de administrador delegado. En función de cómo haya iniciado sesión en los procedimientos anteriores, es posible que tenga que cambiar de usuario, cuenta o rol antes de continuar.

1. Abra una pestaña del navegador con la URL del portal de acceso que le proporcionó el usuario raíz e inicie sesión como administrador de la cuenta.
2. En la página principal de la consola, elija IAM Identity Center.
3. En el panel de navegación, en Permisos para varias cuentas, elijaCuentas de AWS.
4. En la página cuentas de AWS , aparece una lista de la organización en forma de árbol. Seleccione el nombre de la cuenta.
5. Seleccione Asignar usuarios o grupos.
6. En la página Asignar usuarios y grupos, seleccione la pestaña Usuarios.
7. Seleccione la casilla de verificación situada junto al nombre del usuario que se convertirá en administrador. CodeWhisperer
8. Elija Siguiente.
9. En la página Asignar conjuntos de permisos, seleccione la casilla de verificación situada junto a CodeWhisperer _administrator.
10. Elija Siguiente.
11. En la página Revisar y enviar asignaciones, elija Enviar.

Ahora el CodeWhisperer administrador tiene el acceso adecuado.

El siguiente paso es que el CodeWhisperer administrador autorice a un desarrollador profesional a utilizar CodeWhisperer Professional a través de un IDE.

API útiles

CodeWhisperer no tiene API públicas, en el sentido de que no se puede llamar a ninguna CodeWhisperer API mediante programación y ningún SDK las proporciona. Sin embargo, puede seguir haciendo referencia a las siguientes API en las políticas de IAM o en los conjuntos de permisos del IAM Identity Center.

- GenerateRecommendations - Obtiene sugerencias de código CodeWhisperer para AWS Cloud9 y CodeWhisperer para la consola Lambda.
- GenerateCompletions - Obtiene sugerencias de código CodeWhisperer para VS Code y JetBrains.
- StartCodeAnalysis - Inicia un análisis de seguridad en CodeWhisperer busca de VS Code y JetBrains.
- GetCodeAnalysis - Obtiene el estado de un análisis de seguridad en curso.
- ListCodeAnalysisFindings - Se llama después de una GetCodeAnalysis señal de finalización del trabajo. Devuelve la lista de todos los problemas de seguridad de los archivos analizados.
- CreateUploadUrl - Crea la URL para cargar los archivos de código que se escanearán en VS CodeWhisperer Code y JetBrains.
- CreateProfile - Se llama cuando el CodeWhisperer administrador crea una nueva CodeWhisperer aplicación.
- UpdateProfile - Se llama cuando el CodeWhisperer administrador actualiza CodeWhisperer los perfiles.
- ListProfiles - Se llama cuando el CodeWhisperer administrador muestra una lista CodeWhisperer de perfiles.
- TagResource - Se llama cuando el CodeWhisperer administrador añade o crea una etiqueta en el CodeWhisperer recurso.
- UnTagResource - Se llama cuando el CodeWhisperer administrador elimina una etiqueta del CodeWhisperer recurso.
- ListTagsForResource- Se llama al cargar la CodeWhisperer página de la consola para mostrar las etiquetas del CodeWhisperer recurso.
- StartDataCollection - Se utiliza para iniciar una recopilación de datos de la fuente de datos del cliente para utilizarlos en la creación de una personalización.
- GetDataCollectionStatus - Se utiliza para sondear el estado de un trabajo de recopilación de datos.

- CreateCustomization - Se utiliza para crear una personalización a partir de los datos recopilados de los clientes.
- DeleteCustomization - Se utiliza para eliminar una personalización de los datos de clientes recopilados.
- ListCustomizations - Se utiliza para enumerar las personalizaciones en función de su estado.
- UpdateCustomization - Activa o desactiva una personalización.
- ListCustomizationVersions - Muestra las versiones de una personalización.
- GetCustomization - Se utiliza para describir una personalización.

Administración de usuarios finales

Si CodeWhisperer ya se ha configurado para su organización

Puede configurarla CodeWhisperer en cualquier cuenta de miembro de su organización. Como práctica recomendada, no debería ser la cuenta de administración de Organizaciones. No tiene que ser la misma cuenta que utilice para la administración del IAM Identity Center.

Para eliminar CodeWhisperer de una cuenta, selecciona Eliminar en la parte superior de la página de CodeWhisperer configuración.

Añadir la CodeWhisperer aplicación al Centro de identidades de IAM

> **Warning**
>
> En este procedimiento, actúa como CodeWhisperer administrador. En el procedimiento anterior, actuó como AWS Organizations administrador. Si es necesario, cierre la sesión de la AWS consola y vuelva a iniciarla como CodeWhisperer administrador.

Para añadir la CodeWhisperer aplicación al Centro de identidades de IAM, siga estos pasos:

1. Abra una pestaña del navegador con la URL del portal de acceso e inicie sesión como CodeWhisperer administrador.
2. En la parte superior de la siguiente pantalla, elija el cubo naranja que representa la cuenta de AWS . Si la cuenta es la única de la organización de AWS , solo habrá una opción.
3. El nombre de la cuenta aparecerá en una barra, junto con el número de cuenta y la dirección de correo electrónico asociada.

Elija la barra.

4. La barra se expandirá para mostrar CodeWhisperer_administrator. También puede mostrar otros perfiles de acceso, en función de cómo esté configurada la cuenta.

   En la misma fila que Acceso de administrador, elija la Consola de administración.

5. En la página de inicio de la consola, selecciona Amazon CodeWhisperer.

6. En la página de la CodeWhisperer consola, selecciona Configurar CodeWhisperer.

   > **Note**
   >
   > Tras la configuración inicial, la página Configuración se convierte en la página Ajustes.

7. En la página Configuración, en Detalles, está seleccionada de forma predeterminada la opción Incluir sugerencias con referencias de código. Si procede, déjela seleccionada.

   Para obtener más información sobre esta opción, consulte Referencias de código.

> **Note**
>
> El período de espera de su sesión CodeWhisperer o de Amazon Q es el período de tiempo de espera que haya establecido en el Centro de identidad de IAM o el período de espera de su proveedor de identidad externo, lo que sea inferior.
> Para cambiar el tiempo de espera en el Centro de Identidad de IAM, en la página de configuración, seleccione la pestaña Autenticación. A continuación, en Configuración de la sesión, seleccione Configurar.

Asignación de usuarios y grupos a IAM Identity Center

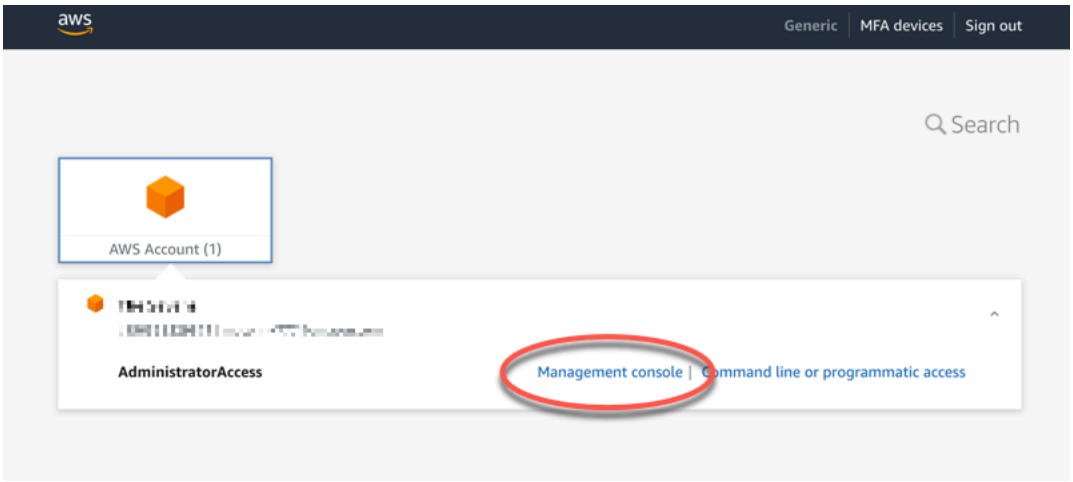
> **Warning**
>
> En este procedimiento, actúa como administrador de Organizaciones y ha iniciado sesión en la cuenta de administrador del delegado. En función de cómo haya iniciado sesión en los procedimientos anteriores, es posible que tenga que cambiar de usuario, cuenta o rol antes de continuar.

Los colaboradores de su organización se autentican mediante AWS IAM Identity Center. Para autorizar a los desarrolladores de su organización a trabajar con CodeWhisperer Professional, primero debe crearlos o importarlos como usuarios en el Centro de identidades de IAM.

1. Abra una pestaña del navegador con la URL del portal de acceso que le proporcionó el usuario raíz.
2. Inicie sesión en la cuenta que el usuario raíz creó para usted. O el usuario raíz le proporcionó una contraseña de un solo uso que ahora debe cambiar o recibió un correo electrónico con instrucciones para configurar la propia contraseña.
3. En la parte superior de la siguiente pantalla, elija el cubo naranja que representa la cuenta de AWS . Si la cuenta es la única de la organización de AWS , solo habrá una opción.
4. El nombre de la cuenta aparecerá en una barra, junto con el número de cuenta y la dirección de correo electrónico asociada.

   Elija la barra.
5. La barra se expandirá para mostrar Acceso de administrador. También puede mostrar otros perfiles de acceso, en función de cómo esté configurada la cuenta.

   En la misma fila que Acceso de administrador, elija la Consola de administración.



6. En la página de inicio de la consola, elija IAM Identity Center.
7. En el panel, elija Elegir el origen de identidad.

   El origen de identidad predeterminado es el directorio del Centro de identidades. Con el directorio del Centro de identidades, los usuarios y los grupos se administran completamente desde el IAM Identity Center.

8. (Opcional) Si desea elegir un origen de identidad diferente, en el menú desplegable Acciones, elija Cambiar origen de identidad.

   En la página Elegir el origen de la identidad, las otras dos opciones son:

   - Active Directory: seleccione esta opción si ya tiene los usuarios y grupos configurados en Active Directory.
   - Proveedor de identidad externo: seleccione esta opción si ya tiene los usuarios y grupos configurados en un sistema externo que no sea Active Directory.

El resto del proceso para agregar usuarios y grupos al IAM Identity Center está más allá del ámbito de esta guía. Para obtener información adicional sobre el IAM Identity Center y cómo configurarlo, consulte la Guía del usuario del IAM Identity Center de AWS. Asegúrese de configurar la creación o importación de al menos dos usuarios más: uno para el CodeWhisperer administrador y otro para el desarrollador profesional. Luego, vuelva a esta guía para Asignación de derechos de administración CodeWhisperer.

Autorizar a los desarrolladores profesionales a utilizar CodeWhisperer

> **Warning**
>
> En este procedimiento, usted actúa como CodeWhisperer administrador. Si es necesario, cierre la sesión de la AWS consola y vuelva a iniciarla como CodeWhisperer administrador.

Para autorizar a usuarios específicos a trabajar con CodeWhisperer ellos, complete los siguientes pasos:

1. En la CodeWhispererconsola, selecciona Configuración para abrir el menú Configuración.
2. Si lo desea, en la sección Detalles, seleccione Incluir sugerencias con referencias de código.

   Tras realizar esta selección, los desarrolladores individuales no podrán cambiarla en el IDE.
3. En la vista de usuarios, selecciona las personas que requieren autorización para su uso CodeWhisperer.

   Los usuarios que seleccione aparecerán en Usuarios y grupos seleccionados.

> **Note**
>
> Para poder elegir un usuario aquí, el administrador del IAM Identity Center debe agregarlo primero en el IAM Identity Center. Para obtener más información, consulte Asignación de usuarios y grupos a IAM Identity Center.

> **Note**
>
> Incluso si el mismo usuario actúa como CodeWhisperer desarrollador en dos cuentas diferentes de la misma organización, a tu organización solo se le facturará por ese usuario una vez por ciclo de facturación.

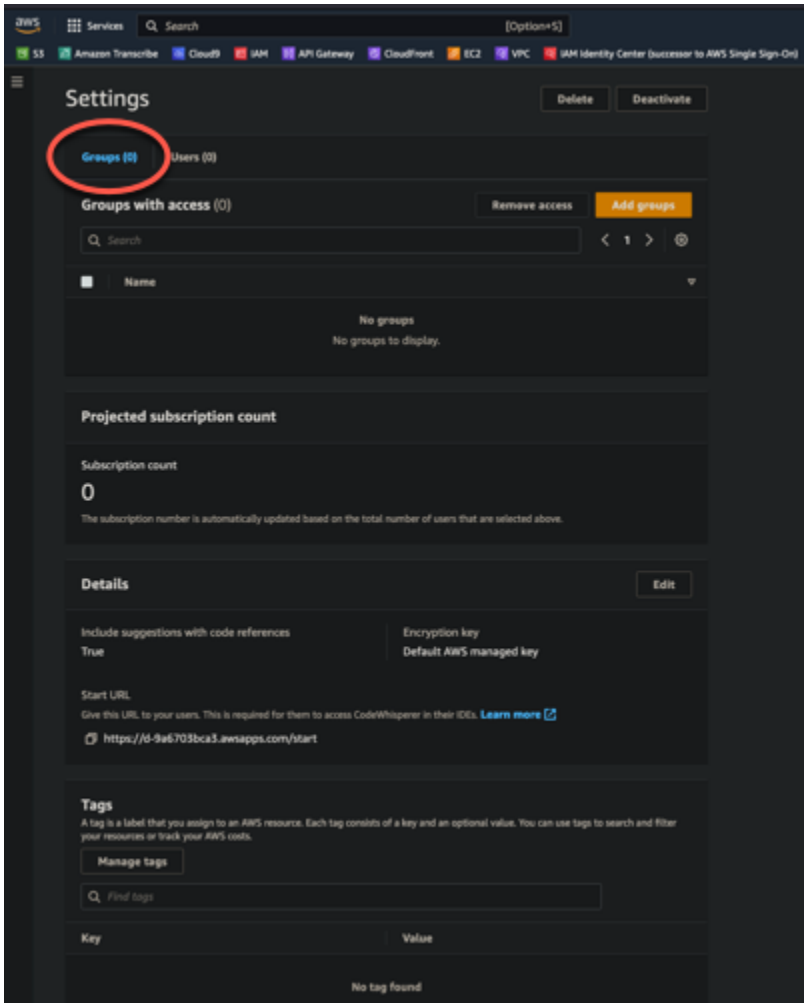
4. Elija Set up (Configurar) CodeWhisperer.

Para autorizar el uso de grupos de usuarios CodeWhisperer, complete los siguientes pasos:

1. En la CodeWhispererconsola, selecciona Configuración para abrir el menú Configuración.
2. En la esquina superior derecha de la ventana de la consola, confirme que la región se establece en Este de EE. UU. (Norte de Virginia).

   Este paso es necesario, independientemente de la región que haya utilizado al añadir la CodeWhisperer aplicación al Centro de Identidad de IAM o de la región que haya utilizado el administrador de la cuenta al añadir o crear usuarios y grupos en el Centro de Identidad de IAM.
3. Si lo desea, en la sección Detalles, seleccione Incluir sugerencias con referencias de código.

   Tras realizar esta selección, los desarrolladores individuales no podrán cambiarla en el IDE.
4. En la pestaña Grupos, elija Agregar grupos para abrir la vista Agregar grupos.



5. En la vista Añadir grupos, seleccione los grupos que requieren autorización para su uso. CodeWhisperer
6. Elija Agregar grupos para autorizar el CodeWhisperer acceso a los grupos seleccionados.

El CodeWhisperer administrador elimina el acceso a CodeWhisperer

Puede eliminar el CodeWhisperer acceso de los usuarios y grupos de usuarios individuales.

Para eliminar el CodeWhisperer acceso de los usuarios individuales, siga estos pasos:

1. En la CodeWhisperer consola, selecciona Configuración para abrir el menú Configuración.
2. En la pestaña Usuarios, elija Eliminar acceso.
3. Cuando se te pida, selecciona Eliminar para confirmar que deseas eliminar el CodeWhisperer acceso del usuario.

Para eliminar el CodeWhisperer acceso de un grupo de usuarios, siga estos pasos:

1. En la CodeWhisperer consola, selecciona Configuración para abrir el menú Configuración.
2. En la pestaña Grupos, elija Eliminar acceso.
3. Cuando se le solicite, elija Eliminar para confirmar que desea eliminar el CodeWhisperer acceso al grupo de usuarios.

CodeWhisperer perfiles

Un CodeWhisperer perfil es la configuración de la CodeWhisperer aplicación de su empresa. Incluye las decisiones que tomas sobre la cuenta (por ejemplo, si deseas incluir sugerencias con referencias de código), así como los usuarios y grupos a los que das acceso CodeWhisperer.

El concepto del CodeWhisperer perfil puede ser importante si vas a cambiar los permisos de IAM relacionados CodeWhisperer con ellos. En esa situación, el perfil es el recurso sobre el que se CodeWhisperer actúa.

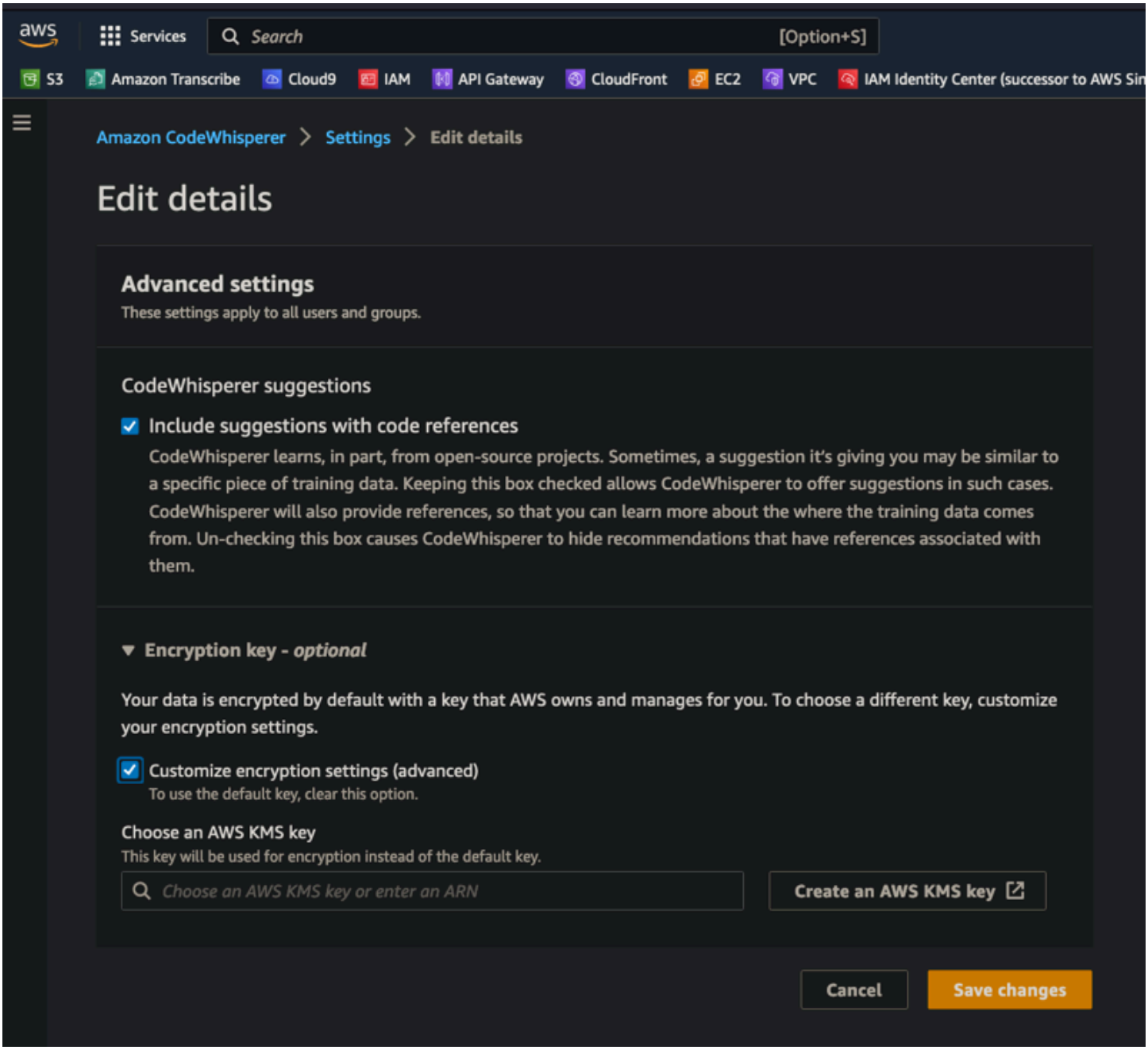
Para obtener más información, consulte Control del acceso a los recursos de AWS mediante políticas en la Guía del usuario de IAM.

Elección de la clave de cifrado

De forma predeterminada, los datos recopilados con este fin Análisis de seguridad se almacenan mediante Amazon S3 y Amazon DynamoDB. CodeWhisperer Estos datos solo se almacenan durante el tiempo que sea necesario para ese fin. Los datos se cifran mediante las capacidades de data-at-rest cifrado de Amazon S3 y Amazon DynamoDB, con una clave propiedad de Builder ID.

Sin embargo, los administradores de CodeWhisperer Professional tienen la opción de cifrar los datos de su empresa (que se utilizan con fines de análisis de seguridad) con la. CodeWhisperer AWS Key Management Service

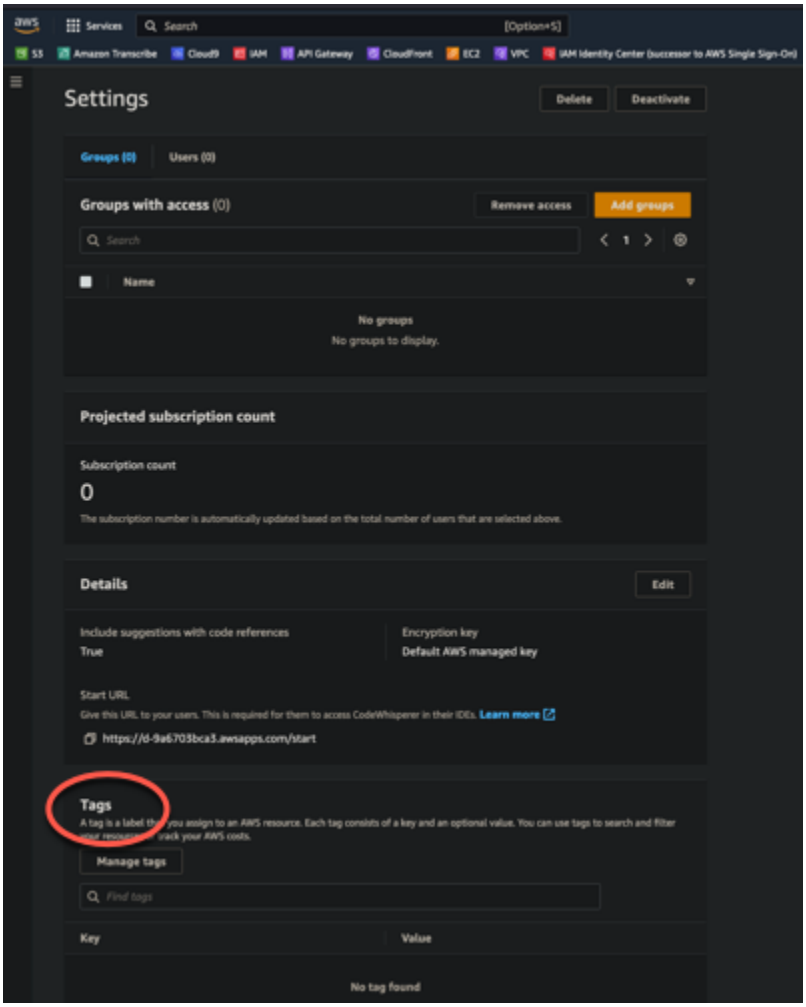
Para obtener más información AWS KMS, consulte AWS Key Management Service los conceptos de la Guía para AWS Key Management Service desarrolladores.



Descripción de las etiquetas CodeWhisperer de perfil

Es posible que desees añadir etiquetas al CodeWhisperer perfil para hacer un seguimiento más sencillo de los gastos o para conceder permisos de IAM.

Para obtener más información, consulte Cómo etiquetar AWS los recursos en la Guía del usuario sobre cómo etiquetar AWS los recursos.



Activación y desactivación de la aplicación CodeWhisperer

Puede controlar el acceso CodeWhisperer de su organización activando o desactivando la aplicación.

Para deshabilitar la CodeWhisperer aplicación, complete los siguientes pasos:

1. En la CodeWhisperer consola, selecciona Configuración para abrir el menú Configuración.
2. Selecciona Desactivar CodeWhisperer.
3. Cuando se le solicite, elija Desactivar en el IAM Identity Center para abrir el IAM Identity Center.
4. En Aplicaciones configuradas del Centro de identidades de IAM, elija CodeWhisperer.
5. En la lista de acciones, seleccione Desactivar la aplicación que desee deshabilitar CodeWhisperer.

Para volver a activar la CodeWhisperer aplicación, complete los siguientes pasos:

1. En la CodeWhisperer consola, selecciona Configuración para abrir el menú Configuración.

   > **Note**
   >
   > La consola muestra una alerta que indica que se CodeWhisperer ha desactivado.

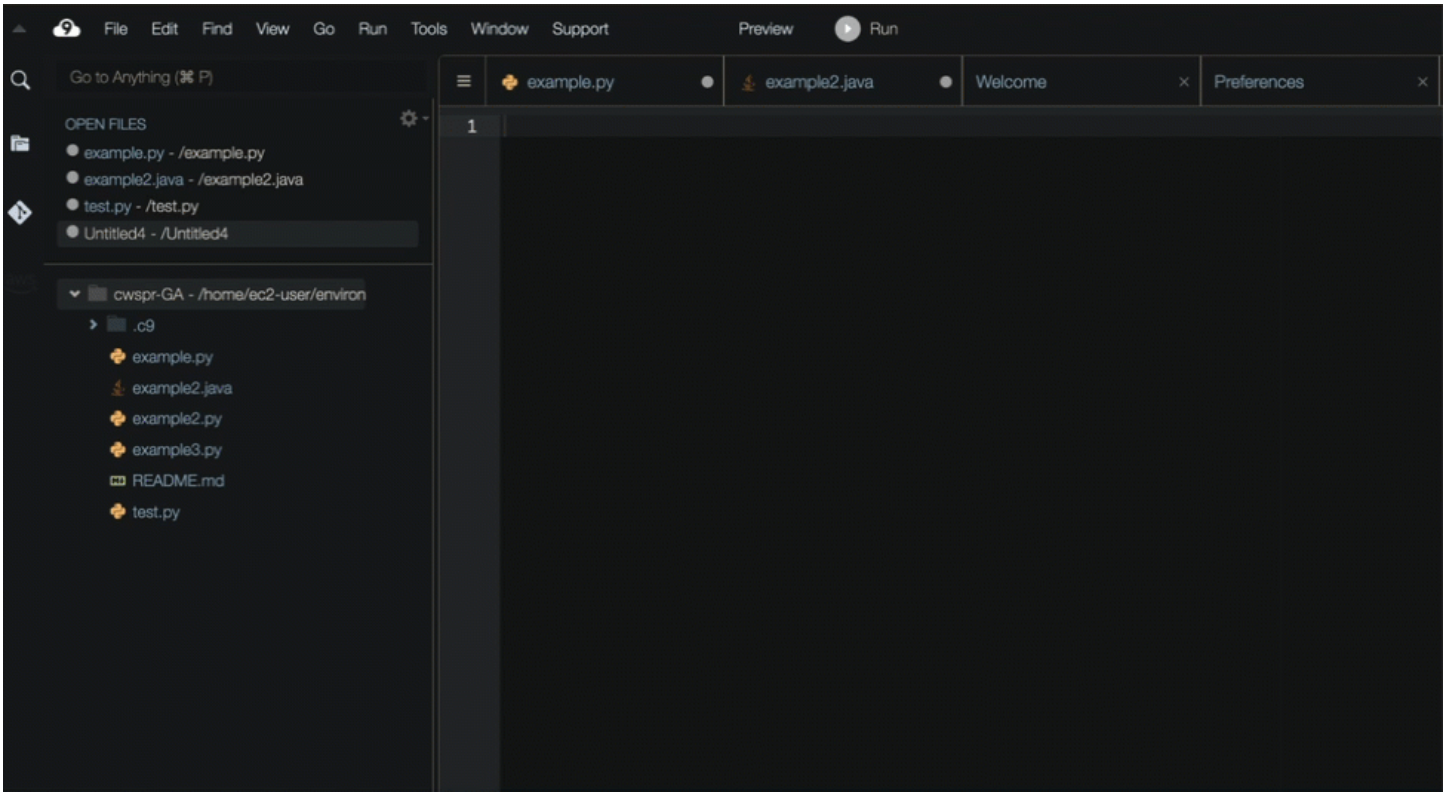
2. Cuando se le solicite, elija IAM Identity Center.
3. En la pestaña Grupos, elija Agregar acceso.

Si está realizando la transición a Amazon Q Developer, el siguiente paso es suscribirse a Amazon Q Developer Pro.

Introducción

> **Note**
>
> La forma más rápida de empezar CodeWhisperer es utilizar CodeWhisperer para desarrolladores individuales con VS Code o JetBrains.
> Si ya has iniciado sesión en la AWS consola, también puedes empezar a utilizarla rápidamente CodeWhisperer con AWS Cloud9.

A continuación AWS Cloud9, se muestra un ejemplo de cómo CodeWhisperer trabajar de forma integrada, completar comentarios, completar una sola línea, line-by-line realizar recomendaciones y completar funciones.



En las siguientes secciones se describe cómo configurarlo CodeWhisperer para su uso con cada uno de los cuatro IDE posibles: AWS Toolkit for JetBrains AWS Toolkit for Visual Studio Code,, Lambda y. AWS Cloud9

Con Lambda y AWS Cloud9, la configuración simplemente implica la activación CodeWhisperer dentro del IDE.

Si utiliza CodeWhisperer VS Code o CodeWhisperer Professional en nombre JetBrains de su organización. En ese caso, los administradores de la organización deben completar pasos adicionales antes de que pueda empezar a programar. Para obtener más información, consulte Configuración de Amazon CodeWhisperer para administradores.

Si lo usa CodeWhisperer, en su propio nombre, con VS Code o JetBrains, entonces, usa CodeWhisperer Individual. En ese caso, puede ir directamente a Primeros pasos CodeWhisperer en VS Code y JetBrains.

Temas

- CodeWhisperer para línea de comandos
- Primeros pasos CodeWhisperer en VS Code y JetBrains
- Uso CodeWhisperer con Visual Studio
- Uso CodeWhisperer con Amazon SageMaker Studio
- Uso CodeWhisperer con JupyterLab
- Introducción a CodeWhisperer Amazon EMR Studio
- Uso CodeWhisperer con AWS Glue Studio
- Uso de Amazon CodeWhisperer con AWS Lambda
- Uso CodeWhisperer con AWS Cloud9
- Uso CodeWhisperer con otros servicios

CodeWhisperer para línea de comandos

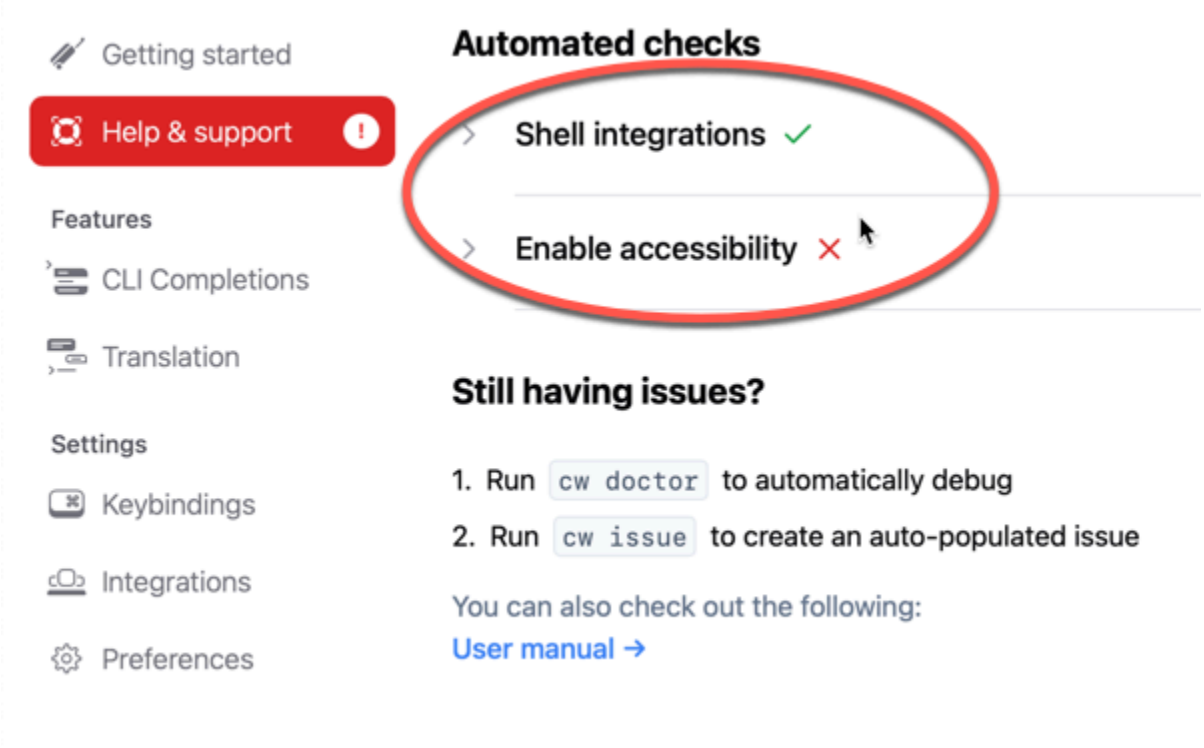
Temas

- Instalación CodeWhisperer para línea de comandos
- Finalizaciones de CLI
- Traducción de lenguaje natural a bash
- Depuración para la línea CodeWhisperer de comandos
- Añada sus propias especificaciones de finalización a CodeWhisperer

Instalación CodeWhisperer para línea de comandos

Para realizar la instalación CodeWhisperer desde la línea de comandos, siga los pasos que se indican a continuación.

1. Descargar CodeWhisperer para línea de comandos (solo macOS)
2. Autentícate con Builder ID para usuarios CodeWhisperer individuales o con IAM Identity Center para usuarios CodeWhisperer profesionales mediante la URL de inicio que te proporcionó el administrador de tu cuenta.
3. Siga las instrucciones para instalar las integraciones de intérprete de comandos y conceder permisos de accesibilidad de macOS.



Entornos de línea de comandos compatibles

CodeWhisperer ya que la línea de comandos se integra con los siguientes entornos:

- Sistemas operativos: macOS
- Intérpretes de comandos: bash, ash, fish
- Emuladores de terminal: iTerm2, terminal de macOS, Hyper, Alacritty, Kitty, WezTerm
- IDE: terminal de VS Code, terminales de Jetbrains (excepto Flota)
- CLI: más de 500 de las CLI más populares, como git, aws, docker, npm, yarn

Verificación de la descarga

Tras realizar la descarga CodeWhisperer para la línea de comandos, puede comprobar su firma de código de la siguiente manera:

```
codesign -v /Applications/CodeWhisperer.app
```

Si no hay ningún resultado, la firma en código de la aplicación es válida y no se ha manipulado desde que se firmó.

Para obtener información más detallada sobre la firma de la aplicación, ejecute:

```
codesign -dv --verbose=4 /Applications/CodeWhisperer.app
```

Para obtener más información sobre la utilidad de codiseño de macOS, consulte la Code Signing Guide en el sitio web para desarrolladores de Apple.

Desinstalar CodeWhisperer para la línea de comandos

CodeWhisperer Para realizar la desinstalación desde la línea de comandos, complete los siguientes pasos.

1. Abra una ventana de terminal.
2. Ejecute el siguiente comando:

   ```
   cw uninstall
   ```

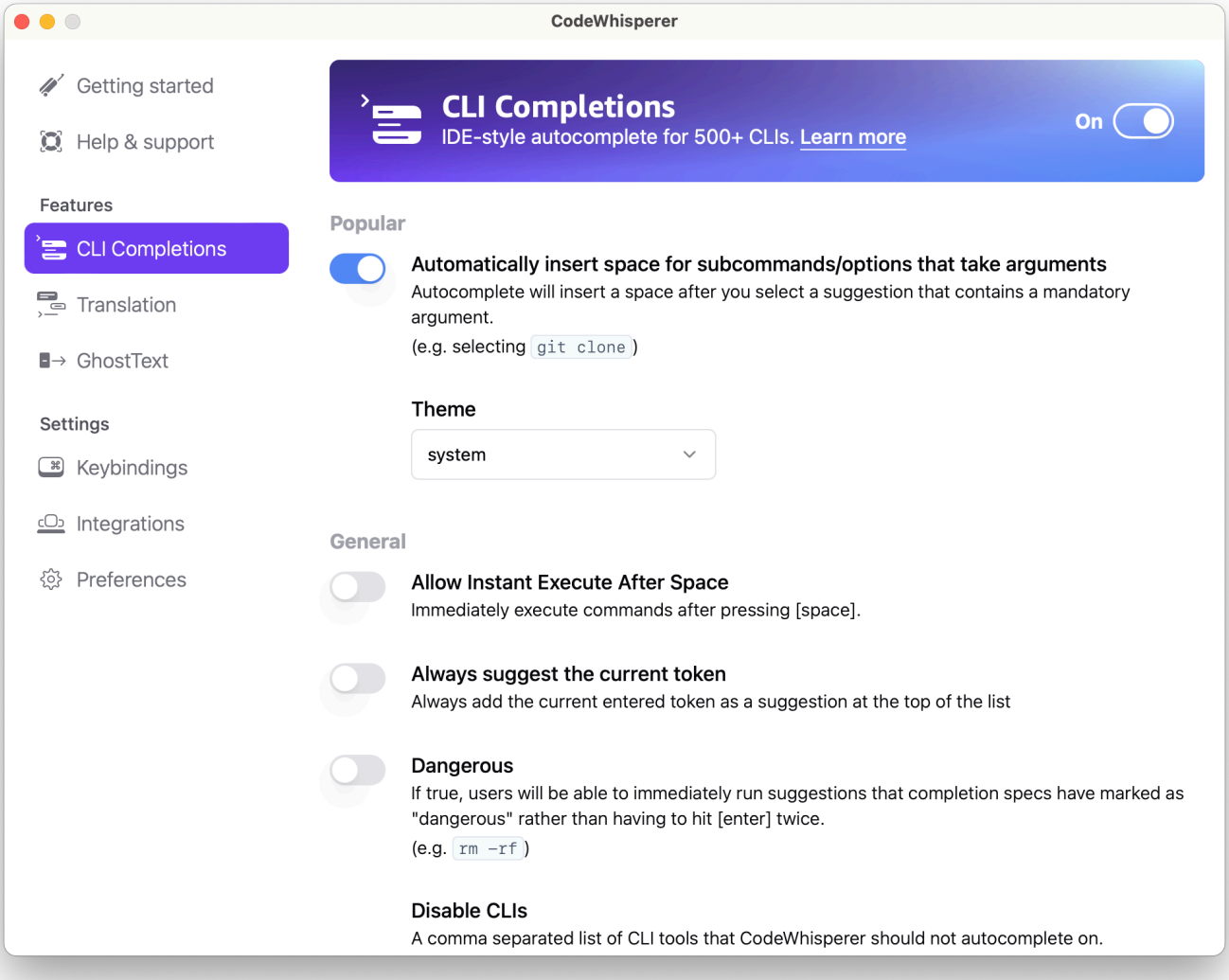
Finalizaciones de CLI

CodeWhisperer para la línea de comandos agrega terminaciones al estilo IDE para cientos de CLI populares como`git`,`npm`, `docker` y. `aws` Empieza a escribir y CodeWhisperer aparecerán subcomandos, opciones y argumentos contextualmente relevantes.

Configuraciones populares

Es posible que la configuración predeterminada proporcionada CodeWhisperer por la línea de comandos no sea adecuada y que interrumpa su flujo de trabajo actual. Puede personalizar la configuración en cualquier momento ejecutando `cw` para abrir el panel de configuración. Estas son algunas configuraciones populares de

- enlaces de teclado. Cambiar la combinación de teclas de `tab` a “Insertar un prefijo común o navegar” puede hacer que las terminaciones de CLI se parezcan más a las terminaciones de intérprete de comandos tradicionales, mientras que “Insertar un prefijo común o insertar” se parecerá más a un IDE
- Tema. Ya sabe lo que es esto. Elija al favorito.
- Ejecución instantánea después del espacio. Muchos desarrolladores suelen escribir un carácter de espacio justo antes de ejecutarlo. Activa esta configuración para evitar CodeWhisperer bloquearte
- Finalización del primer token. Habilitación de esta configuración para completar las CLI en sí, no solo los subcomandos, las opciones y los argumentos



Traducción de lenguaje natural a bash

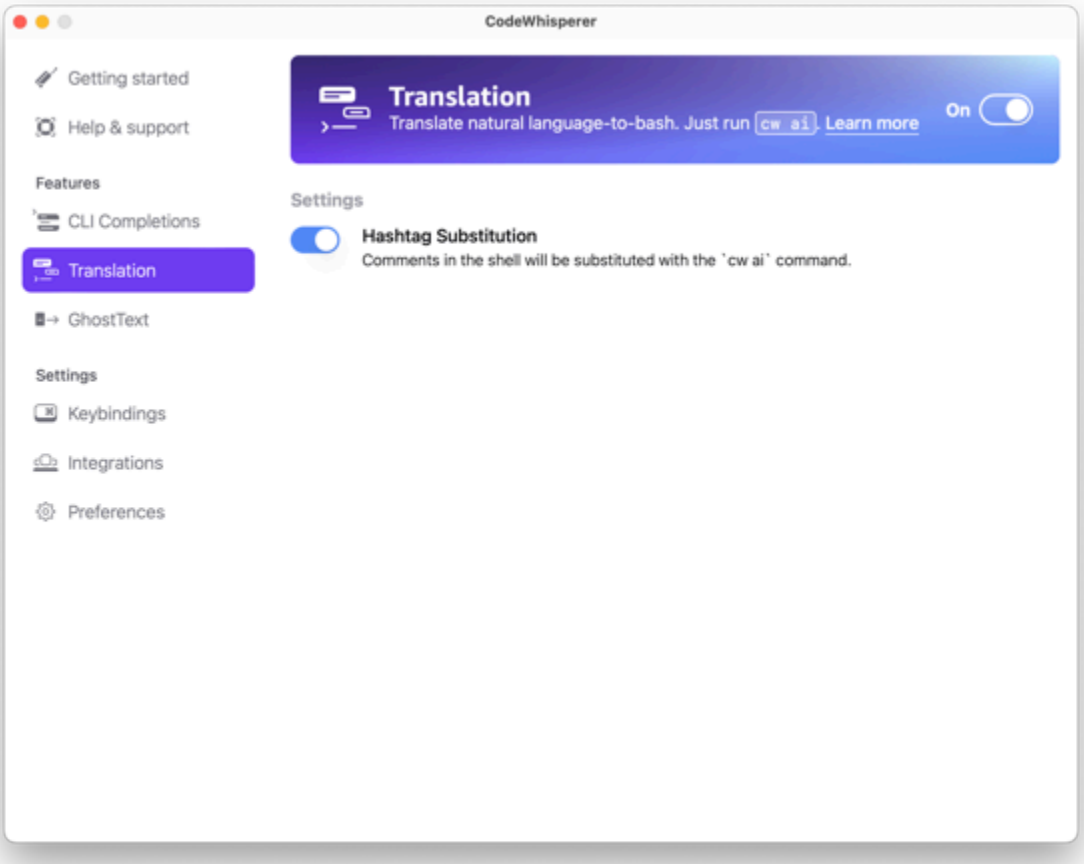
El `cw ai` comando le permite escribir una instrucción en lenguaje natural, como «copiar todos los archivos de mi directorio actual a Amazon S3». CodeWhisperer a continuación, la traducirá a un fragmento de código shell que se puede ejecutar al instante. El comando `cw ai` es útil en aquellas situaciones comunes en las que es fácil olvidar la sintaxis correcta de bash. Algunos ejemplos son invertir una confirmación de `git`, encontrar cadenas dentro de archivos con `grep` o comprimir archivos con `tar`.

Para comenzar, ejecute cualquiera de las acciones siguientes

- `cw ai` *`prompt`*

- `# prompt`

Para dejar de usar la función # de invocación CodeWhisperer, ve a Configuración -> Translate y desactiva la sustitución por hashtag.



Depuración para la línea CodeWhisperer de comandos

Si tiene problemas con la línea CodeWhisperer de comandos, ejecute`cw doctor`.

`cw doctor` identifica y corrige problemas comunes. La mayoría de las veces, no necesitará hacer nada más.

Resultado previsto

```
$ cw doctor

# Everything looks good!

CodeWhisperer still not working? Run cw issue to let us know!
```

Si el resultado no tiene el mismo aspecto que el anterior, siga las instrucciones para resolver el problema. Si sigue sin funcionar, ejecute `cw issue` para informar del error.

Añada sus propias especificaciones de finalización a CodeWhisperer

En esta sección se explica cómo crear las especificaciones propias de acabado y contribuir a ellas.

Una especificación de finalización es un esquema declarativo que especifica los subcomandos, las opciones y los argumentos de una herramienta CLI. CodeWhisperer for command line utiliza estos esquemas para generar sugerencias.

Para editar una especificación existente o aportar la suya propia, consulte https://fig.io/docs.

Primeros pasos CodeWhisperer en VS Code y JetBrains

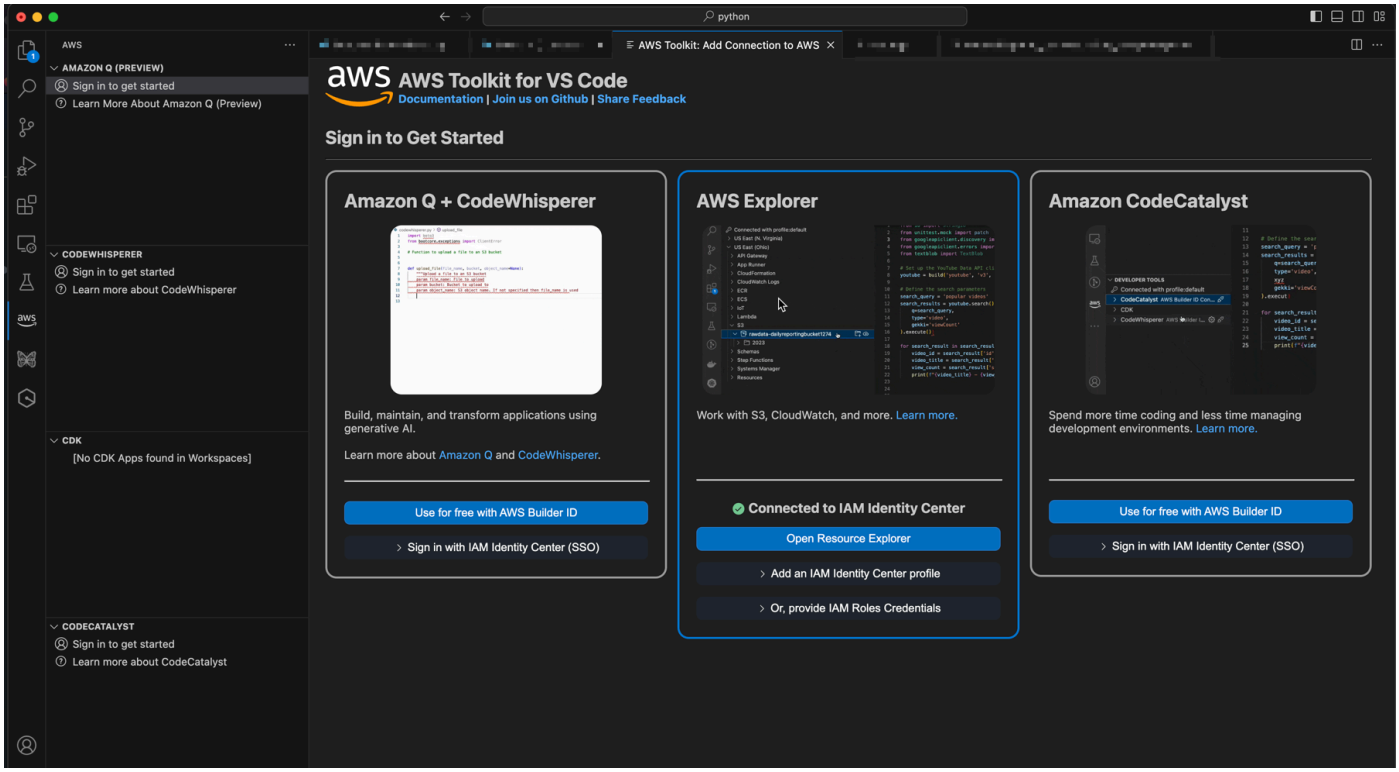
> **Important**
>
> Antes de continuar, asegúrese de estar utilizando la última versión de su IDE y del AWS kit de herramientas.

> **Note**
>
> AWS recomienda que, antes de usarla CodeWhisperer, deshabilite cualquier otra extensión que proporcione la funcionalidad de completar código.

VS Code

1. Desde el AWS Toolkit for VS Code, en AWS el panel de CodeWhispererabajo, selecciona Iniciar sesión para empezar.

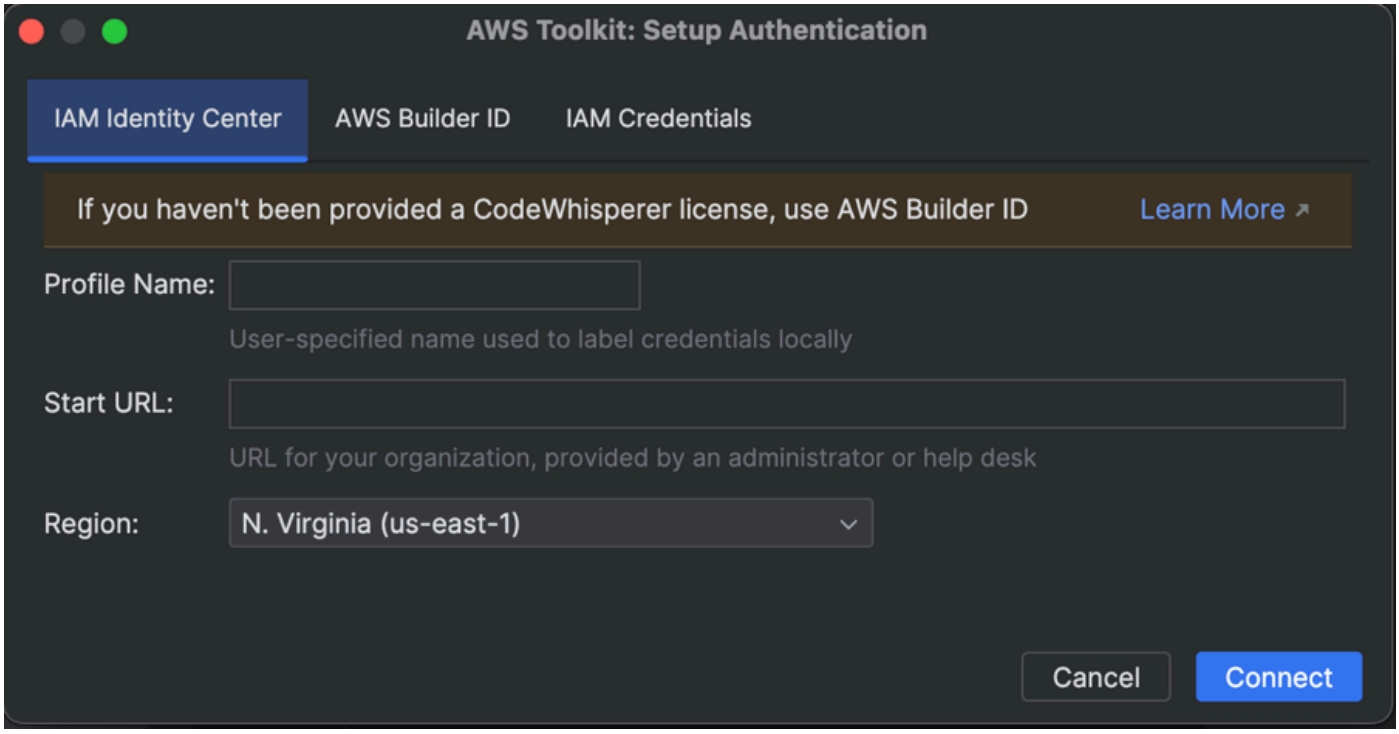
   Se abrirá la pestaña kit de herramientas de AWS : Agregar conexión a AWS.
2. Selecciona el panel de CodeWhisperer autenticación de Amazon Q +.
3. Seleccione el método de autenticación adecuado e inicie sesión.



JetBrains

1. Desde AWS Toolkit for JetBrains, selecciona la CodeWhisperer pestaña Amazon Q +.
2. En CodeWhisperer, selecciona Iniciar sesión para empezar.

   Se abrirá el modal kit de herramientas de AWS : Configurar autenticación.
3. Seleccione el método de autenticación adecuado e inicie sesión.



Autenticarse con un kit de CodeWhisperer herramientas AWS

Para usarlo CodeWhisperer con AWS Toolkit for Visual Studio Code o con el AWS kit de herramientas JetBrains, debe establecer una conexión autenticada con AWS (pero no necesita una cuenta). AWS En esta página se describe cada método de autenticación con el AWS kit de herramientas y su relación con cada uno de ellos. CodeWhisperer

AWS IAM Identity Center

El IAM Identity Center amplía las capacidades de IAM para proporcionar un lugar central que agrupa la administración de los usuarios y su acceso a las AWS cuentas y las aplicaciones en la nube. Los usuarios del IAM Identity Center los administra un administrador empresarial de TI o de la nube o el administrador del proveedor de identidades de la empresa, como Okta, Ping o Azure.

Cuando lo utilices CodeWhisperer, debes autenticarte con el Centro de Identidad de IAM si eres un desarrollador de nivel profesional. Es decir, trabajas CodeWhisperer como empleado de una organización que tiene una AWS cuenta y que paga una licencia profesional. CodeWhisperer Para poder autenticarse mediante el IAM Identity Center, el administrador debe agregarle como usuario. A continuación, el administrador le proporcionará la URL de inicio que necesita para iniciar sesión en el IAM Identity Center.

En el nivel profesional, puedes utilizarla CodeWhisperer para darte sugerencias que se ajusten a las bibliotecas internas de tu equipo con personalizaciones.

Obtención de más información sobre el IAM Identity Center

ID de creador

AWS Builder ID es un perfil personal para constructores. Lo representa como persona, fuera del ámbito de la empresa o escuela. Puedes registrarte en AWS Builder ID con tu nombre y correo electrónico.

Al usarlo CodeWhisperer, debes autenticarte con Builder ID si eres un desarrollador individual. Es decir, está trabajando en un proyecto personal o si su organización no se autentica para AWS utilizar el IAM Identity Center.

Si ha adquirido la herramienta de forma independiente de su equipo u organización, utilizará CodeWhisperer Individual y la utilizará ID de creador de AWS para iniciar sesión.

Obtención de información sobre el ID de creador

AWS Identity and Access Management

AWS Identity and Access Management es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos. Con IAM, puede administrar el acceso AWS creando políticas y adjuntándolas a las identidades (usuarios, grupos de usuarios o roles) o recursos de IAM. AWS Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director utiliza una entidad de IAM (usuario o rol) para realizar una solicitud. CodeWhisperer, cuando se usa con AWS Toolkit, no admite la autenticación con IAM. Sin embargo, se requieren credenciales de IAM para utilizarlas CodeWhisperer con AWS Cloud9Lambda o.

Obtención de más información sobre IAM

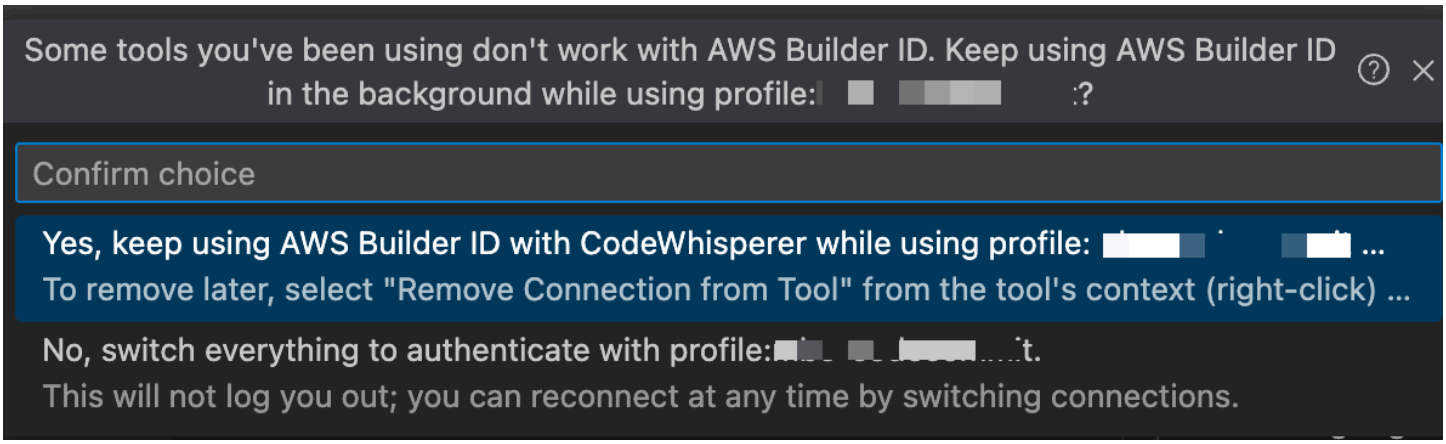
Cambio entre métodos de autenticación

Aunque CodeWhisperer no admite la autenticación con IAM, puede utilizar IAM para acceder a otros AWS servicios desde el mismo IDE. Sin embargo, en esos casos, su acceso CodeWhisperer seguirá gestionándose a través del IAM Identity Center o del Builder ID.

Por ejemplo, supongamos que lo está utilizando CodeWhisperer en su JetBrains IDE y está autenticado con el Builder ID. A continuación, decide cambiar de tarea, pero sin salir JetBrains.

Ahora quiere invocar una función Lambda en AWS su cuenta. Sin embargo, el acceso a Lambda requiere credenciales de IAM. Por lo tanto, debe cambiar los perfiles internos JetBrains, de su perfil de Builder ID a otro perfil que se autentique con sus credenciales de IAM.

En esos casos, el IDE presenta una alerta que le recuerda que está cambiando a un servicio con un método de autenticación diferente. También tendrá la opción de permanecer conectado CodeWhisperer (mediante Builder ID o IAM Identity Center) y, al mismo tiempo, utilizar otro servicio al que esté conectado mediante IAM.



Uso CodeWhisperer con Visual Studio

La integración de CodeWhisperer Visual Studio está en versión preliminar y está sujeta a cambios.

En esta página se describe cómo configurar y empezar a utilizar Visual CodeWhisperer Studio.

> **Note**
>
> Los lenguajes CodeWhisperer compatibles con Visual Studio son: C, C++ y C#.

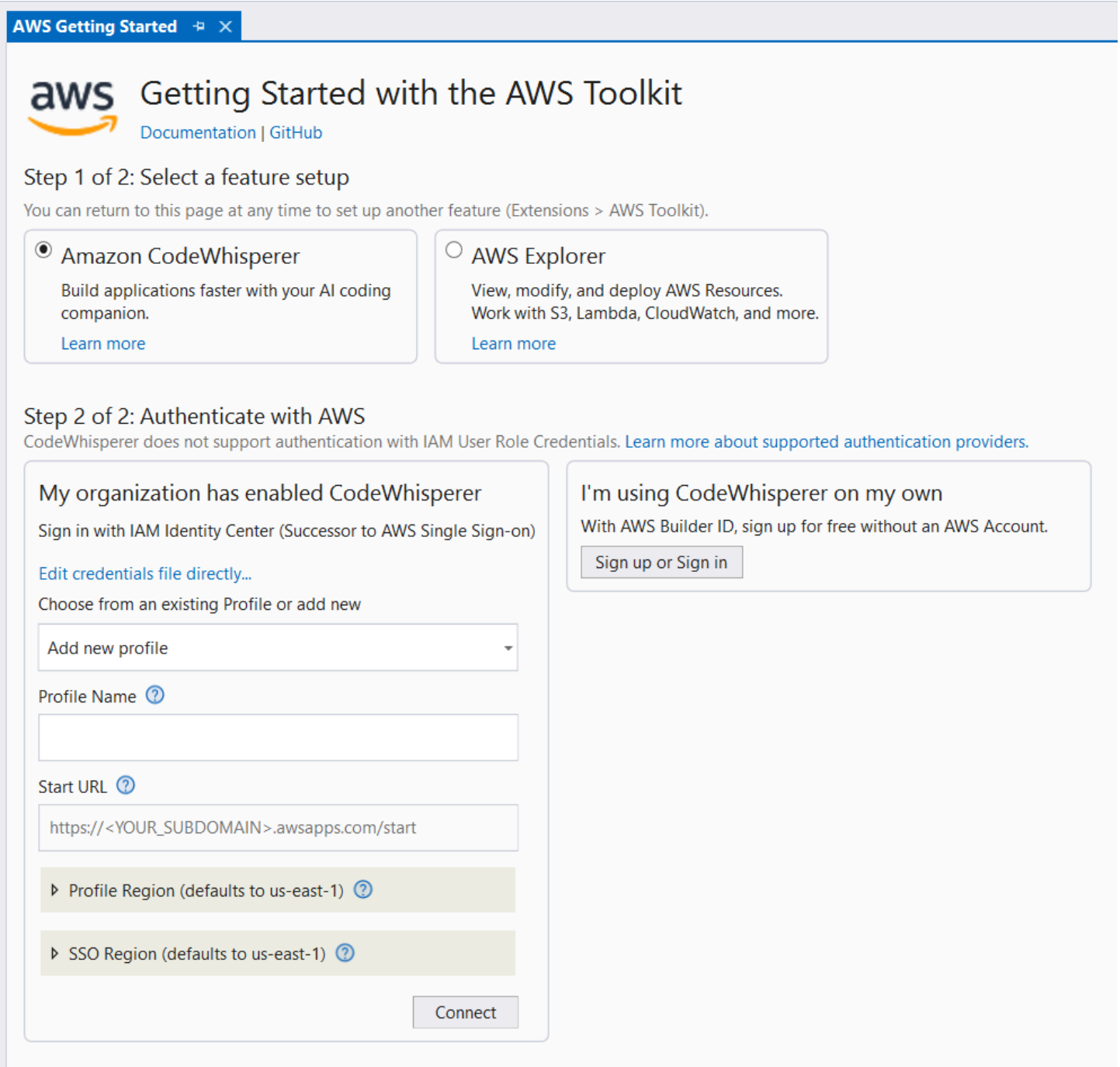
> **Note**
>
> El AWS kit de herramientas proporciona CodeWhisperer funcionalidad a través de un programa independiente denominado servidor de idiomas. Al abrir una solución en Visual Studio, el kit de herramientas descarga y actualiza el servidor de lenguajes en segundo

plano. A continuación, el kit de herramientas inicia el servidor de lenguajes como un proceso independiente del de Visual Studio. El servidor de lenguajes se ejecuta con el mismo nivel de privilegios que Visual Studio y se cierra automáticamente al cerrar Visual Studio.

1. Instale Visual Studio 2022.
2. Instale la versión más reciente del kit de herramientas de AWS para Visual Studio 2022.
3. En la página de introducción del kit de herramientas, seleccione. CodeWhisperer

   Puede volver a la página de Introducción en cualquier momento con Extensiones -> kit de herramientas de AWS -> Introducción.
4. Autenticate con el Centro de Identidad de IAM (para CodeWhisperer profesionales) o ID de creador de AWS (para CodeWhisperer usuarios individuales).

   Úselo CodeWhisperer de forma gratuita en el nivel individual autenticándose con. ID de creador de AWS Como alternativa, utilice el nivel profesional si la empresa tiene una licencia mediante autenticación con el IAM Identity Center.



Uso CodeWhisperer con Amazon SageMaker Studio

En esta página se describe cómo configurar y activar Amazon CodeWhisperer para Amazon SageMaker Studio. Una vez activado, CodeWhisperer puedes hacer recomendaciones de código automáticamente a medida que escribes tu código.

> **Note**
>
> Python es el único lenguaje de programación CodeWhisperer compatible con SageMaker Studio.

1. Configura los SageMaker requisitos previos de Amazon.

   Los requisitos previos para su uso SageMaker incluyen la creación de una AWS cuenta y la creación de un usuario administrativo.

   Para obtener más información, consulta Cómo configurar los SageMaker requisitos previos de Amazon en la Guía del SageMaker usuario de Amazon.
2. Configura un SageMaker dominio de Amazon.

   Para utilizar Amazon SageMaker Studio, debe completar el proceso de incorporación de SageMaker dominios de Amazon mediante la SageMaker consola o la AWS CLI. Para obtener más información, consulta Cómo incorporarse a un SageMaker dominio de Amazon en la Guía del SageMaker usuario de Amazon.
3. Añada los permisos CodeWhisperer relacionados a su función SageMaker de ejecución.

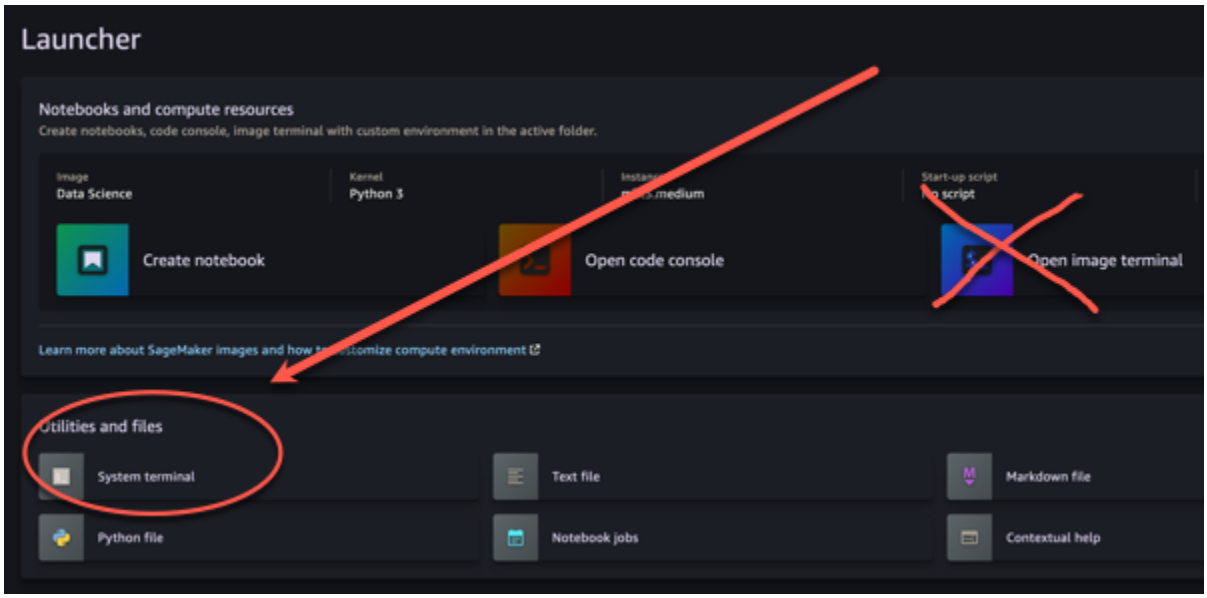
   Cree una política de IAM que contenga la siguiente instrucción. A continuación, asocie esa política al rol de ejecución (IAM) o al conjunto de permisos (IAM Identity Center) asociado al perfil de usuario.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "CodeWhispererPermissions",
         "Effect": "Allow",
         "Action": ["codewhisperer:GenerateRecommendations"],
         "Resource": "*"
       }
     ]
   }
   ```

   Para obtener información, consulte Creación de políticas de IAM y Agregar y eliminar permisos de identidad de IAM en la Guía del usuario de IAM.

4. Habilita la CodeWhisperer extensión en tu dominio de SageMaker Studio.

   Abra la pestaña del lanzador. A continuación, en el terminal del sistema (no en el terminal de imagen) de SageMaker Studio, ejecuta los siguientes comandos.




```
conda activate studio
pip install amazon-codewhisperer-jupyterlab-ext~=1.0
jupyter server extension enable amazon_codewhisperer_jupyterlab_ext
conda deactivate
restart-jupyter-server
```

   Para obtener más información sobre este paso y los siguientes, consulta Utilizar Amazon SageMaker Studio Launcher en la Guía para SageMaker desarrolladores de Amazon.

5. Abra un bloc de notas nuevo.

> **Note**
>
> Las terminaciones de código CodeWhisperer solo aparecen en las celdas de código. No aparecen en las celdas de marcado.

Ahora deberías estar preparado para programar con él CodeWhisperer en SageMaker Studio. (Puede que tenga que actualizar primero el navegador).

Para obtener atajos de teclado, consulte Acciones del usuario.

Uso CodeWhisperer con JupyterLab

En esta página se describe cómo configurar y activar Amazon CodeWhisperer para JupyterLab. Una vez activado, CodeWhisperer puede hacer recomendaciones de código automáticamente a medida que escribe su código.

> **Note**
>
> Python es el único lenguaje de programación que lo CodeWhisperer admite JupyterLab.

JupyterLab Instalándose solo

Instálelo JupyterLaben su ordenador o, si ya lo ha JupyterLab instalado, compruebe su versión ejecutando el siguiente comando.

```
pip show jupyterlab
```

Tenga en cuenta la versión en la respuesta y siga las instrucciones de uso correspondientes en una de las siguientes secciones.

Instalación mediante Pip para la versión >= 4.0 de Jupyter Lab

Puede instalar y habilitar la CodeWhisperer extensión para JupyterLab 4 con los siguientes comandos.

```
# JupyterLab 4
pip install amazon-codewhisperer-jupyterlab-ext
sudo systemctl restart jupyter-server
```

Después de ejecutar el código anterior, actualiza tu navegador. Deberías poder usarlo CodeWhisperer.

Si tienes un problema con los permisos, ejecuta:

```
aws sts get-caller-identity
```

Esto devolverá el nombre de la identidad cuyo uso requiere permiso CodeWhisperer. Si lo está utilizando SageMaker, será el rol de SageMaker ejecución.

Añada los permisos adecuados a la función y vuelva a actualizar el navegador.

Instalación mediante Pip para la versión >= 3.6 y < 4.0 de Jupyter Lab

Puede instalar y habilitar la CodeWhisperer extensión para JupyterLab 3 con los siguientes comandos.

```
# JupyterLab 3
pip install amazon-codewhisperer-jupyterlab-ext~=1.0
jupyter server extension enable amazon_codewhisperer_jupyterlab_ext
sudo systemctl restart jupyter-server
```

Después de ejecutar el código anterior, actualiza tu navegador. Deberías poder usarlo CodeWhisperer.

Si tienes un problema con los permisos, ejecuta:

```
aws sts get-caller-identity
```

Esto devolverá el nombre de la identidad cuyo uso requiere permiso CodeWhisperer. Si lo está utilizando SageMaker, será el rol de SageMaker ejecución.

Añada los permisos adecuados a la función y vuelva a actualizar el navegador.

Autenticarse con ID de creador de AWS

En el siguiente procedimiento, configurará el Builder ID, que utilizará para autenticarse cuando lo habilite. CodeWhisperer

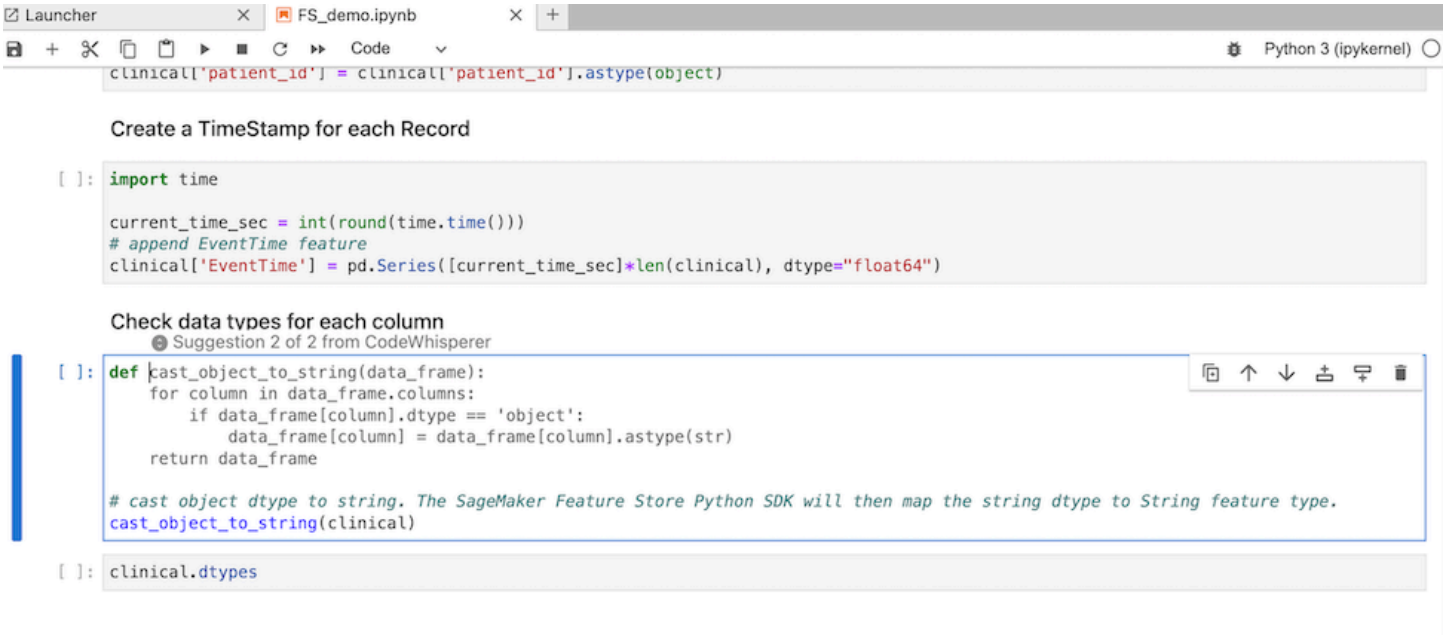
1. Actualice la pestaña del navegador en la que está utilizando JupyterLab.
2. En el CodeWhisperer panel situado en la parte inferior de la ventana, selecciona Iniciar CodeWhisperer.
3. En la ventana emergente, elija Copiar código y continuar.
4. En la página Crear ID de creador de AWS, si no tiene un ID de creador, ingrese una dirección de correo electrónico personal y elija Siguiente.

   Si ya tiene un ID de creador, siga al paso de la página Autorizar solicitud.
5. En la página Crear ID de creador de AWS, ingrese un nombre y elija Siguiente.

6. Cuando reciba el código de verificación por correo electrónico, ingréselo en el campo en blanco y elija Verificar.
7. En la siguiente pantalla, elige y confirma una contraseña y, a continuación, selecciona Crear ID de creador de AWS
8. En la página siguiente, selecciona Permitir para permitir CodeWhisperer el acceso a tus datos.

Ahora deberías iniciar CodeWhisperer sesión JupyterLab con Builder ID.

Para empezar a codificar, consulte Acciones del usuario.



Introducción a CodeWhisperer Amazon EMR Studio

En esta página se describe cómo configurar y activar Amazon CodeWhisperer para Amazon EMR Studio. Una vez activado, CodeWhisperer puede hacer recomendaciones de código automáticamente a medida que escribe su código ETL.

> **Note**
>
> CodeWhisperer es compatible con Python, que se puede utilizar para codificar scripts de ETL para trabajos de Spark en Amazon EMR Studio.

Utilice el siguiente procedimiento para configurar Amazon EMR Studio para que funcione con él. CodeWhisperer

1. Configure el bloc de notas de Amazon EMR Studio.
2. Asocie la siguiente política al rol del usuario de IAM para el bloc de notas de Amazon EMR Studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CodeWhispererPermissions",
            "Effect": "Allow",
            "Action": [
                "codewhisperer:GenerateRecommendations"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Abra la consola de Amazon EMR.
4. En Amazon EMR Studio, elija Espacios de trabajo (cuadernos).
5. Seleccione el espacio de trabajo deseado y elija Lanzamiento rápido.

Uso CodeWhisperer con AWS Glue Studio

En esta página se describe cómo configurar y activar Amazon CodeWhisperer for AWS Glue Studio Notebook. Una vez activado, CodeWhisperer puede hacer recomendaciones de código automáticamente a medida que escribe su código ETL.

> **Note**
>
> CodeWhisperer es compatible con Python y Scala, los dos lenguajes que se utilizan para codificar scripts ETL para los trabajos de Spark en AWS Glue Studio.

En el siguiente procedimiento, se configurará AWS Glue para trabajar con CodeWhisperer.

1. Configure AWS Glue Studio Notebook.
2. Asociación de la siguiente política al rol de IAM para el bloc de notas de Glue Studio

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CodeWhispererPermissions",
            "Effect": "Allow",
            "Action": [
                "codewhisperer:GenerateRecommendations"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Apertura de la consola de Glue
4. En Trabajos de ETL, elija Blocs de notas.
5. Verifique que se ha seleccionado Cuaderno de Jupyter. Seleccione Crear.
6. Ingrese un Job name (Nombre de trabajo).
7. Para el rol de IAM, selecciona el rol con el que has configurado para interactuar CodeWhisperer
8. Elija Iniciar bloc de notas.

Uso de Amazon CodeWhisperer con AWS Lambda

En este documento se describe cómo configurar y activar Amazon CodeWhisperer para la consola Lambda. Una vez activado, CodeWhisperer puede hacer recomendaciones de código a pedido en el editor de código Lambda a medida que desarrolla su función.

> **Note**
>
> En la consola Lambda, CodeWhisperer solo admite funciones que utilicen los tiempos de ejecución de Python y Node.js.

AWS Identity and Access Management permisos para Lambda

CodeWhisperer Para proporcionar recomendaciones en la consola Lambda, debe habilitar los permisos de IAM correctos para su usuario o rol de IAM. Se debe agregar el permiso `codewhisperer:GenerateRecommendations`, como se describe en la política de IAM de ejemplo que se muestra a continuación:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeWhispererPermissions",
      "Effect": "Allow",
      "Action": ["codewhisperer:GenerateRecommendations"],
      "Resource": "*"
    }
  ]
}
```

Se recomienda utilizar políticas de IAM para conceder permisos restrictivos a entidades principales de IAM. Para obtener más información sobre cómo trabajar con IAM for AWS Cloud9, consulte la administración de identidades y accesos AWS Cloud9 en la guía del usuario. AWS Cloud9

Activación de Amazon CodeWhisperer con Lambda

Para activarlo CodeWhisperer en el editor de código de la consola Lambda, complete estos pasos.

> **Note**
>
> CodeWhisperer para Lambda solo se admite en EE. UU. Este (Norte de Virginia).

1. Abra la página Function (Función) de la consola de Lambda y elija la función que desea editar.
2. En el editor de código de Code source (Origen del código), elja Tools (Herramientas) en la barra de menú superior.
3. Elija sugerencias de código de CodeWhisperer . Esto activa inmediatamente el servicio CodeWhisperer y aparece una marca de verificación junto a esta opción. Para desactivarlo, vuelve a seleccionar esta opción.

Para ver las teclas de acceso directo, consulte Acciones del usuario.

Uso CodeWhisperer con AWS Cloud9

AWS Identity and Access Management permisos para AWS Cloud9

CodeWhisperer Para poder ofrecer recomendaciones en la AWS Cloud9 consola, debe habilitar los permisos de IAM correctos para su usuario o rol de IAM. Se debe agregar el permiso `codewhisperer:GenerateRecommendations`, como se describe en la política de IAM de ejemplo que se muestra a continuación:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeWhispererPermissions",
      "Effect": "Allow",
      "Action": ["codewhisperer:GenerateRecommendations"],
      "Resource": "*"
    }
  ]
}
```

Se recomienda utilizar políticas de IAM para conceder permisos restrictivos a entidades principales de IAM. Para obtener más información sobre cómo trabajar con IAM AWS Cloud9, consulte la sección Gestión de identidades y accesos AWS Cloud9 en la guía del AWS Cloud9 usuario.

Activar Amazon CodeWhisperer con AWS Cloud9

Para activarlo CodeWhisperer en el editor de código de la AWS Cloud9 consola, sigue estos pasos.

1. Desde su AWS Cloud9 entorno actual, elija el AWS logotipo en el borde izquierdo de la ventana. Un panel se expandirá hacia la derecha.
2. En la parte inferior del panel, en Herramientas para desarrolladores, abre el CodeWhisperermenú desplegable.
3. Selecciona Activar. CodeWhisperer

Para ver ejemplos de cómo CodeWhisperer se integra AWS Cloud9 y muestra las sugerencias de código en el AWS Cloud9 IDE, consulte Ejemplos de código.

Uso CodeWhisperer con otros servicios

AWS Identity and Access Management permisos para otros servicios

CodeWhisperer Para ofrecer recomendaciones en el contexto de otro servicio, debe habilitar los permisos de IAM correctos para su usuario o rol de IAM. Se debe agregar el permiso `codewhisperer:GenerateRecommendations`, como se describe en la política de IAM de ejemplo que se muestra a continuación:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeWhispererPermissions",
      "Effect": "Allow",
      "Action": ["codewhisperer:GenerateRecommendations"],
      "Resource": "*"
    }
  ]
}
```

Se recomienda utilizar políticas de IAM para conceder permisos restrictivos a entidades principales de IAM. Para obtener más información sobre cómo trabajar con IAM, consulte las prácticas recomendadas de seguridad en la guía del usuario de IAM.

Características

CodeWhisperersu característica más destacada es su capacidad de proporcionarte sugerencias mientras escribes código.

CodeWhisperer anticipa cómo vas a terminar una línea de código o una línea de comentario. Puede generar una función completa para usted o puede completar un bloque de código. Puede sugerir funciones para completar cadenas de documentos y puede proporcionar line-by-line sugerencias a medida que codificas a tu propio ritmo.

Cuando lo usas CodeWhisperer con VS Code o JetBrains, se integra con Amazon CodeGuru para realizar escaneos de seguridad tanto en tu archivo activo como en sus dependientes, resaltando cualquier problema que encuentre.

Temas

- Personalizaciones
- Panel de control
- Acciones del usuario
- Soporte de idiomas en Amazon CodeWhisperer
- Pausar las sugerencias con Amazon CodeWhisperer
- Análisis de seguridad
- Referencias de código

Personalizaciones

La función de CodeWhisperer personalizaciones está en vista previa y está sujeta a cambios.

> **Note**
>
> Las personalizaciones solo están disponibles con CodeWhisperer Professional.

Cada equipo de desarrollo de software tiene una forma diferente de escribir código. Quizá quieras darte sugerencias que se ajusten CodeWhisperer a las bibliotecas internas de tu equipo, a las técnicas algorítmicas patentadas y al estilo de código empresarial.

En ese caso, CodeWhisperer las personalizaciones pueden ayudarte. Una personalización es un conjunto de elementos que CodeWhisperer permiten proporcionarle sugerencias basadas en el código base de su empresa.

Temas

- Requisitos previos para CodeWhisperer las personalizaciones
- Creación de la personalización
- Eliminación de la personalización
- Evaluación y optimización de la personalización
- Registro y solución de problemas
- Activar tus CodeWhisperer personalizaciones
- Actualizar tus personalizaciones CodeWhisperer
- Añadir usuarios y grupos a las CodeWhisperer personalizaciones
- Uso de personalizaciones CodeWhisperer

Requisitos previos para CodeWhisperer las personalizaciones

> La función de CodeWhisperer personalizaciones se encuentra en versión preliminar y está sujeta a cambios.

CodeWhisperer las personalizaciones se basan en las bases de CodeWhisperer Professional y utilizan sus funciones.

Para utilizar CodeWhisperer las personalizaciones, primero debe seguir el proceso de configuración CodeWhisperer profesional que se describe a continuación. Configuración de Amazon CodeWhisperer para administradores Esto incluye añadir a tu perfil CodeWhisperer profesional cualquier usuario al que también desees conceder acceso a las CodeWhisperer personalizaciones.

Al utilizar CodeWhisperer las personalizaciones, el CodeWhisperer administrador debe estar autorizado a acceder a su base de código, que puede almacenar en Amazon S3 o a través de ella. AWS CodeStar Sin embargo, durante el proceso de configuración estándar de CodeWhisperer

Professional, su AWS Organizations administrador no le proporciona acceso a esos servicios. CodeWhisperer

> **Note**
>
> Si los utiliza GitHub como fuente de datos, puede restringir el uso a determinados repositorios. Consulte Crear una conexión a GitHub en la Guía del usuario de Developer Tools Console.

Por lo tanto, antes de utilizar CodeWhisperer las personalizaciones, debe añadir los siguientes permisos a su función de CodeWhisperer administrador:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "sso-directory:DescribeUsers"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codewhisperer:CreateCustomization",
                "codewhisperer:DeleteCustomization",
                "codewhisperer:ListCustomizations",
                "codewhisperer:UpdateCustomization",
                "codewhisperer:GetCustomization",
                "codewhisperer:ListCustomizationPermissions",
                "codewhisperer:AssociateCustomizationPermission",
                "codewhisperer:DisassociateCustomizationPermission"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "codestar-connections:ListConnections",
                "codestar-connections:ListOwners",
                "codestar-connections:ListRepositories",
                "codestar-connections:GetConnection"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "codestar-connections:UseConnection",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "codestar-connections:ProviderAction": [
                        "GitPull",
                        "ListRepositories",
                        "ListOwners"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:ListBucket*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Acceder a los mensajes relacionados con la personalización en Amazon Logs CloudWatch

CodeWhisperer almacena información sobre la creación de su personalización en Amazon CloudWatch Logs.

Puede autorizar a su CodeWhisperer administrador a ver esos registros con el siguiente conjunto de permisos.

Para obtener más información sobre los permisos necesarios para entregar registros a varios recursos, consulte Registros que requieren permisos adicionales [V2] en la Guía del usuario de Amazon CloudWatch Logs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:PutDeliverySource",
                "logs:GetDeliverySource",
                "logs:DeleteDeliverySource",
                "logs:DescribeDeliverySources",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestination",
                "logs:DeleteDeliveryDestination",
                "logs:DescribeDeliveryDestinations",
                "logs:CreateDelivery",
                "logs:GetDelivery",
                "logs:DeleteDelivery",
                "logs:DescribeDeliveries",
                "firehose:ListDeliveryStreams",
                "firehose:DescribeDeliveryStream",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:account number:log-group:*",
                "arn:aws:firehose:us-east-1:account number:deliverystream/*",
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

Para obtener más información sobre cómo configurar los permisos necesarios para administrar CodeWhisperer Professional, consulteAsignación de derechos de administración CodeWhisperer.

> **Note**
>
> La clave de cifrado que configuró para CodeWhisperer Professional también se utiliza para CodeWhisperer las personalizaciones.

Es importante crear la personalización mediante el mejor material de origen posible. Al preparar el origen de datos, agregue código que contenga patrones que el equipo recomiende. Evite el código que contenga antipatrones, errores, vulnerabilidades de seguridad, problemas de rendimiento, etc.

La fuente de datos debe contener al menos 20 MB y, como máximo, 7 GB de archivos de código fuente de los idiomas compatibles. No hay límite en el número de archivos, pero debe incluir al menos 10 archivos para cada lenguaje que desee que admita la personalización. En el origen de datos de Amazon S3, asegúrese de que todo el código fuente esté ubicado en un directorio y no en nivel raíz. Se ignorarán los archivos que se encuentren en el nivel raíz.

> **Note**
>
> CodeWhisperer Las personalizaciones admiten los siguientes idiomas y extensiones de archivo:
>
> - Java (.java)
> - JavaScript (.js, .jsx)
> - Python (.py)
> - TypeScript (.ts, .tsx)

Creación de la personalización

La función de CodeWhisperer personalizaciones está en vista previa y está sujeta a cambios.

En esta sección se explica cómo crear una personalización con CodeWhisperer.

Para crear la personalización, siga este procedimiento:

1. Complete la configuración de CodeWhisperer Professional. Esto incluye habilitar el IAM Identity Center y autorizar a un administrador a CodeWhisperer activar la CodeWhisperer consola.

2. Abra la consola. CodeWhisperer
3. En el panel de navegación izquierdo, elija Personalizaciones.
4. Aparecerá la página de personalizaciones.
5. Elija Creación de personalización.
6. Escriba un nombre y (opcional) una descripción de personalización.

> **Note**
>
> Utilice nombres y descripciones que sirvan de información a los desarrolladores. Los desarrolladores de su organización que estén autorizados a usar CodeWhisperer Enterprise podrán verlos en VS Code o JetBrains mediante el AWS complemento.

Conexión con el origen de datos

La función de CodeWhisperer personalizaciones está en versión preliminar y está sujeta a cambios.

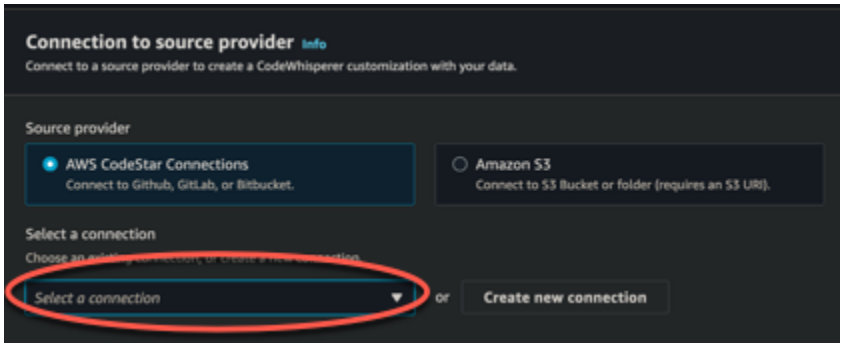
Antes de crear una personalización, debe conectarse al origen de datos que contiene el código base. La forma de hacerlo depende de donde esté el origen de datos.

Si tu fuente de datos está en Github o Bitbucket, debes conectarte a ella con. GitLab CodeConnections De lo contrario, utilice Amazon S3.

Para obtener más información CodeConnections, consulta ¿Qué son las conexiones? en la Guía del usuario de la consola Developer Tools

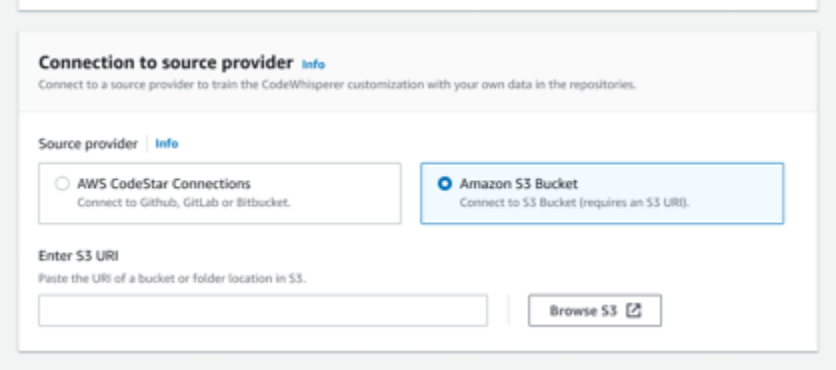
Para conectarse a su fuente de datos mediante CodeConnections, siga este procedimiento:

1. En Conexión al proveedor de origen, seleccione CodeConnections.
2. Si está utilizando una conexión existente, elija Seleccionar conexión existente. Luego, en Seleccionar una conexión, seleccione la conexión en el menú desplegable.



De lo contrario, elija Creación de una nueva conexión.

3. En la ventana emergente que se abre, navegue hasta el origen de datos y siga las instrucciones de la consola.
4. Tras crear el origen de datos, vuelva a la página Creación de personalización.
5. En Seleccionar una conexión, seleccione la conexión en el menú desplegable.



Para conectarse al origen de datos a través de Amazon S3, siga este procedimiento:

1. En Conexión al proveedor de origen, seleccione Amazon S3.
2. Elija Explorar Amazon S3.
3. Navegue hasta el bucket o la carpeta que contiene el código base y anote el URI.

   Para obtener más información, consulte Creación, configuración y trabajo con buckets de Amazon S3 y Prácticas recomendadas de control de acceso en la Guía del usuario de Amazon S3.
4. Pegue la URL en el campo etiquetado Ingresar el URI de Amazon S3.

Antes de crear la personalización, tiene la opción de agregarle etiquetas.

Para obtener más información sobre las etiquetas, consulta la Guía del usuario sobre cómo etiquetar tus AWS recursos.

Tras seguir los procedimientos anteriores, elija Creación de personalización.

Las personalizaciones y los datos

CodeWhisperer las personalizaciones utilizan su contenido para presentarle sugerencias al estilo de los desarrolladores de su organización.

Sin embargo, no AWS almacenará ni utilizará su contenido en ningún contexto que no sea directamente útil para su empresa.

AWS no utilizará su contenido para ofrecer sugerencias de código a otros clientes.

CodeWhisperer no hará referencia a los escaneos de seguridad de otros clientes (ni de ti).

Solución de problemas relacionados con la creación de la personalización

- Es posible que reciba el error: `Total size of the provided repositories exceeds the maximum allowed size of number for a customization.`

  En ese caso, elimine un repositorio del origen de datos e inténtelo de nuevo.
- Es posible que reciba el error: `Insufficient data to create a customization. Add more files from supported languages and retry.`

  Para que el código escrito en un lenguaje determinado se utilice para crear una personalización, debe haber al menos 10 archivos que contengan código en ese lenguaje del origen de datos. El tamaño total de todos los archivos de códigos (que contienen uno o más idiomas de la fuente de datos debe ser de al menos 20 MB.

  Algunos archivos, aunque estén en el idioma correspondiente, no se tendrán en cuenta hacia los 20 MB. Por ejemplo, los archivos duplicados y los archivos en un formato no compatible no se tendrán en cuenta.

  Si recibe este error, agregue más archivos que contengan el lenguaje de programación en el que se centra la personalización e inténtelo de nuevo.

Eliminación de la personalización

La función de CodeWhisperer personalizaciones está en vista previa y está sujeta a cambios.

En esta sección se explica cómo eliminar una personalización con CodeWhisperer.

> **Warning**
>
> Al eliminar una personalización, se eliminarán todas las versiones asociadas al recurso.

Para eliminar la personalización, siga este procedimiento:

1. Abre la CodeWhisperer consola.
2. En el panel de navegación izquierdo, elija Personalizaciones.
3. Aparecerá la página de personalizaciones.
4. Si la personalización que quiere eliminar sigue activa, elija Desactivar.
5. Elija Eliminar.

> **Note**
>
> También puede eliminar una personalización de la página que contiene los detalles de dicha personalización.
> Para ello, elija Eliminar de la esquina superior derecha de la página de detalles de la personalización.

Si está realizando la transición a Amazon Q Developer, el siguiente paso es desactivar la CodeWhisperer aplicación.

Evaluación y optimización de la personalización

La función de CodeWhisperer personalizaciones está en vista previa y está sujeta a cambios.

Evaluación de la personalización

En esta sección se explica cómo evaluar la personalización.

1. En la CodeWhisperer consola, en el panel de navegación, selecciona Personalizaciones.
2. Elija el nombre de la personalización que desee examinar.
3. En la parte derecha de la ventana se mostrará una puntuación de evaluación. Esta puntuación indica CodeWhisperer la evaluación de la eficacia de la personalización.

Con la puntuación de evaluación en mente, ahora debe considerar si debe activar o no la personalización. Al tomar esta decisión, tenga en cuenta los siguientes factores.

- Muy bien de 8 a 10: se CodeWhisperer recomienda activar esta personalización.
- De 5 a 7: se CodeWhisperer recomienda activar esta personalización.

  Si no ve una mejora significativa, tenga en cuenta las siguientes sugerencias de optimización. Si no son eficaces, considere la posibilidad de cambiar a un código fuente diferente.
- Malo 1-4: es probable que esta personalización no sea útil. Tenga en cuenta las siguientes sugerencias de optimización. Si no son eficaces, considere la posibilidad de cambiar a un código fuente diferente.

Optimización de la personalización

Esta sección contiene sugerencias para optimizar la sugerencia a fin de lograr una puntuación de evaluación más alta.

- Considere la posibilidad de ampliar el origen de datos para incluir más repositorios de código.
- Si incluyó principalmente datos de lenguajes de programación limitados, considere la posibilidad de ampliarlos a más lenguajes.
- Elimine los archivos y repositorios generados automáticamente o los generados a partir de plantillas. Capacitar una personalización para generar o completar dichos archivos no suele ser útil y, por lo general, no hace más que agregar ruido.

> **Note**
>
> CodeWhisperer filtra automáticamente los archivos que no son de código, como los archivos de configuración y los archivos de texto.

- Es posible que la base de código no utilice bibliotecas internas con frecuencia. Si sabe que esto es cierto, es posible que el CodeWhisperer modelo básico ya haya funcionado lo mejor posible.

Optimización para los lenguajes que utiliza

Para que el código de un idioma concreto se utilice en una personalización, debe incluir al menos 10 archivos de datos que contengan ese idioma y todos los archivos fuente juntos deben ocupar al menos 20 MB. Si los desarrolladores escriben el código en un lenguaje que no es compatible con la personalización, CodeWhisperer las recomendaciones en ese idioma se basarán en el modelo CodeWhisperer base (no en la personalización). En otras palabras, serán las mismas recomendaciones que recibiría si no tuviera una personalización. Esto, a su vez, podría afectar a las métricas en el panel. Por ejemplo, las «líneas de código generadas por CodeWhisperer» pueden ser inferiores a las que habrían sido si se hubiera incluido en la personalización el lenguaje que suelen utilizar los desarrolladores.

Registro y solución de problemas

Configuración de entrega de registros

CodeWhisperer puede proporcionarle archivos de registro que le ayudarán a comprender y solucionar los problemas relacionados con la personalización.

Puede hacer que sus archivos de registro se envíen a un grupo de Amazon CloudWatch Logs., a un bucket de Amazon S3, a un Amazon Data Firehose o a cualquier combinación.

Para configurar la entrega de registros, seleccione la pestaña Entregas de registros en la página de la consola para personalizarlos. Siga las instrucciones de la interfaz para configurar las entregas de registros. A continuación, elija Creación de entregas de registros.

El prefijo de registros entregados a un bucket de Amazon S3 será: `AWSLogs/`*`account_id`*`/codeWhispererCustomizationLogs/`*`region`*`/`*`customization_id`*`/`*`year`*`/`*`month`*`/`*`day`*`/`*`hour`*`/`

Los archivos se comprimirán con el formato de denominación: *`account_id`*`_codeWhispererCustomizationLogs_`*`customization_id_date_file_id`*`.log.gz`

> **Warning**
>
> Para aprovechar al máximo los registros de personalización, es mejor configurar la entrega de registros en los cinco minutos siguientes a la creación de la personalización.

Para obtener más información sobre los permisos necesarios para entregar registros a varios recursos, consulte Registros que requieren permisos adicionales [V2] en la Guía del usuario de Amazon CloudWatch Logs.

Descripción de los mensajes de registro relacionados con la personalización

En la siguiente tabla se muestran los mensajes de registro que pueden ayudarle a comprender los problemas relacionados con la personalización.

Mensajes de registro	Nivel de registro
`Starting to ingest number repos from source source`	Información
`Downloading data from repo: repo name`	Información
`Received amount MB of supported data. amount MB required. Add more data and retry.`	Error
`The provided CodeStar Connection ARN: Arn is invalid.`	Error
`Access denied when attempting to reach the provided CodeStar Connection: Arn`	Error
`Failed to download with AWS CodeStar Connection: Arn probably deleted by customer`	Error

Mensajes de registro	Nivel de registro
`ProviderThrottlingException from CodeStar Connection: Arn while cloning repository: repository`	Error
`Processing data from S3: S3 URI`	Información
`Invalid S3 path specified: S3 Directory`	Error
`Unable to access the provided S3 bucket: bucket name`	Error
`The provided S3 bucket: bucket name does not exist.`	Error
`The provided S3 key S3 URI does not exist.`	Error
`Failed to ingest number of failed repos / total number of repos repositories`	Error
`Unable to process repository: repo name, with a size of repo size GB, exceeds the limit of max size GB.`	Advertencia
`Unable to process file: file name, with a size of file size, which exceeds the limit of max file size MB`	Error
`Unable to process collection: collection name , with total size of total repo size MB, which exceeds the limit of max total repo size MB`	Error

Mensajes de registro	Nivel de registro
`The following languages will be used for customization: list of languages . Languages may be excluded from customization if they are not sufficiently represented in your files.`	Información

Descripción de los mensajes de error relacionados con la personalización en la consola

La siguiente tabla le ayudará a entender los mensajes relacionados con la personalización en la CodeWhisperer consola.

Mensaje de error	Acción sugerida
Ha activado el número máximo de personalizaciones.	Desactive una personalización activa e inténtelo de nuevo.
Ha superado el *límite* máximo de permisos de grupo.	Elimine un grupo y vuelva a intentarlo.
Ha superado el *límite* máximo de permisos de usuario.	Elimine un usuario y vuelva a intentarlo.
Se ha alcanzado el número máximo de trabajos activos.	Espere a que finalice un trabajo en curso en la misma cuenta. Vuelva a intentar la operación.
Se ha producido un error inesperado al procesar la solicitud.	Vuelva a intentar la operación. Si sigue produciendo error, contacte con el servicio de atención al cliente.
Acceso denegado al intentar acceder a la conexión de AWS CodeStar proporcionada.	Valide los permisos de la conexión y del proveedor de terceros. A continuación, vuelva a ejecutar la operación.

Mensaje de error	Acción sugerida
No se encontraron uno o más repositorios al acceder a la conexión proporcionada. AWS CodeStar	Valide los permisos y la lista de repositorios del proveedor de terceros. A continuación, vuelva a ejecutar la operación.
El ARN de AWS CodeStar conexión proporcio nado no es válido.	Actualice la personalización con un ARN de conexión corregido.
El host asociado a la AWS CodeStar conexión proporcionada no está disponible.	Intente establecer la conexión en 5 minutos.
Se ha especificado una ruta de Amazon S3 no válida.	Actualice la personalización con un URI de Amazon S3 válido.
No se puede acceder al bucket de Amazon S3 proporcionado.	Valide los permisos para el rol de administr ador. Vuelva a intentarlo después de solucionar cualquier problema con los permisos.
El bucket de Amazon S3 proporcionado no existe.	Actualice la personalización con un URI de Amazon S3 válido.
La clave de Amazon S3 proporcionada no existe.	Actualice la personalización con un URI de Amazon S3 válido.
Datos insuficientes para crear una personali zación. Agregue más archivos de los lenguajes compatibles y vuelva a intentarlo.	Agregue más datos al mismo origen de datos y actualice la personalización con la misma referencia.
El tamaño total de los repositorios proporcio nados supera el *tamaño* máximo permitido para una personalización.	Elimine algunos datos del origen de datos proporcionado. Actualice la personalización con la misma referencia.
Ha creado el número máximo de personali zaciones. Elimine una personalización existente e inténtelo de nuevo.	Elimine la personalización actual y vuelva a intentarlo.

Mensaje de error	Acción sugerida
Existen personalizaciones dentro de la cuenta. Debe eliminar todas las personalizaciones antes de eliminar el perfil.	Elimine todas las personalizaciones asociadas a la cuenta y vuelva a intentarlo.

Activar tus CodeWhisperer personalizaciones

La función de CodeWhisperer personalizaciones se encuentra en una vista previa y está sujeta a cambios.

Activación de una versión

En esta sección se describe cómo activar y desactivar una versión de la personalización.

Puede activar una nueva versión de una personalización, incluso cuando los desarrolladores de la organización utilicen la versión anterior. Tras activar la nueva versión, los desarrolladores empezarán a utilizarla sin problemas, sin necesidad de realizar ajustes por parte del desarrollo.

También puede devolver la personalización a un estado previamente activo. Sin embargo, en realidad CodeWhisperer no reactiva una versión previamente activada. En su lugar, crea una nueva versión copiando una versión anterior y, a continuación, activando la copia.

Por ejemplo, suponga que tiene tres versiones: 1, 2 y 3. La versión activa es la 3. Decide volver a la versión 1. Pero “reactivar” la versión 1 en realidad es simplemente copiar la versión 1 y crear la versión 4. Esa es la versión que usa: la versión 4, la nueva copia de la versión anterior.

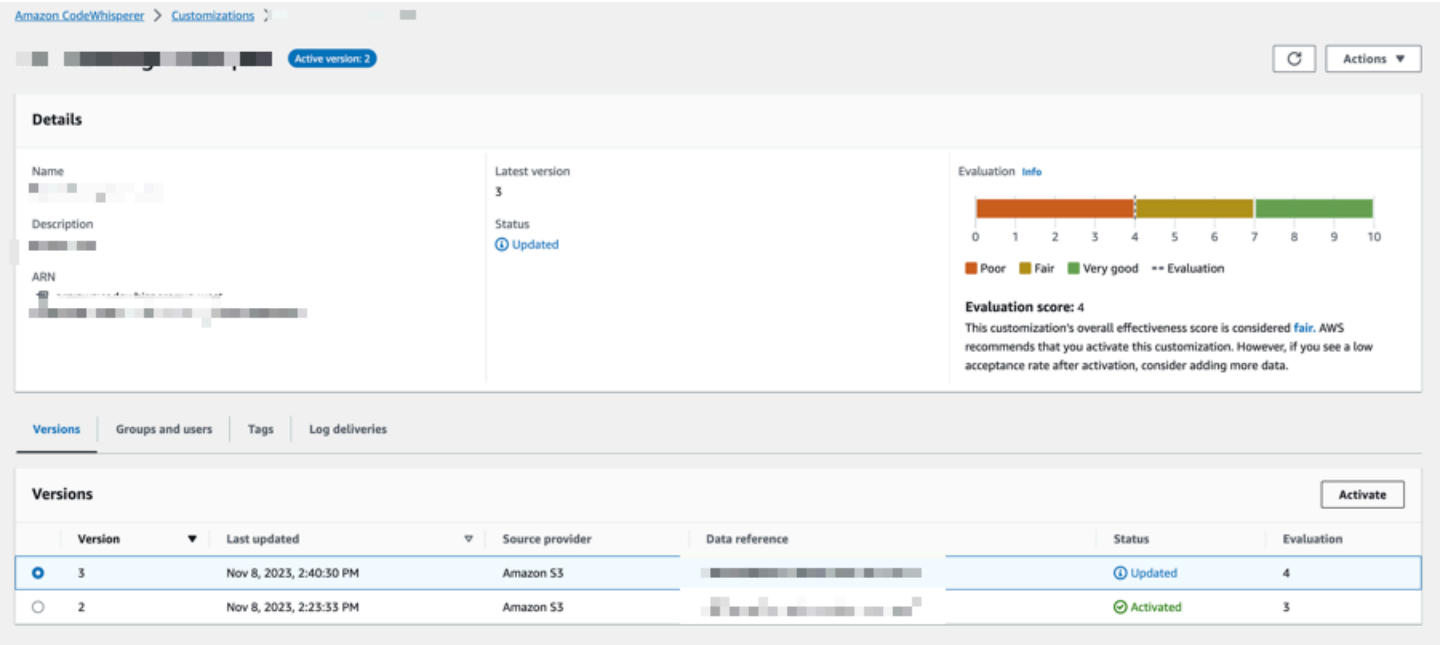
Para activar una versión de la personalización, siga este procedimiento:

1. Abre la CodeWhisperer consola.
2. En el panel de navegación izquierdo, elija Personalizaciones.

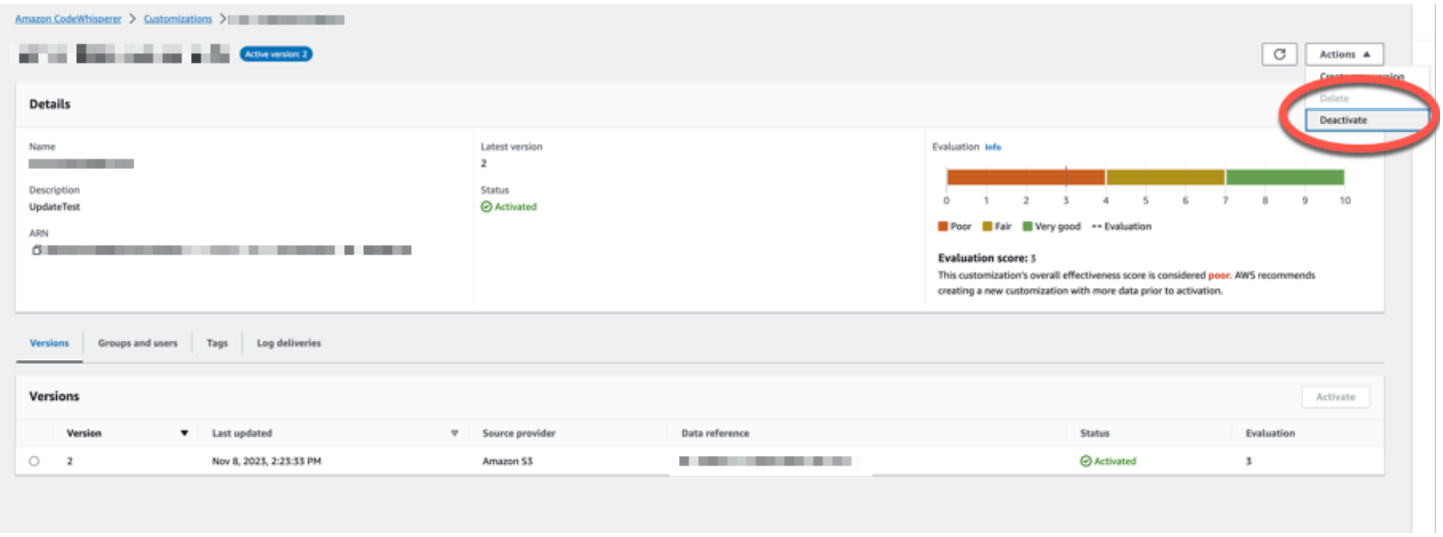
   Aparecerá la página de personalizaciones.
3. Elija la personalización para la que desea activar una versión.

   Aparecerá la página de detalles de personalización.
4. Elija la versión que desee activar en la tabla de versiones.

5. Seleccione Activar.



Para desactivar una personalización, elija Desactivar en el menú desplegable.



Actualizar tus personalizaciones CodeWhisperer

La función de CodeWhisperer personalizaciones está en versión preliminar y está sujeta a cambios.

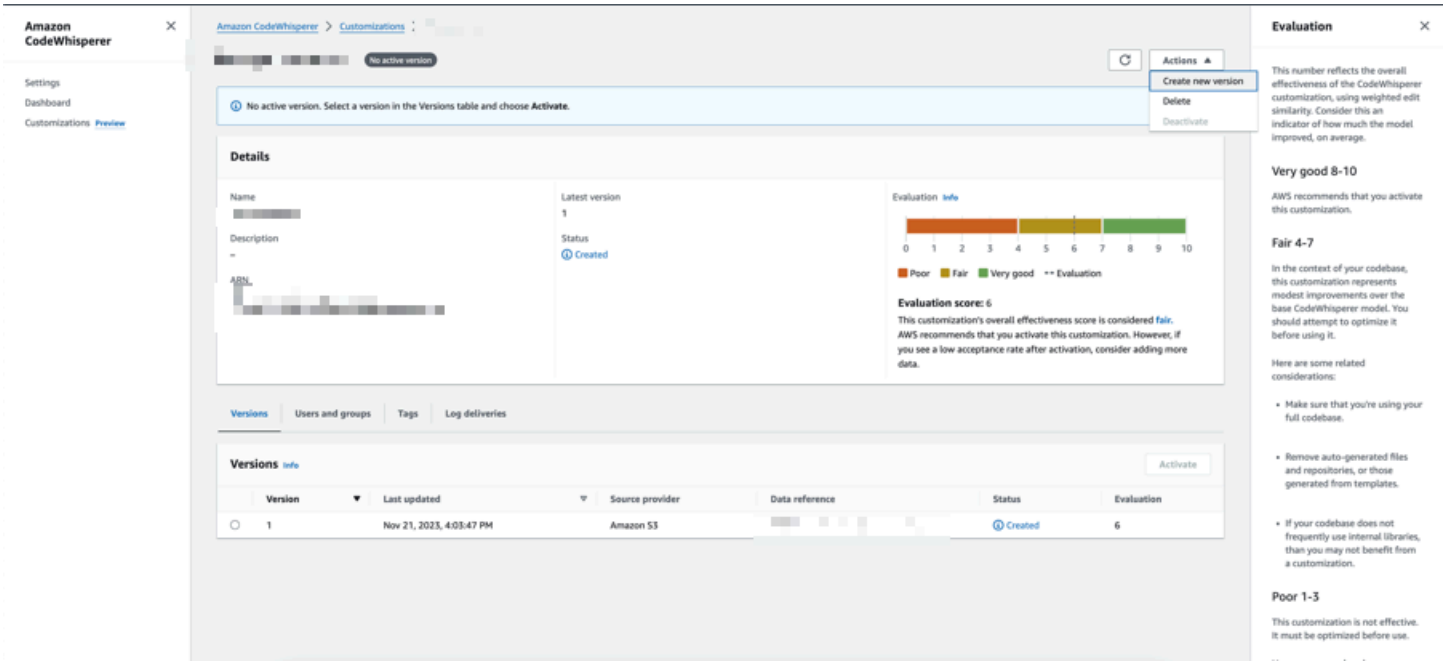
En esta sección se explica cómo actualizar una personalización con CodeWhisperer.

Una personalización puede tener varias versiones.

CodeWhisperer los administradores tienen acceso a un máximo de tres versiones para cada personalización:

- la versión más reciente
- la versión actualmente activa
- la versión activa más reciente que no está activa actualmente

Creación de una nueva versión

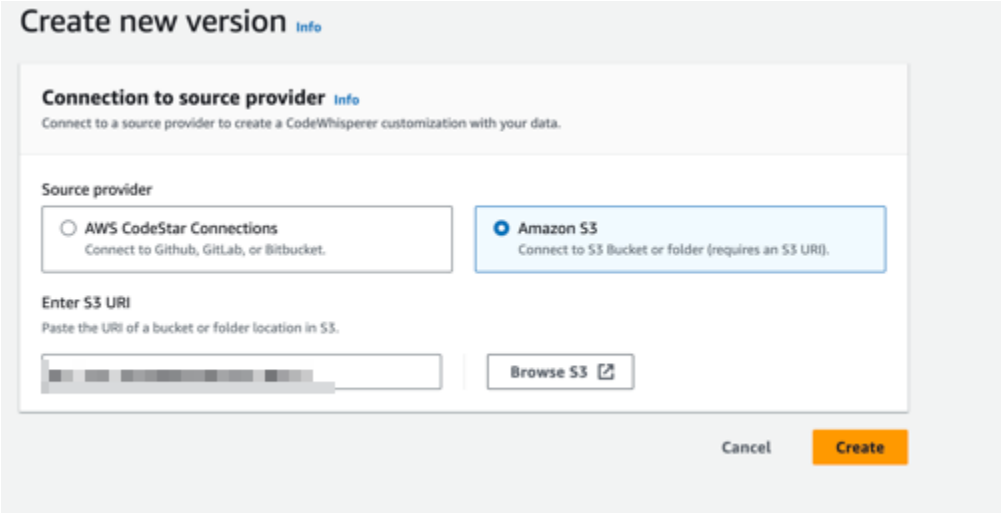


Para crear una nueva versión de la personalización, siga este procedimiento:

1. Abra la CodeWhisperer consola.
2. En el panel de navegación izquierdo, elija Personalizaciones.

   Aparecerá la página de personalizaciones.
3. Elija la personalización para la que desea crear una nueva versión.

   Aparecerá la página de detalles de personalización.
4. Seleccione Creación de nueva versión en el menú desplegable Acciones.
5. Si corresponde, cambie el origen de datos.



6. Seleccione Crear.

Si recibe mensajes de error, consulte Solución de problemas relacionados con la creación de la personalización.

Añadir usuarios y grupos a las CodeWhisperer personalizaciones

La función de CodeWhisperer personalizaciones está en versión preliminar y está sujeta a cambios.

Esta sección contiene información acerca de cómo agregar usuarios y grupos a las personalizaciones.

> **Note**
>
> Debe activar una personalización antes de poder agregarle usuarios.

> **Note**
>
> Solo puedes añadir un usuario o un grupo a una personalización si ya lo has añadido a tu perfil CodeWhisperer profesional. Para obtener más información, consulte Configuración de Amazon CodeWhisperer para administradores

1. En la CodeWhisperer consola, en el panel de navegación, selecciona Personalizaciones.
2. Elija el nombre de la personalización a la que desea agregar usuarios o grupos.
3. En la mitad inferior de la ventana, si es necesario, seleccione la pestaña Usuarios y grupos y, a continuación, la subpestaña Usuarios o Grupos.
4. Seleccione los usuarios o grupos que requieren acceso a la personalización.
5. Elija Agregar usuarios o Agregar grupos.

Uso de personalizaciones CodeWhisperer

> La función de CodeWhisperer personalizaciones se encuentra en una vista previa y está sujeta a cambios.

Esta sección contiene información acerca de cómo usar personalizaciones como desarrollador.

CodeWhisperer solo admite personalizaciones en VS Code e JetBrains IDE.

AWS Toolkit for Visual Studio Code

Cómo utilizar las personalizaciones con VS Code.

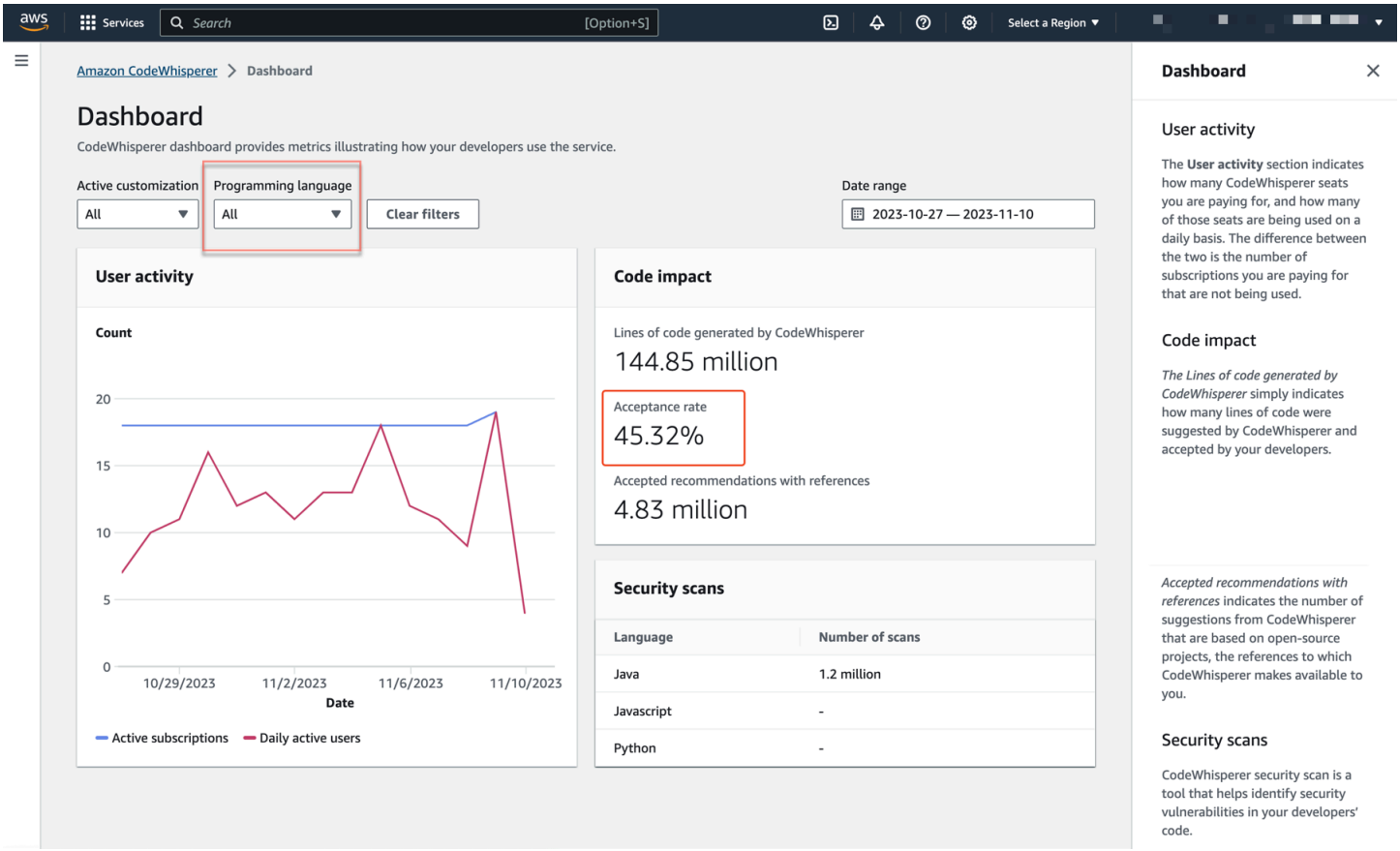
1. Realice la autenticación CodeWhisperer profesional con IAM Identity Center siguiendo los pasos que se indican a continuación. Primeros pasos CodeWhisperer en VS Code y JetBrains
2. En el panel Herramientas para desarrolladores, en CodeWhisperer, seleccione Seleccionar personalización.
3. En la parte superior de la ventana, en el menú desplegable, seleccione la personalización adecuada.

AWS Toolkit for JetBrains

1. Para autenticarse en CodeWhisperer Professional con IAM Identity Center, siga los pasos que se indican a continuación. Primeros pasos CodeWhisperer en VS Code y JetBrains
2. En el panel Herramientas para desarrolladores, en CodeWhisperer, seleccione Seleccionar personalización.

3. En la ventana emergente, seleccione la personalización adecuada.
4. Elija Conectar.

Panel de control



Disponible solo para los administradores y solo en el nivel profesional, el CodeWhisperer panel resume datos útiles sobre cómo los desarrolladores utilizan el servicio. Entre las métricas útiles se encuentra la tasa de aceptación, que indica la frecuencia con la que aceptas CodeWhisperer las sugerencias.

Puede filtrar los datos en el panel por rango de fechas. El intervalo mínimo es de dos semanas y el máximo de un año. También puede filtrar por lenguaje de programación.

Para ver las métricas en el panel de control, debes tener los `cloudwatch:listMetrics` permisos `cloudwatch:GetMetricData` y. Este permiso se concede a los administradores como parte de la asignación de derechos de CodeWhisperer administración.

Actividad de los usuarios

La sección de actividad del usuario indica cuántos CodeWhisperer asientos está pagando y cuántos de esos asientos se utilizan a diario. La diferencia entre ambos es la cantidad de suscripciones que está pagando y que no se están utilizando.

Impacto del código

Las líneas de código generadas por CodeWhisperer simplemente indican cuántas líneas de código sugirieron CodeWhisperer y aceptaron sus desarrolladores.

Las recomendaciones aceptadas con referencias indican el número de sugerencias CodeWhisperer que se basan en proyectos de código abierto, cuyas referencias CodeWhisperer pone a su disposición.

Si utilizas CodeWhisperer muy poco durante un período de dos semanas, la sección sobre el impacto del código se verá afectada de la siguiente manera:

- Si no se invoca ninguna recomendación durante dos semanas, no aparecerá ningún dato en la sección Code impact.

- Si se invoca una recomendación, pero no se acepta o rechaza ninguna, no aparecerá ningún dato en la sección sobre el impacto del código.

- Si se invoca una recomendación y no se acepta ninguna, pero se rechaza alguna, se mostrará la tasa de aceptación (0%), pero no se mostrará ningún dato sobre las líneas de código generadas por CodeWhisperer o las recomendaciones aceptadas con referencias.

Análisis de seguridad

CodeWhisperer el análisis de seguridad es una herramienta que ayuda a identificar las vulnerabilidades de seguridad en el código de los desarrolladores.

Los datos mostrados indican cuántos análisis han realizado correctamente los desarrolladores en los IDE.

Acciones del usuario

Amazon SageMaker

Acción	Método abreviado de teclado
Actívala manualmente CodeWhisperer	MacOS: Opción + C Windows: Alt + C
Aceptar una recomendación	Tab
Siguiente recomendación	Flecha hacia abajo
Recomendación anterior	Flecha hacia arriba
Rechazar una recomendación	ESC

JupyterLab

Acción	Método abreviado de teclado
Activar manualmente CodeWhisperer	MacOS: Opción + C Windows: Alt + C
Aceptar una recomendación	Tab
Siguiente recomendación	Flecha hacia abajo
Recomendación anterior	Flecha hacia arriba
Rechazar una recomendación	ESC

AWS Glue Studio Notebook

Acción	Método abreviado de teclado
Activar manualmente CodeWhisperer	MacOS: Opción + C

Acción	Método abreviado de teclado
	Windows: Alt + C
Aceptar una recomendación	Tab
Siguiente recomendación	Flecha hacia abajo
Recomendación anterior	Flecha hacia arriba
Rechazar una recomendación	ESC

Toolkit for Visual Studio

Acción	Método abreviado de teclado
Activar manualmente CodeWhisperer `AWSToolkit.CodeWhisperer.GetSuggestion` en los enlaces de teclado	Alt + C
Aceptar una recomendación	Tab
Siguiente recomendación `Edit.NextSuggestion` en los enlaces de teclado	Alt + .
Recomendación anterior `Edit.PreviousSuggestion` en los enlaces de teclado	Alt + ,
Rechazar una recomendación	ESC, retroceso o seguir intentando y la recomendación desaparecerán tan pronto como haya una falta de coincidencia de caracteres.

Consulte también los atajos de teclado predeterminados de Visual Studio de Microsoft.

Para cambiar los enlaces de teclado en Visual Studio, utilice Herramientas -> Opciones -> Teclado.

AWS Toolkit for Visual Studio Code

Acción	Método abreviado de teclado
Activar manualmente CodeWhisperer	MacOS: Opción + C Windows: Alt + C
Aceptar una recomendación	Tab
Siguiente recomendación	Flecha derecha
Recomendación anterior	Flecha izquierda
Rechazar una recomendación	ESC, retroceso o seguir intentando y la recomendación desaparecerán tan pronto como haya una falta de coincidencia de caracteres.

Para cambiar los enlaces de teclado en VS Code, consulte Enlaces de teclado para Visual Studio Code en el sitio web de VS Code.

> **Note**
>
> La barra de herramientas de sugerencias insertadas de VS Code está desactivada de forma predeterminada. Para obtener más información, consulte la barra de herramientas de sugerencias insertadas rediseñada en el sitio web de VS Code.

AWS Toolkit for JetBrains

Acción	Método abreviado de teclado
Activar manualmente CodeWhisperer	MacOS: Opción + C Windows: Alt + C

Acción	Método abreviado de teclado
Aceptar una recomendación	Tab
Siguiente recomendación	Flecha derecha
Recomendación anterior	Flecha izquierda
Rechazar una recomendación	ESC, retroceso o seguir intentando y la recomendación desaparecerán tan pronto como haya una falta de coincidencia de caracteres.

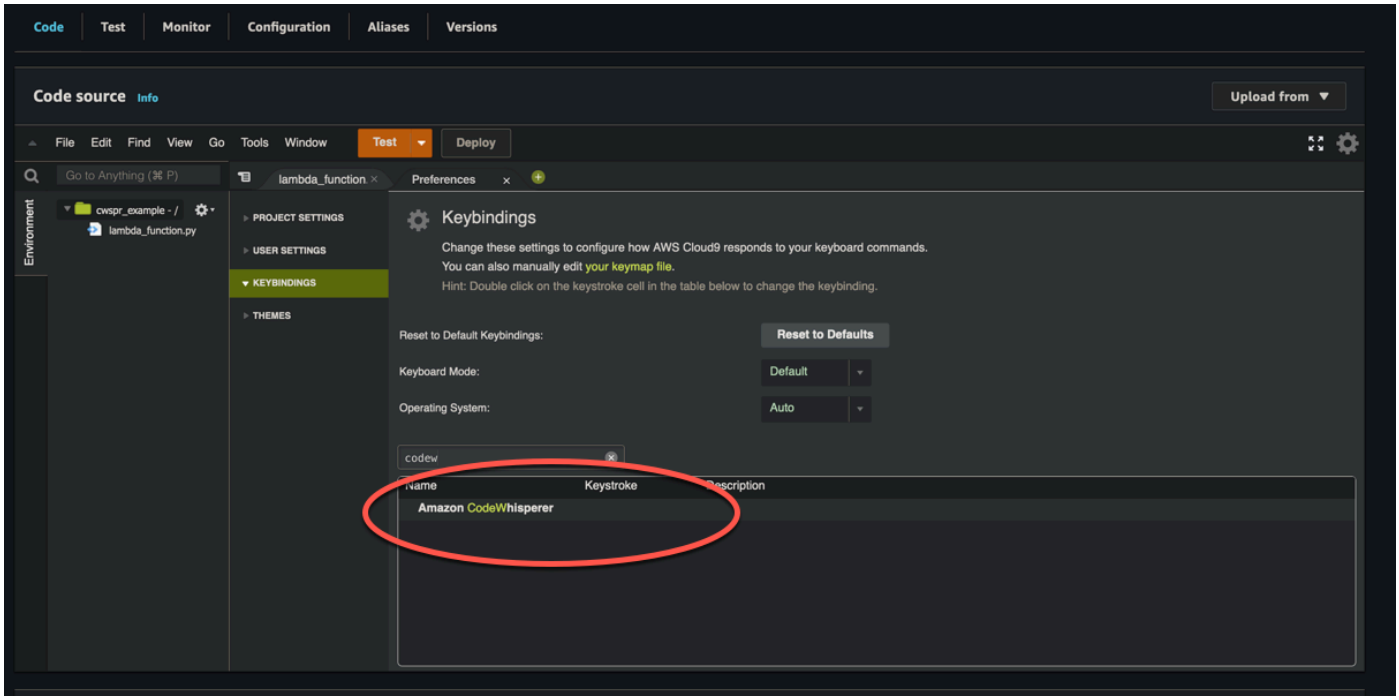
Para cambiar las combinaciones de teclas en IntelliJ, consulte los atajos de teclado de IntelliJ IDEA en el sitio web. JetBrains

Lambda

Acción	Método abreviado de teclado
Obtener manualmente una sugerencia de código	MacOS: Opción + C Windows: Alt + C
Aceptar una sugerencia	Tab
Rechazar una sugerencia	ESC, Retroceso, desplácese en cualquier dirección o siga escribiendo y la recomenda ción desaparece automáticamente.

Para cambiar los enlaces de teclado claves, use el procedimiento siguiente.

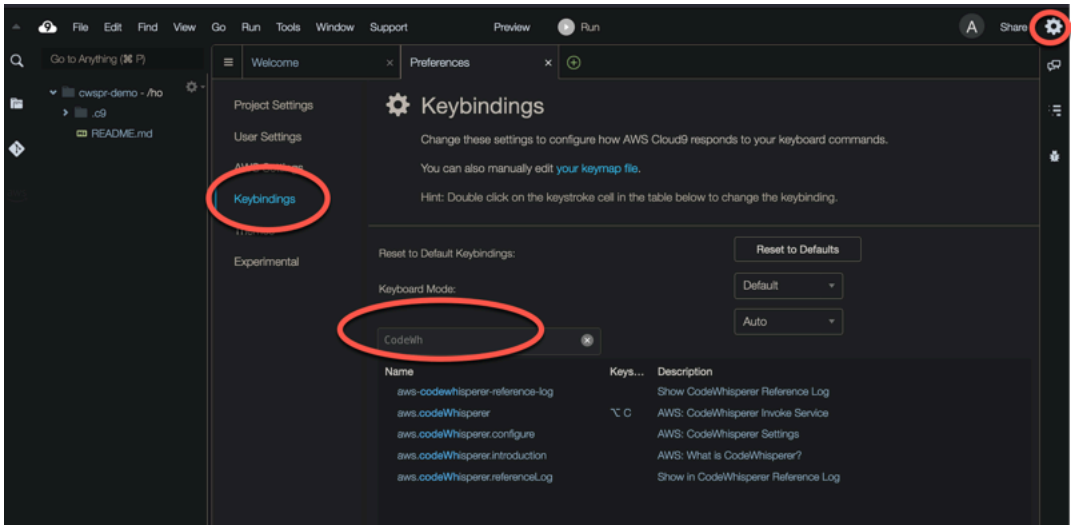
1. Mientras se visualiza una función en particular, elija el icono de engranaje para abrir la pestaña de preferencias.
2. En la pestaña Preferencias, elija Enlaces de teclado.
3. En el cuadro de búsqueda de combinaciones de teclas, introduzca. CodeWhisperer



AWS Cloud9

Acción	Método abreviado de teclado
Obtener manualmente una sugerencia de código	MacOS: Opción + C Windows: Alt + C
Aceptar una sugerencia	Tab
Rechazar una sugerencia	ESC, Retroceso, desplácese en cualquier dirección o siga escribiendo y la recomenda ción desaparece automáticamente.

1. Mientras se visualiza un entorno en particular, elija el icono de engranaje para abrir la pestaña de preferencias.
2. En la pestaña Preferencias, elija Enlaces de teclado.
3. En el cuadro de búsqueda de combinaciones de teclas, introduzca. CodeWhisperer
4. En la columna Combinación de teclas, haga doble clic en el espacio correspondiente a la función que le interese.
5. Ingrese las teclas a las que desee vincular la función.



Soporte de idiomas en Amazon CodeWhisperer

Soporte de idiomas en Amazon CodeWhisperer

CodeWhisperer admite la generación de código para varios lenguajes de programación. La precisión y la calidad de la generación de código para un lenguaje de programación dependen del tamaño y la calidad de los datos de entrenamiento.

En cuanto a la calidad de los datos de entrenamiento, los lenguajes de programación más compatibles son:

- Java
- Python
- JavaScript
- TypeScript
- C#
- Go
- PHP
- Rust
- Kotlin
- SQL

Los lenguajes de infraestructura como código (IaC) más compatibles son:

- JSON (AWS CloudFormation)
- YAML (AWS CloudFormation)
- HCL (Terraform)
- CDK (Typescript, Python)

CodeWhisperer también admite la generación de código para:

- Ruby
- C++
- C
- Intérprete de comandos
- Scala

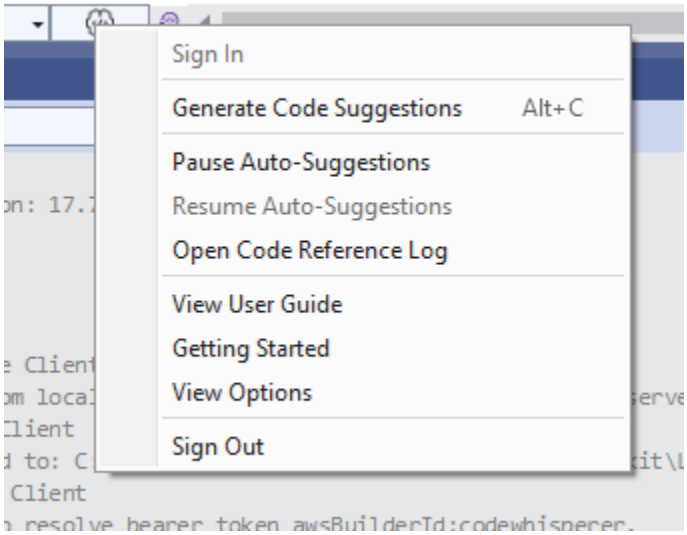
Para obtener una lista de los entornos de codificación compatibles, consulte Primeros pasos.

Pausar las sugerencias con Amazon CodeWhisperer

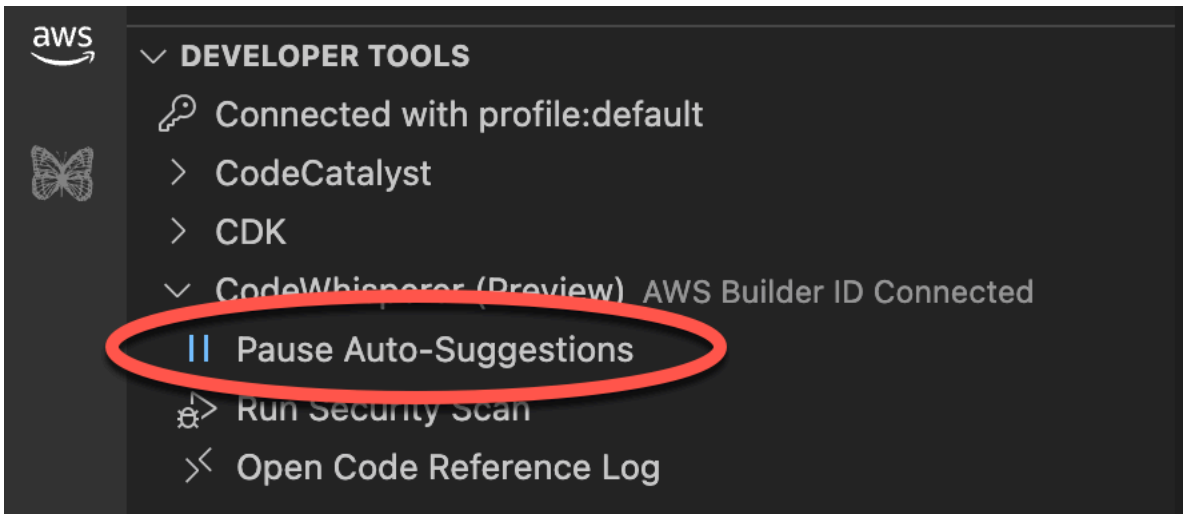
En este capítulo se describe cómo pausar y reanudar las sugerencias automáticas en CodeWhisperer.

Visual Studio

1. Desde el borde de la ventana, selecciona el CodeWhisperer icono.
2. Selección de Pausa de las sugerencias automáticas o Reanudación de las sugerencias automáticas

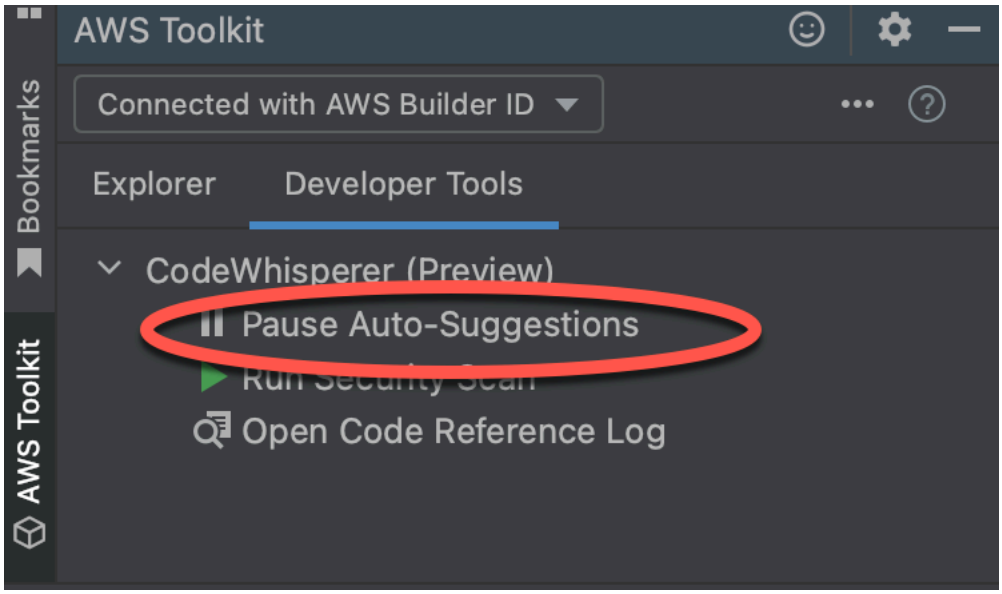


VS Code



1. En VS Code, elige el AWS logotipo en la barra lateral izquierda.
2. En la parte inferior de la ventana de VS Code, amplíe la sección Herramientas para desarrolladores.
3. Amplía la sección CodeWhisperer .
4. Elija Pausar las sugerencias automáticas o Reanudar las sugerencias automáticas.

JetBrains



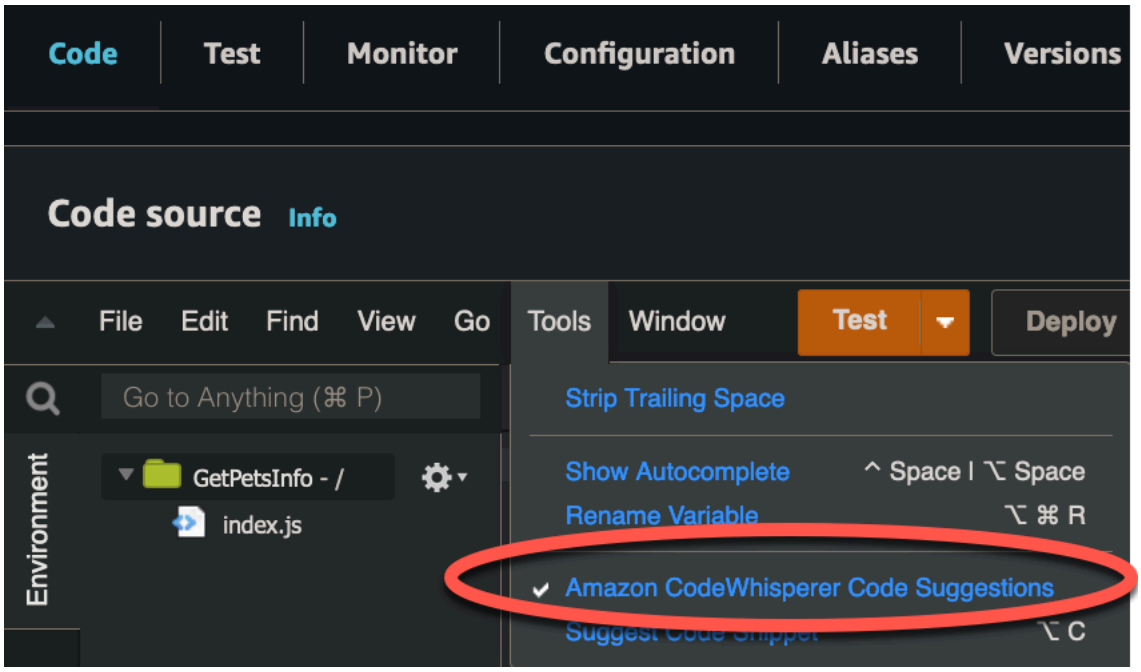
1. En JetBrains, elige el AWS logotipo de la barra lateral izquierda.
2. En la ventana del AWS kit de herramientas, selecciona la pestaña Herramientas para desarrolladores.
3. Amplíe la CodeWhisperer sección.
4. Elija Pausar las sugerencias automáticas o Reanudar las sugerencias automáticas.

AWS Cloud9

CodeWhisperer no permite activar y desactivar las sugerencias. AWS Cloud9

Para dejar de recibir CodeWhisperer sugerencias AWS Cloud9, elimina la política de IAM que da CodeWhisperer acceso AWS Cloud9 del rol o usuario al que estás accediendo. AWS Cloud9 Para obtener más información, consulte AWS Identity and Access Management permisos para AWS Cloud9

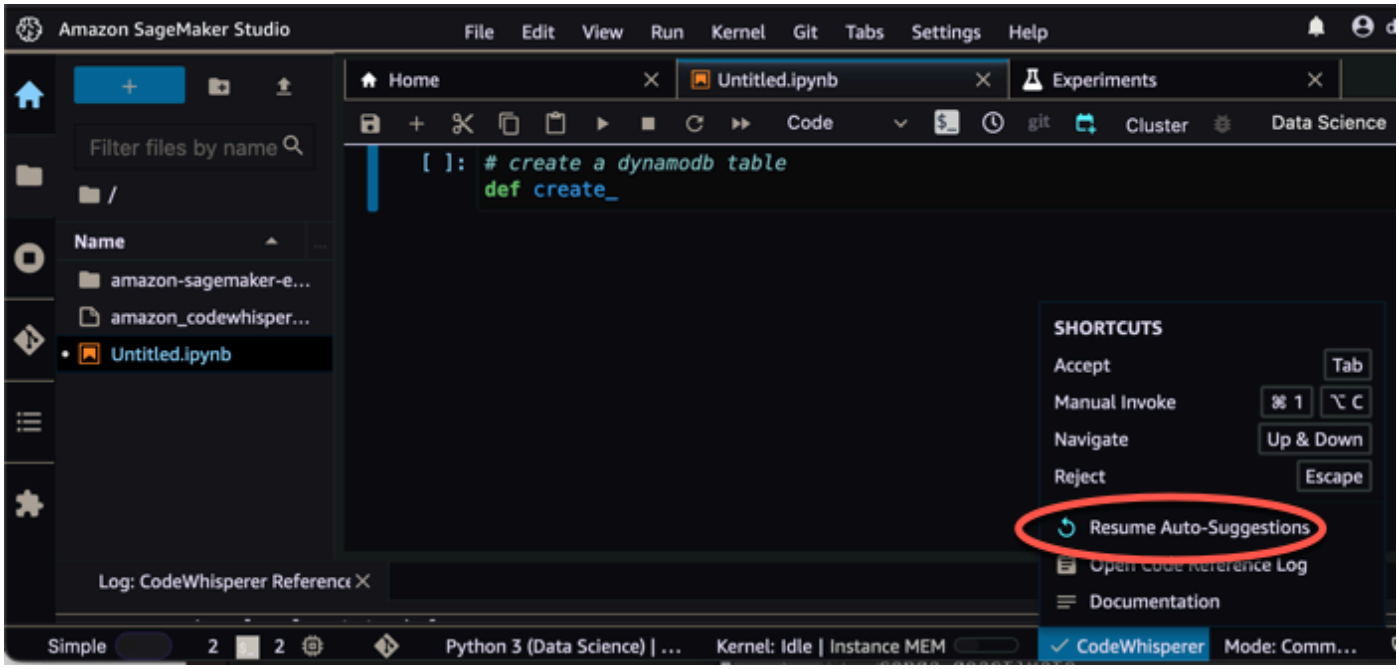
Lambda



Para desactivar o reactivar las sugerencias de CodeWhisperer código en Lambda:

1. En la consola de Lambda, abra la pantalla de una función de Lambda concreta.
2. En la sección Código fuente, en la barra de herramientas, elija Herramientas.
3. En el menú desplegable, selecciona Amazon CodeWhisperer Code Suggestions.

Amazon SageMaker Studio

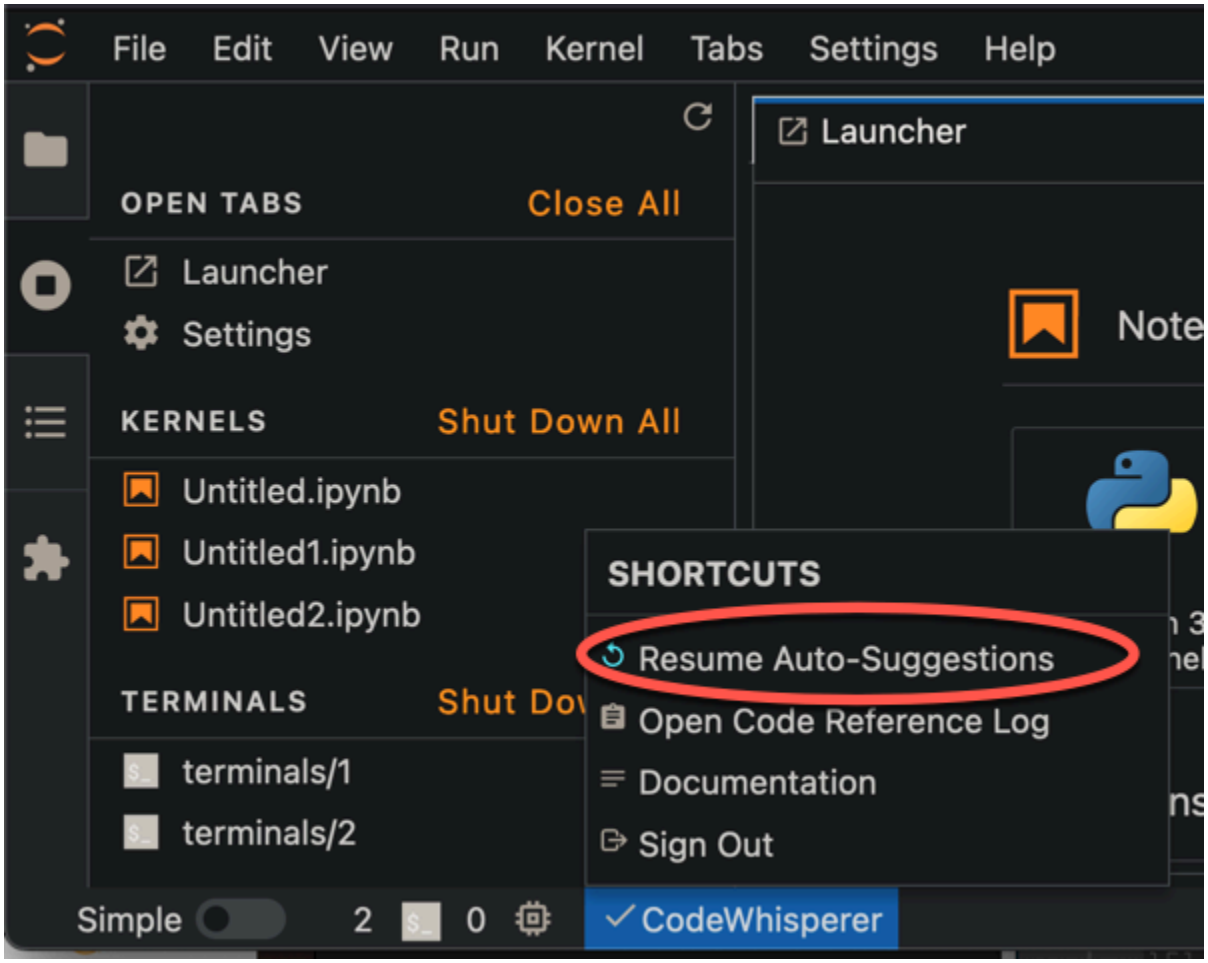


1. En la consola de SageMaker Studio, selecciona CodeWhisperer una opción en la parte inferior de la ventana.

   Se abrirá el CodeWhisperer panel.

2. Elija Pausar las sugerencias automáticas o Reanudar las sugerencias automáticas.

JupyterLab

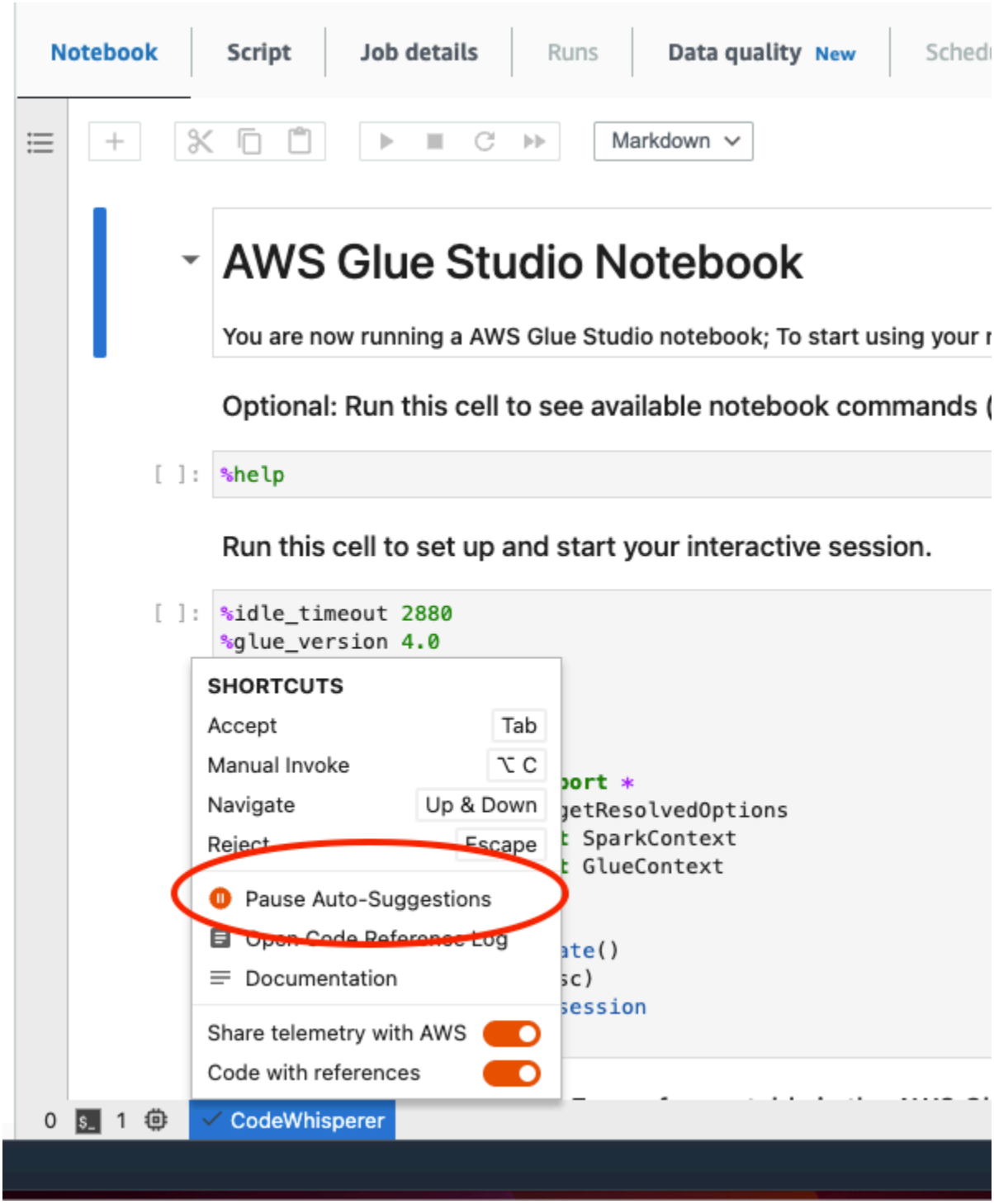


1. En la JupyterLab consola, selecciona CodeWhisperer una opción en la parte inferior de la ventana.

   Se abrirá el CodeWhisperer panel.

2. Elija Pausar las sugerencias automáticas o Reanudar las sugerencias automáticas.

AWS Glue Studio Notebook



1. En la consola de AWS Glue Studio Notebook, selecciona una opción CodeWhisperer en la parte inferior de la ventana.

   Se abrirá el CodeWhisperer panel.

2. Elija Pausar las sugerencias automáticas o Reanudar las sugerencias automáticas.

Análisis de seguridad

Puede utilizarlos CodeWhisperer para detectar infracciones y vulnerabilidades de las políticas de seguridad en su código mediante pruebas estáticas de seguridad de aplicaciones (SAST), detección de secretos y análisis de infraestructura como código (IaC). Los escaneos de seguridad CodeWhisperer identifican las vulnerabilidades de seguridad y sugieren cómo mejorar el código. En algunos casos, CodeWhisperer proporciona código que puede usar para abordar esas vulnerabilidades.

Ejecutar un análisis de seguridad realiza un análisis de seguridad del archivo actualmente activo en el editor IDE y de los archivos dependientes del proyecto. Una vez finalizado el análisis, los problemas de seguridad de los archivos analizados se resaltan en el panel de problemas en VSC. Tenga en cuenta que JetBrains, en el caso de los problemas de seguridad, los problemas de CodeWhisperer seguridad aparecen resaltados en una pestaña independiente del panel de problemas.

Los análisis de seguridad funcionan en el nivel de proyecto, analizan los archivos del proyecto o espacio de trabajo local del usuario y, a continuación, los truncan para crear una carga que se transmita al lado del servidor. Esta carga tiene un límite de tamaño que varía en función del lenguaje de programación.

CodeWhispererSu escáner de seguridad funciona con detectores de la biblioteca de CodeGuru detectores de Amazon. CodeGuruEl departamento de seguridad filtra varios niveles antes de escanear el código para garantizar que puedas centrarte en los problemas más críticos. Como parte de ello, CodeGuru Security filtra los idiomas no compatibles, prueba el código y el código fuente abierto antes de analizarlos para detectar problemas de seguridad.

Temas

- Idiomas con los que funcionan los escaneos de seguridad
- Ejecución de análisis de seguridad
- Límites de datos de análisis de seguridad

Idiomas con los que funcionan los escaneos de seguridad

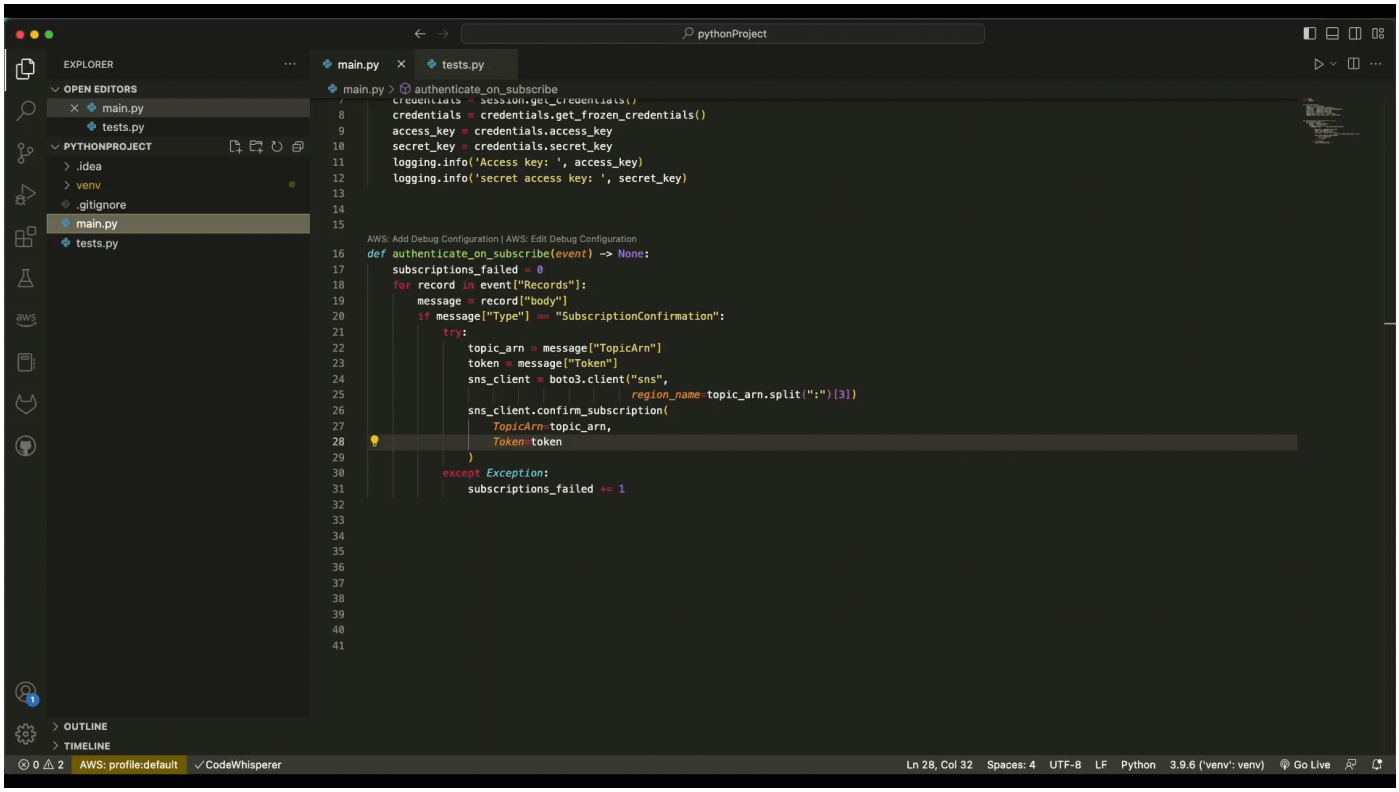
La función CodeWhisperer de escaneo de seguridad es compatible con las siguientes versiones lingüísticas:

- Java - Java 17 y versiones anteriores
- JavaScript - ECMAScript 2021 y versiones anteriores
- Python - Python 3.11 y versiones anteriores, dentro de la serie Python 3
- C# - Todas las versiones (se recomienda .Net 6.0 y versiones posteriores)
- TypeScript - Todas las versiones
- Ruby - Ruby 2.7 y 3.2
- Go - Go 1.18
- Lenguajes de infraestructura como código (IaC)
  - AWS CloudFormation
  - Terraform - 1.6.2 y versiones anteriores
  - AWS CDK - TypeScript y Python

CodeWhisperer solo proporcionará sugerencias de corrección de código para el código escrito en Java, Python o JavaScript,

Ejecución de análisis de seguridad

AWS Toolkit for Visual Studio Code



Para iniciar un análisis de seguridad en VS Code, utilice el siguiente procedimiento.

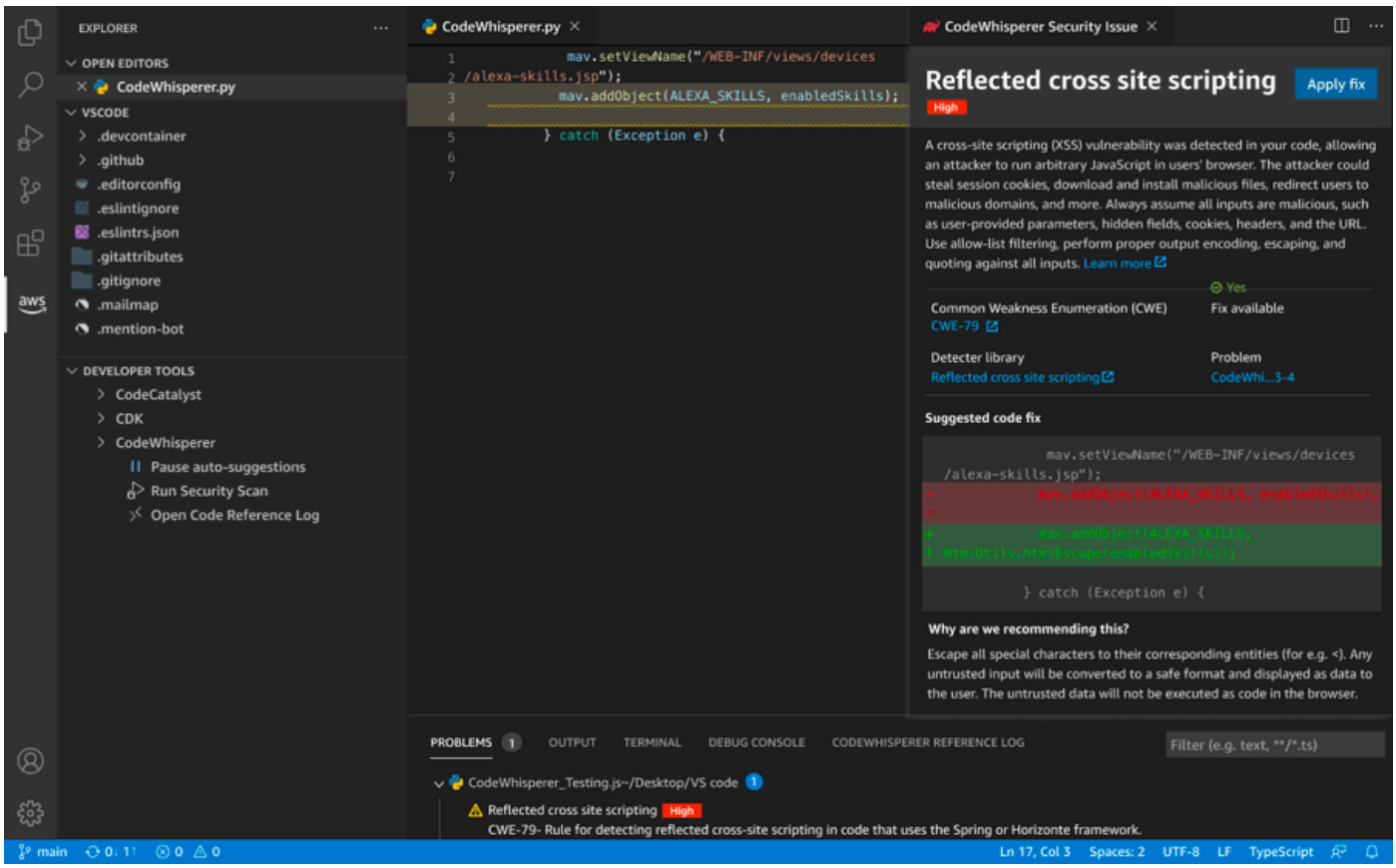
1. En VS Code, elija el AWS logotipo en la parte izquierda de la ventana. Se abrirá el panel del AWS kit de herramientas.
2. En el panel del AWS kit de herramientas, en Herramientas para desarrolladores CodeWhisperer, seleccione Ejecutar un análisis de seguridad.
3. Tras crear un análisis, puede consultar los resultados en la pestaña Problemas.

   Para consultar información sobre el resultado y la solución sugerida, mantenga el cursor sobre el código subrayado.
4. Si el código está escrito en Java, Python o JavaScript, CodeWhisperer podría proporcionar una solución de código sugerida.

   - Si proporciona una solución y quiere implementarla, elija Aplicar corrección. La información sobre el resultado desaparecerá.

- Si no proporciona una solución, actualice el código de acuerdo con la información proporcionada.

  Ejecute otro análisis de seguridad para comprobar que la vulnerabilidad se ha corregido.



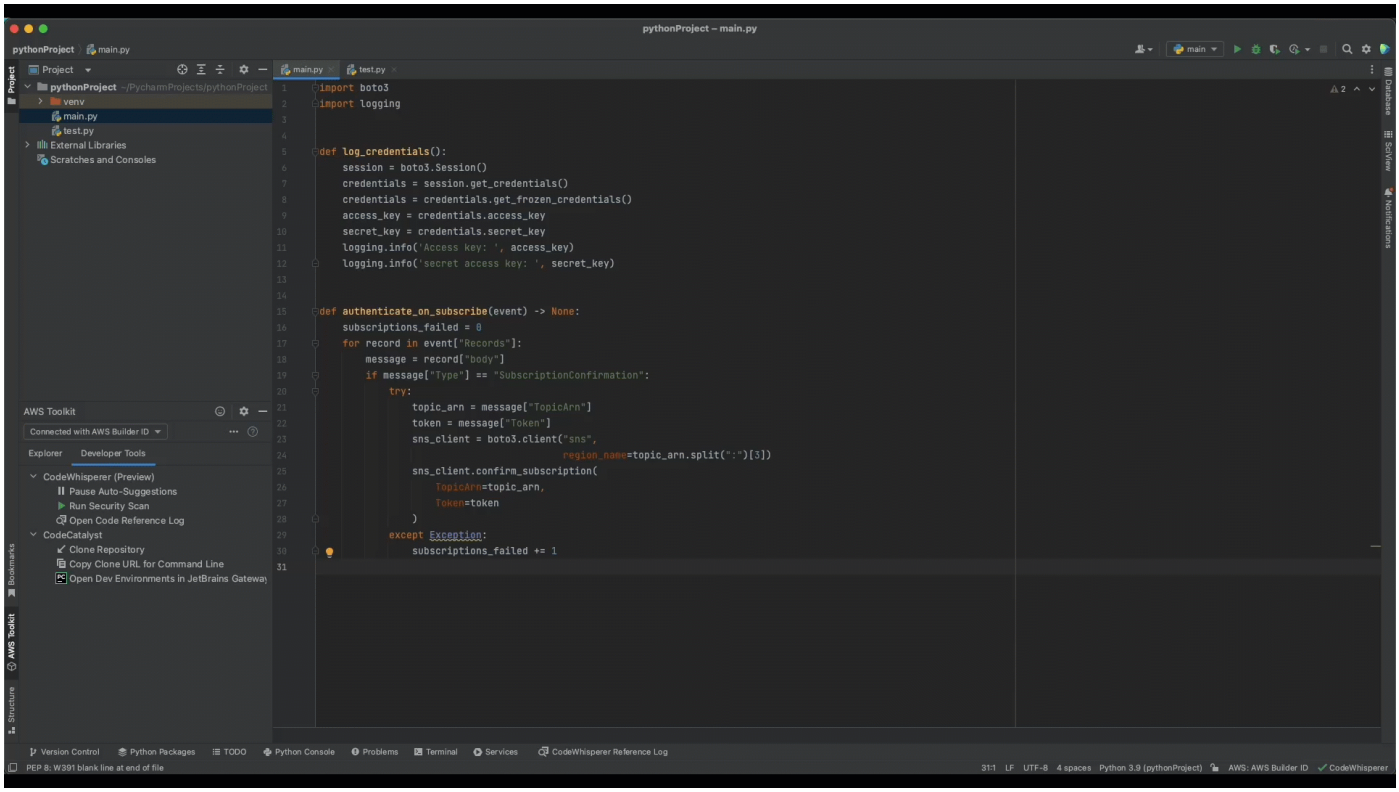
Un análisis puede tardar hasta 60 segundos. Tiene la opción de elegir detener un análisis de seguridad en curso seleccionando Detener el análisis de seguridad. Tenga en cuenta que, una vez iniciado, un análisis se tiene en cuenta para los límites de uso mensuales (por usuario) de los análisis de seguridad. Para obtener más información, consulte Límites de datos de análisis de seguridad.

> **Note**
>
> Si está realizando un análisis de seguridad en un archivo o proyecto de Java, se requieren los artefactos de compilación (archivos .class). Si tiene problemas al analizar el archivo o proyecto Java, compruebe lo siguiente:

1. Asegúrese de que la estructura del proyecto sea válida para el sistema de compilación que está utilizando.
2. Cree su proyecto en VS Code antes de ejecutar un análisis de seguridad para asegurarse de que CodeWhisperer tiene acceso a sus artefactos de compilación.

> **Note**
>
> Si el proyecto se ha creado correctamente en VS Code, pero el análisis de seguridad no funciona y aparece un mensaje de error: `Cannot find build artifacts for the project`, solucione el error especificando la ubicación de los artefactos de compilación en la ruta de salida del compilador.

AWS Toolkit for JetBrains



Para iniciar un análisis de seguridad JetBrains, utilice el siguiente procedimiento.

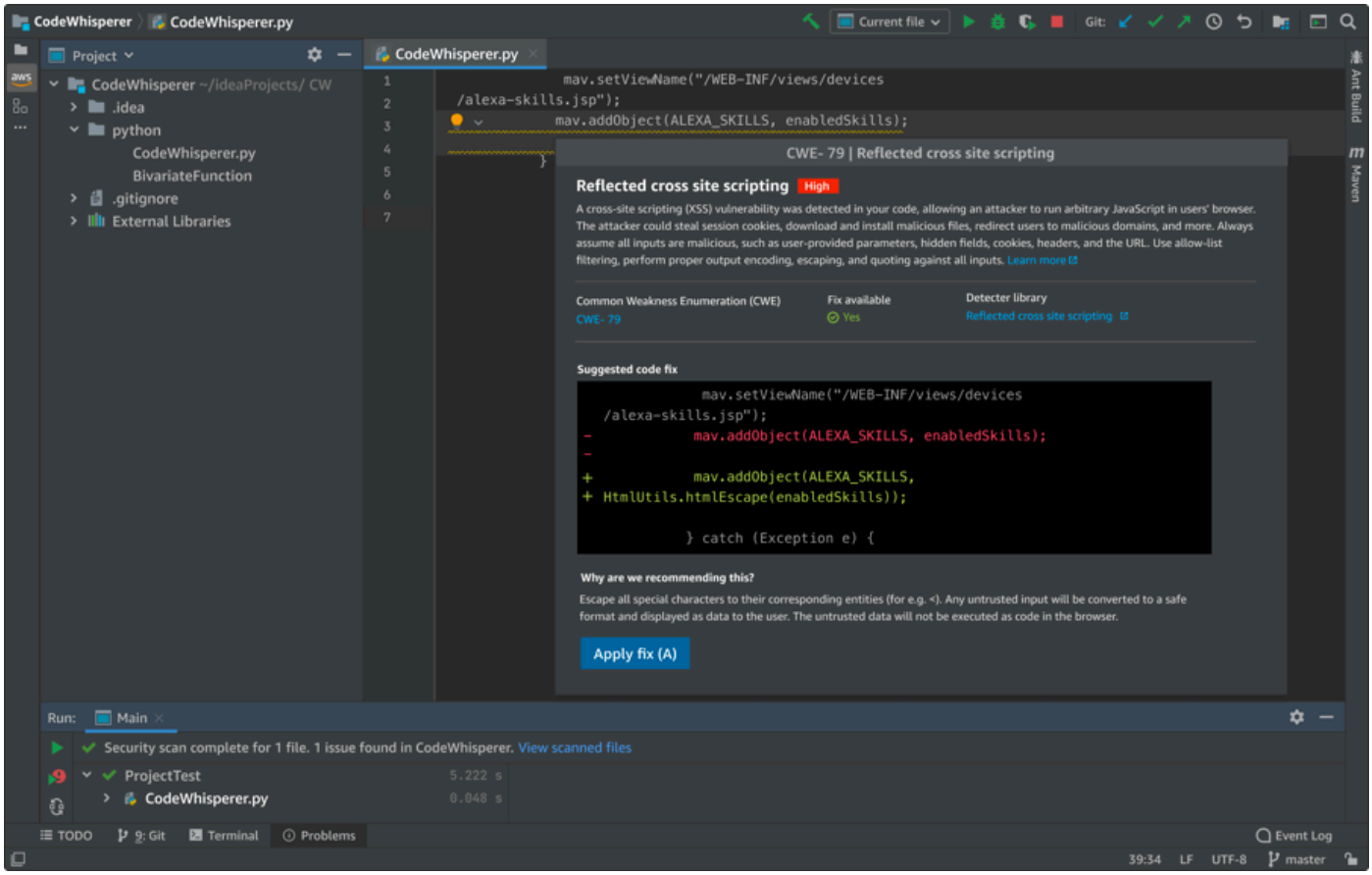
1. En JetBrains, selecciona el AWS logotipo de la parte izquierda de la ventana. Se abrirá el panel del AWS kit de herramientas.

2. En el panel del AWS kit de herramientas, en Herramientas para desarrolladores CodeWhisperer, seleccione Iniciar análisis de seguridad.
3. Tras crear un análisis, puede ver los resultados en la pestaña Problemas de CodeWhisperer seguridad del panel Problemas.

   Para consultar información sobre el resultado y la solución sugerida, mantenga el cursor sobre el código subrayado.
4. CodeWhisperer puede o no proporcionar una solución de código sugerida.

   - Si proporciona una solución y quiere implementarla, elija Aplicar corrección. La información sobre el resultado desaparecerá.
   - Si no proporciona una solución, actualice el código de acuerdo con la información proporcionada.

     Ejecute otro análisis de seguridad para comprobar que la vulnerabilidad se ha corregido.



Un análisis puede tardar hasta 60 segundos. Tiene la opción de elegir detener un análisis de seguridad en curso seleccionando Detener el análisis de seguridad. Tenga en cuenta que, una vez iniciado, un análisis se tiene en cuenta para los límites de uso mensuales (por usuario) de los análisis de seguridad. Para obtener más información, consulte Límites de datos de análisis de seguridad.

> **Note**
>
> Para ejecutar un análisis de seguridad en un archivo o proyecto de Java, se requieren los artefactos de compilación (archivos .class).
>
> 1. Asegúrese de que la estructura del proyecto sea válida para el sistema de compilación que está utilizando.
> 2. Cree su proyecto en IntelliJ antes de ejecutar un análisis de seguridad, para asegurarse de CodeWhisperer que tiene acceso a sus artefactos de construcción.
>
> Si el proyecto se ha creado correctamente en IntelliJ, pero el análisis de seguridad no funciona y aparece un mensaje de error: `Can not find build artifacts for the project`, solucione el error especificando la ubicación de los artefactos de compilación en la ruta de salida del compilador, como se describe a continuación:
>
> 1. En el menú principal de IntelliJ, amplíe Archivo (Windows) o abra Preferencias (Mac).
> 2. Elija Estructura del proyecto para abrir el panel de navegación de la estructura del proyecto.
> 3. Elija Proyecto para abrir el panel Proyecto.
> 4. Ingrese o seleccione la ubicación de los archivos de artefactos del proyecto en el campo de salida del compilador.

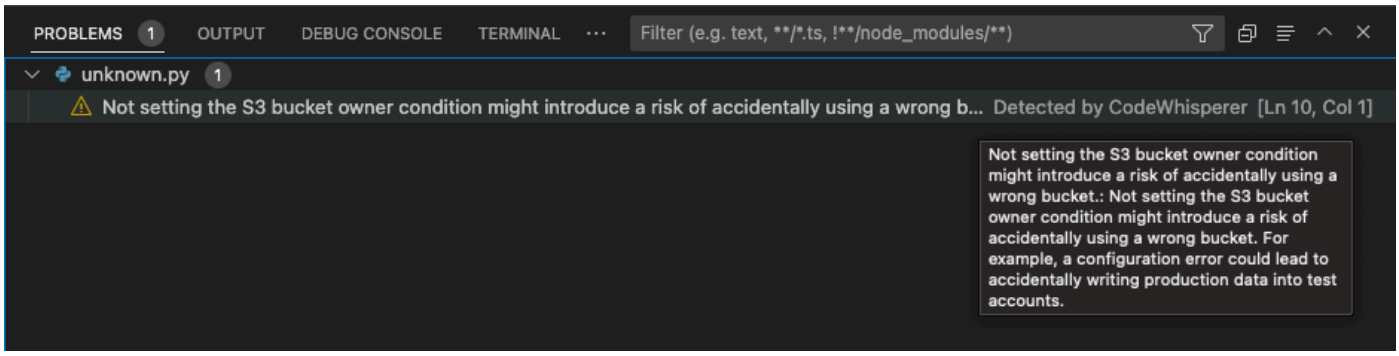
Límites de datos de análisis de seguridad

Cada análisis de seguridad puede incluir más de un archivo. Sin embargo, la cantidad de datos que se pueden analizar cada vez es limitada. Los límites están sujetos a cambios periódicos y también varían según el lenguaje de programación. AWS Si el proyecto supera este límite de datos, no se analizarán todos los archivos. Tras un análisis, puede comprobar el registro para ver los archivos que se analizaron seleccionando Mostrar archivos analizados. Si el archivo que le interesa no se escanea

debido a los límites de datos, ábralo en IDE e inicie otro análisis para asegurarse de que este archivo esté incluido en el análisis.

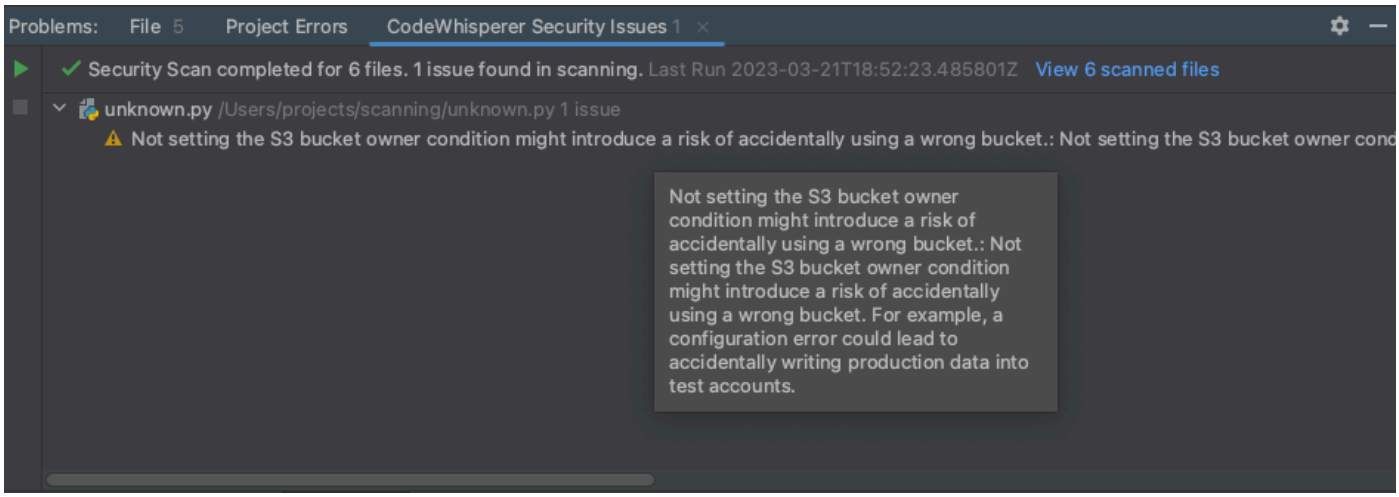
AWS Toolkit for Visual Studio Code

Esta captura de pantalla muestra el aspecto de la lista de archivos analizados en VS Code.



AWS Toolkit for JetBrains

Esta captura de pantalla muestra el aspecto de la lista de archivos escaneados JetBrains.



Referencias de código

Temas

- Visualización de las referencias de código
- Activación y desactivación de las referencias de código
- Desactivación de código con referencias

Visualización de las referencias de código

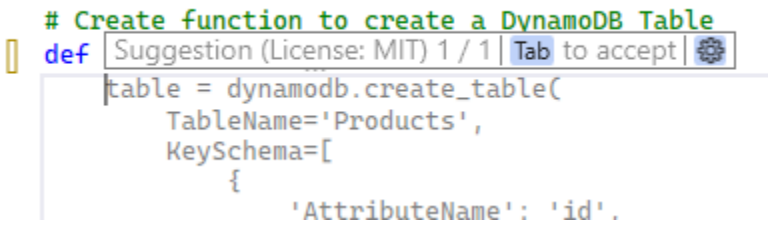
CodeWhisperer aprende, en parte, de proyectos de código abierto. A veces, una sugerencia que está recibiendo puede ser similar a un dato de entrenamiento específico.

Con el registro de referencias, puede ver las referencias a las recomendaciones de código que son similares a los datos de formación. También puede actualizar y editar las recomendaciones de código sugeridas por CodeWhisperer.

En este capítulo se explica cómo ver las referencias de código.

Toolkit for Visual Studio

Cuando CodeWhisperer sugiere código que contiene una referencia en Toolkit for Visual Studio, el tipo de referencia aparece en la descripción de la sugerencia.

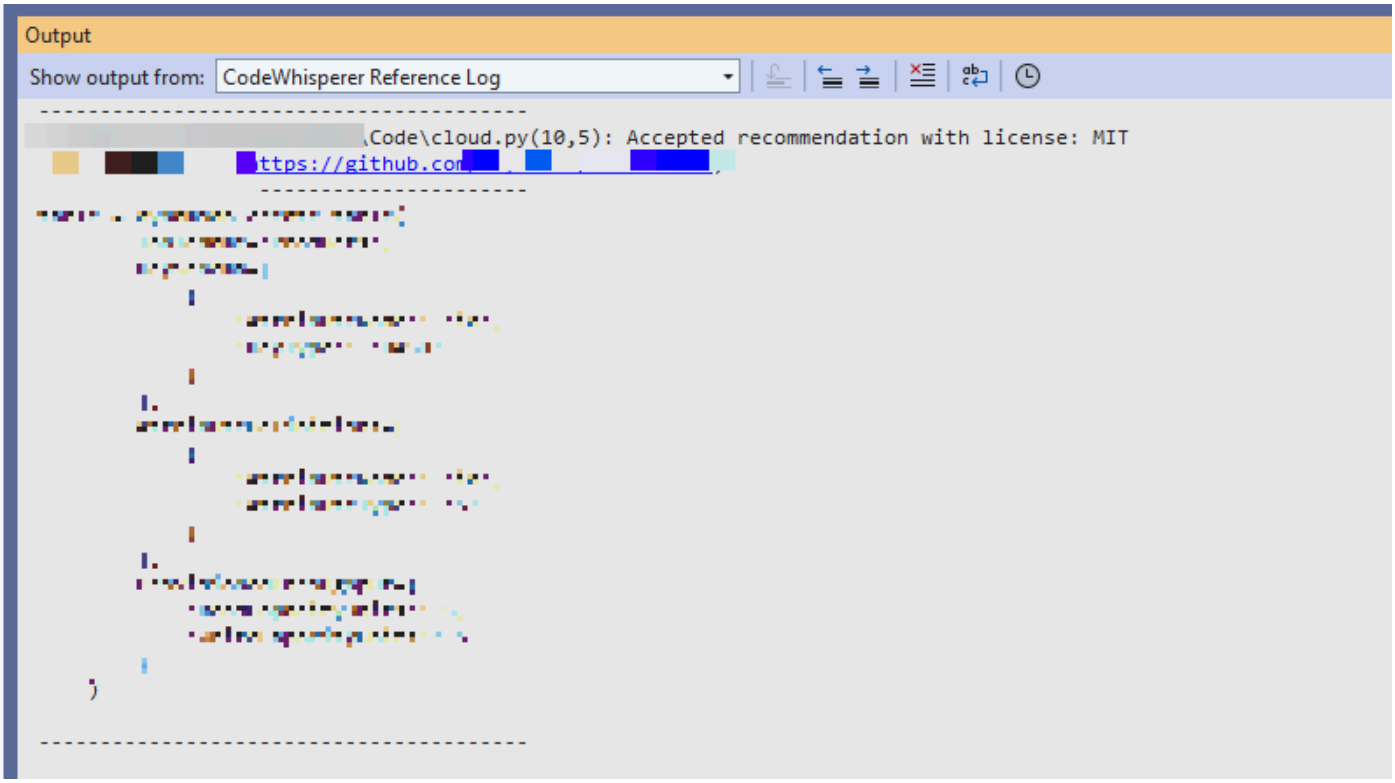


Todas las sugerencias aceptadas que contienen referencias se incluyen en el registro de referencias.

Para acceder al registro de referencia, elija el CodeWhisperer icono y, a continuación, seleccione Abrir registro de referencia de código.

Aparecerá una lista de sugerencias aceptadas que contienen referencias. Esta lista incluye:

- El lugar en el que se aceptó la sugerencia. Al hacer doble clic en ella, accederá a esa ubicación del código.
- La licencia asociada
- El código fuente al que se hace referencia
- El fragmento de código atribuido a la referencia

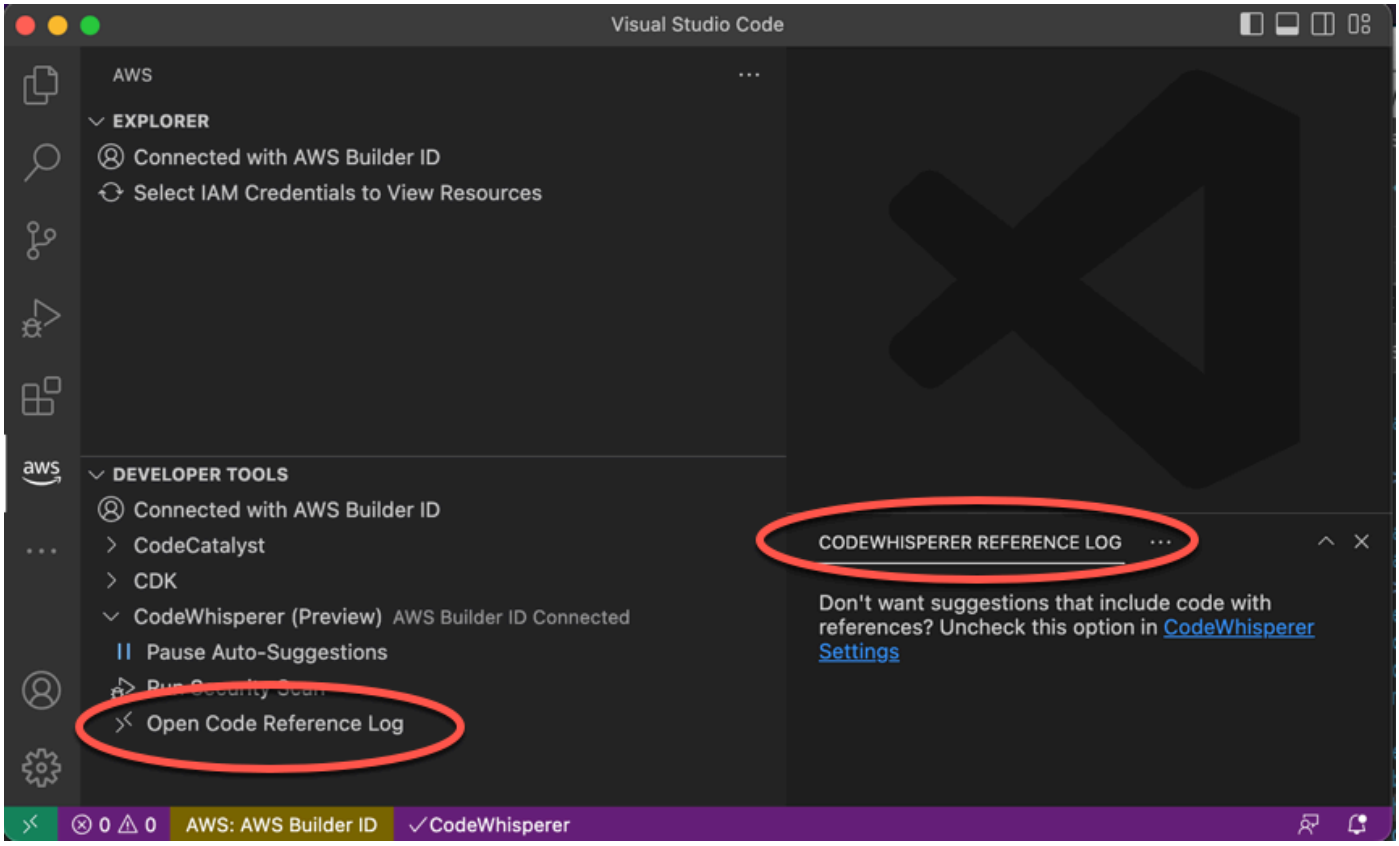


AWS Toolkit for Visual Studio Code

Para mostrar el registro de CodeWhisperer referencia en VS Code, utilice el siguiente procedimiento.

1. Asegúrese de que utiliza la versión más reciente de VS Code y el kit de herramientas de AWS .
2. En VS Code, elija el AWS logotipo en el lado izquierdo de la ventana.
3. Abra el menú desplegable de herramientas para desarrolladores.
4. Elija Abrir registro de referencia de código.

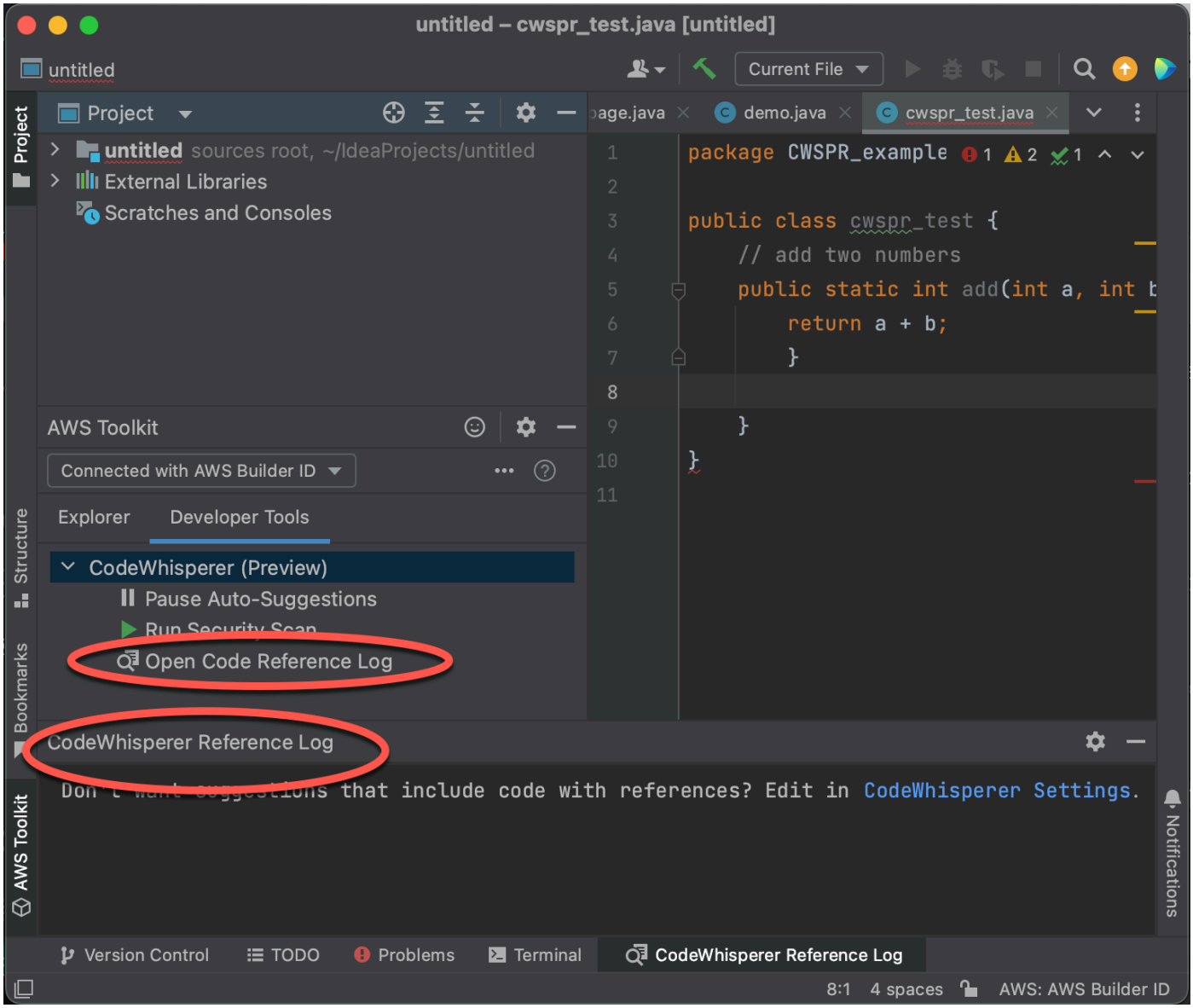
   El registro de referencia de código aparecerá en la parte inferior derecha de la ventana de VS Code.



AWS Toolkit for JetBrains

Para mostrar el registro de CodeWhisperer referencia JetBrains, utilice el siguiente procedimiento.

1. Asegúrese de utilizar la última versión de ambos JetBrains y del AWS kit de herramientas.
2. En la parte izquierda de la JetBrains ventana, selecciona el AWS logotipo.
3. En el panel del AWS kit de herramientas, selecciona la pestaña Herramientas para desarrolladores.
4. En el CodeWhisperer menú desplegable, selecciona Abrir registro de referencia de código.



AWS Cloud 9

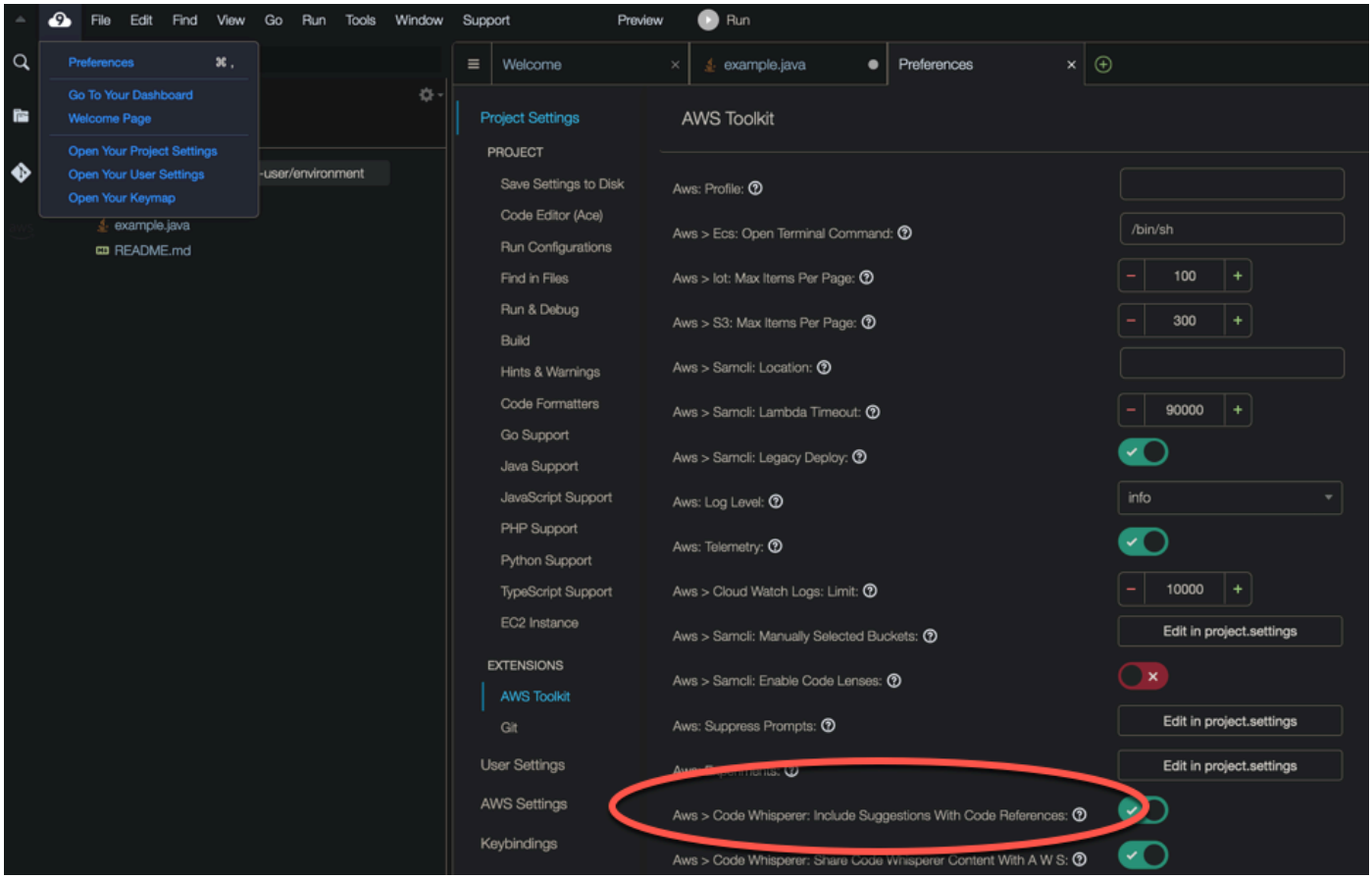
Cuando lo usas CodeWhisperer con AWS Cloud 9, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use el siguiente procedimiento.

1. En la consola de AWS Cloud 9, en la esquina superior izquierda, selecciona el logotipo de AWS Cloud 9.
2. En el menú desplegable, elija Preferencias.

   En el lado derecho de la consola, se abrirá la pestaña Preferencias.

3. En la pestaña Preferencias, en Configuración del proyecto, en Extensiones, seleccione kit de herramientas de AWS .
4. Selecciona o deselecciona CodeWhisperer: Incluye sugerencias con referencias de código.



Lambda

CodeWhisperer en Lambda no admite referencias de código. Cuando se utiliza CodeWhisperer con Lambda, se omiten las sugerencias de código con referencias.

SageMaker Studio

Para mostrar el registro de CodeWhisperer referencias en SageMaker Studio, utilice el siguiente procedimiento.

1. Abre el CodeWhisperer panel en la parte inferior de la ventana de SageMaker Studio.
2. Elija Abrir registro de referencia de código.

JupyterLab

Para mostrar el registro de CodeWhisperer referencia JupyterLab, utilice el siguiente procedimiento.

1. En la parte inferior de la JupyterLab ventana, abra el CodeWhisperer panel.
2. Elija Abrir registro de referencia de código.

AWS Glue Studio Notebook

Para mostrar el registro de CodeWhisperer referencia en AWS Glue Studio Notebook, utilice el siguiente procedimiento.

1. Abre el CodeWhisperer panel en la parte inferior de la ventana de AWS Glue Studio Notebook.
2. Elija Abrir registro de referencia de código.

Activación y desactivación de las referencias de código

Con el registro de referencias, puede ver las referencias a las recomendaciones de código. También puede actualizar y editar las recomendaciones de código sugeridas por CodeWhisperer.

En esta sección, se explica cómo usar las opciones de referencia de código.

AWS Toolkit for Visual Studio Code

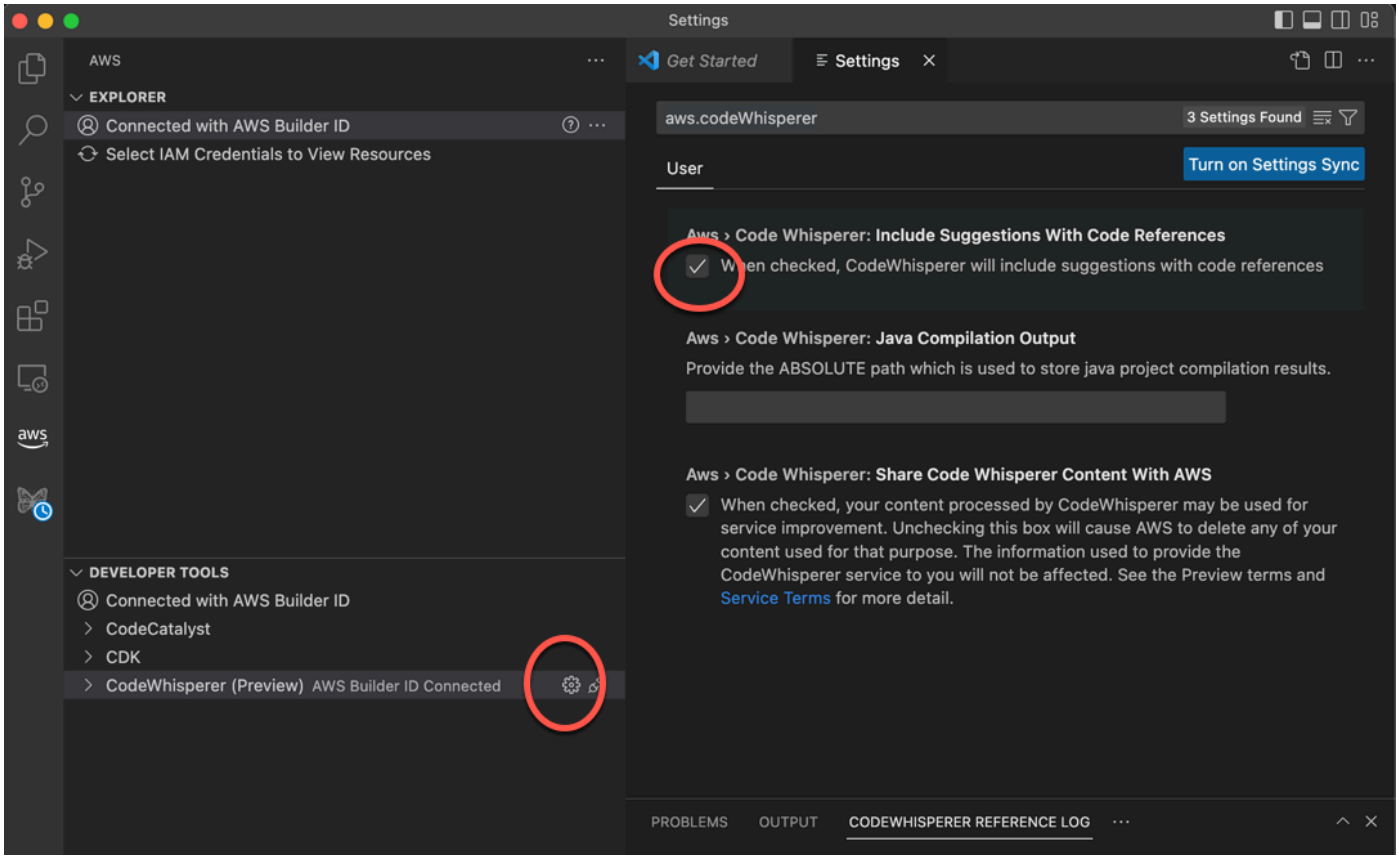
Cuando se usa CodeWhisperer con VS Code, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use los siguientes procedimientos.

1. Asegúrese de que utiliza la versión más reciente de VS Code y el kit de herramientas de AWS .
2. En VS Code, elige el AWS logotipo de la parte izquierda de la ventana.
3. Abra el menú desplegable de herramientas para desarrolladores.
4. Abra el menú desplegable de herramientas para desarrolladores.
5. Junto a la CodeWhispereropción, elige el icono de engranaje.

En un lateral de la ventana de VS Code, se abrirá la pestaña Configuración, donde CodeWhisperer se muestran las opciones relacionadas.

6. Seleccione o anule la selección de la casilla en Incluir sugerencias con referencias de código.



AWS Toolkit for JetBrains

Cuando se utiliza CodeWhisperer con JetBrains, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use los siguientes procedimientos.

1. Asegúrese de utilizar la última versión de ambas JetBrains y del AWS kit de herramientas.
2. En IntelliJ, abra Preferencias.
3. En la ventana de preferencias, en Herramientas, en AWS, seleccione CodeWhisperer.
4. En el CodeWhisperer panel de la derecha, selecciona o desmarca la casilla Incluir sugerencias con referencias de código.

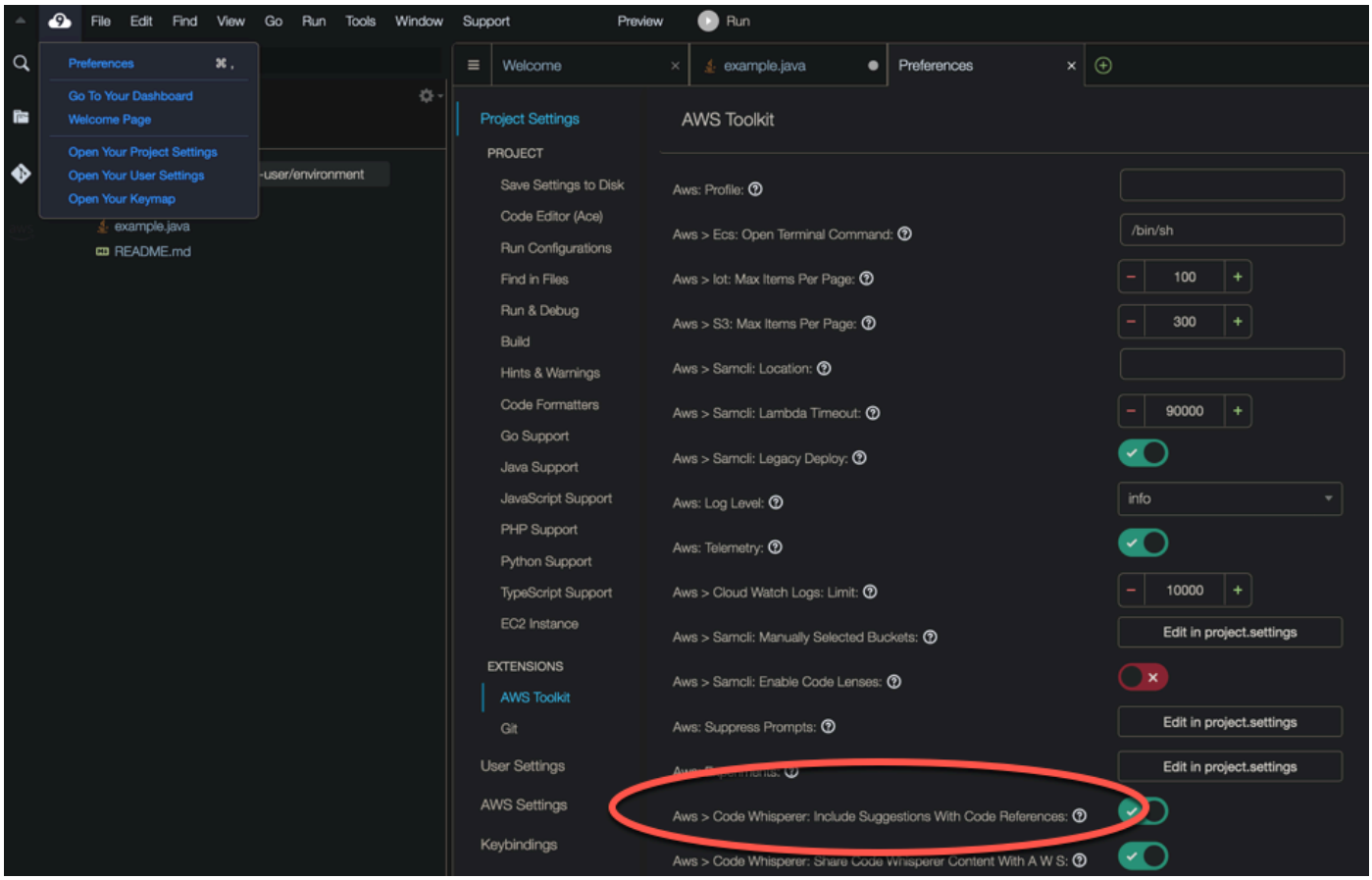
AWS Cloud 9

Cuando lo usas CodeWhisperer con AWS Cloud 9, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use el siguiente procedimiento.

1. En la consola de AWS Cloud 9, en la esquina superior izquierda, selecciona el logotipo de AWS Cloud 9.
2. En el menú desplegable, elija Preferencias.

   En el lado derecho de la consola, se abrirá la pestaña Preferencias.
3. En la pestaña Preferencias, en Configuración del proyecto, en Extensiones, seleccione kit de herramientas de AWS .
4. Selecciona o deselecciona CodeWhisperer: Incluye sugerencias con referencias de código.



Lambda

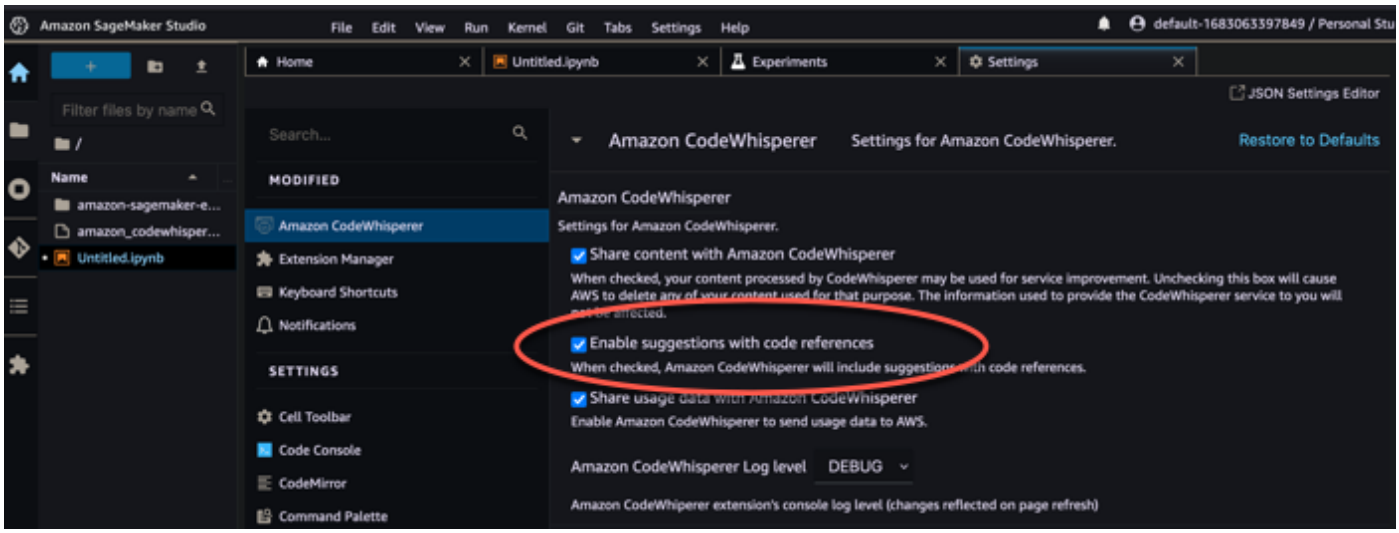
CodeWhisperer en Lambda no admite referencias de código. Cuando se utiliza CodeWhisperer con Lambda, se omiten las sugerencias de código con referencias.

SageMaker Studio

Cuando se usa CodeWhisperer con SageMaker Studio, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use el siguiente procedimiento.

1. En la parte superior de la ventana de SageMaker Studio, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. En el CodeWhisperer menú desplegable de Amazon, selecciona o desmarca la casilla situada junto a Habilitar sugerencias con referencias de código.

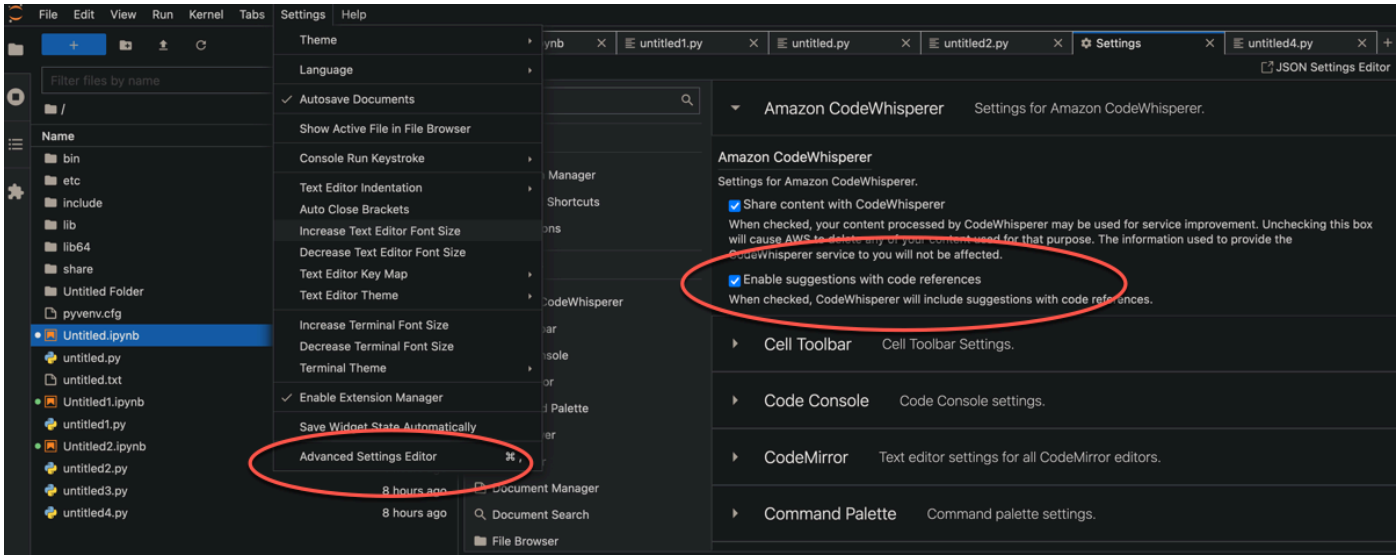


JupyterLab

Cuando se usa CodeWhisperer con JupyterLab, las referencias de código están activadas de forma predeterminada.

Para desactivarlas o volver a activarlas más adelante, use el siguiente procedimiento.

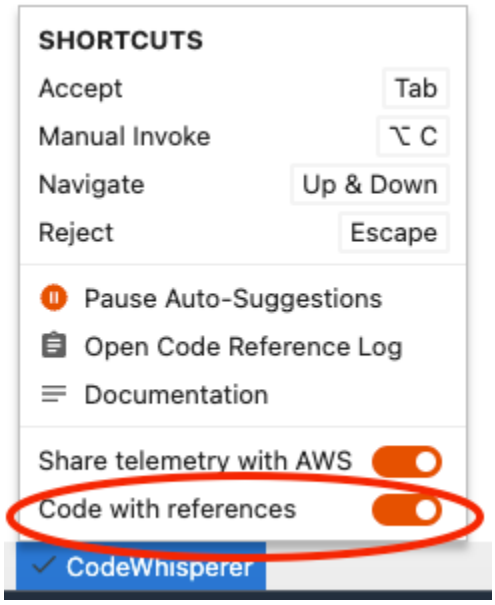
1. En la parte superior de la JupyterLab ventana, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. En el CodeWhisperer menú desplegable de Amazon, selecciona o desmarca la casilla situada junto a Habilitar sugerencias con referencias de código.



AWS Glue Studio Notebook

1. Selecciona la opción situada en la parte inferior de la ventana de AWS Glue Studio Notebook. CodeWhisperer
2. En el menú emergente, active el interruptor situado junto a Código con referencias.

> **Note**
>
> La pausa en las referencias al código solo será válida mientras dure el AWS Glue Studio Notebook actual.



Desactivación de código con referencias

En algunos casos, a nivel empresarial, puede desactivar la recepción de sugerencias con referencias.

En esta sección se explica cómo hacerlo así.

Toolkit for Visual Studio

Puede activar o desactivar las referencias de código en una de las dos formas:

- Elija el CodeWhisperer icono situado en el borde de la ventana y, a continuación, seleccione Opciones...
- Ve a Herramientas -> AWS Kit de herramientas, CodeWhisperer

Luego cambie la opción a Verdadero o Falso, en función de si desea incluir sugerencias con referencias.

AWS Toolkit for Visual Studio Code

Si es administrador de una empresa, puede desactivar las sugerencias con referencias de código para toda la organización. Si lo hace, los desarrolladores individuales de la organización no podrán volver a suscribirse a través del IDE. Esos desarrolladores podrán seleccionar y anular

la selección de la casilla descrita en el procedimiento anterior. Sin embargo, si ha cancelado la suscripción a nivel empresarial, esa acción individual no tendrá ningún efecto.

Para desactivar las sugerencias con referencias a nivel empresarial, utilice el siguiente procedimiento.

1. En la página principal de la CodeWhisperer consola, selecciona Configurar. CodeWhisperer
2. En la página de configuración, en Sugerencias, desactive la casilla etiquetada Incluir sugerencias con referencias de código.
3. En la parte inferior de la ventana de la consola, selecciona Configurar CodeWhisperer.

AWS Toolkit for JetBrains

Si es administrador de una empresa, puede desactivar las sugerencias con referencias de código para toda la organización. Si lo hace, los desarrolladores individuales de la organización no podrán volver a suscribirse a través del IDE. Esos desarrolladores podrán seleccionar y anular la selección de la casilla descrita en el procedimiento anterior. Sin embargo, si ha cancelado la suscripción a nivel empresarial, esa acción individual no tendrá ningún efecto.

Para desactivar las sugerencias con referencias a nivel empresarial, utilice el siguiente procedimiento.

1. En la página principal de la CodeWhisperer consola, selecciona Configurar CodeWhisperer.
2. En la página de configuración, en Sugerencias, desactive la casilla etiquetada Incluir sugerencias con referencias de código.
3. En la parte inferior de la ventana de la consola, selecciona Configurar CodeWhisperer.

AWS Cloud 9

CodeWhisperer in AWS Cloud 9 no admite la exclusión voluntaria de las sugerencias de código con referencias a nivel empresarial.

Para desactivar el nivel de desarrollador individual, consulte Conmutación de las referencias de código.

Lambda

CodeWhisperer en Lambda no admite referencias de código. Cuando se utiliza CodeWhisperer con Lambda, se omiten las sugerencias de código con referencias.

SageMaker Studio

CodeWhisperer no admite la exclusión voluntaria de las sugerencias de código con referencias a nivel empresarial en Studio. SageMaker

JupyterLab

CodeWhisperer no admite la exclusión voluntaria de las sugerencias de código con referencias a nivel empresarial en. JupyterLab

AWS Glue Studio Notebook

CodeWhisperer no admite la exclusión voluntaria de las sugerencias de código con referencias en AWS Glue Studio Notebook.

Tipos de usuarios para CodeWhisperer

Existen varios escenarios en los que puede llegar a utilizarlos CodeWhisperer. Entender en qué se diferencia su situación de la de otros clientes puede ayudarle a entender los problemas relacionados con la autenticación, las opciones de IDE y la facturación. En esta página se explican las diferencias entre los tipos de CodeWhisperer usuarios.

Los desarrolladores de nivel profesional son usuarios que trabajan para una empresa (es decir, una empresa), y es la empresa, no el individuo, con quien tiene una relación financiera. AWS

Usuario root (de una cuenta completa AWS)

El usuario root es el usuario más poderoso de la AWS cuenta. Cuando un cliente configura una AWS cuenta por primera vez, el usuario raíz es el único usuario. Como el usuario raíz es tan poderoso, debería usarse con muy poca frecuencia. El usuario raíz debe crear usuarios administrativos y, a continuación, esos usuarios administrativos deben usarse para la mayoría de las tareas de administración de cuentas.

Administrador del IAM Identity Center

El usuario raíz crea el administrador del IAM Identity Center. El administrador del IAM Identity Center se encarga de agregar usuarios a la cuenta a través del IAM Identity Center. La persona que inicia sesión como administrador del IAM Identity Center puede trabajar en el área de Recursos Humanos. Es posible que no tengan una relación directa con CodeWhisperer. Probablemente también administren usuarios para los mismos profesionales que utilizan AWS servicios distintos de CodeWhisperer. Algunos de los usuarios gestionados por el administrador del Centro de Identidad de IAM, aunque probablemente no todos, pasarán a ser desarrolladores CodeWhisperer profesionales.

CodeWhisperer administrador

El usuario root crea el CodeWhisperer administrador. El CodeWhisperer administrador decide a qué usuarios deben tener acceso CodeWhisperer como desarrolladores profesionales. El grupo de usuarios del que el CodeWhisperer administrador los selecciona es el grupo de usuarios creado por el administrador del Centro de Identidad de IAM. Es posible que el CodeWhisperer administrador no sea un desarrollador y que no se utilice a CodeWhisperer sí mismo en absoluto.

Desarrollador de nivel profesional (con un IDE de terceros)

El administrador del IAM Identity Center agrega al desarrollador de nivel profesional al IAM Identity Center. A continuación, el CodeWhisperer administrador da acceso al desarrollador de nivel profesional a. CodeWhisperer Luego, el desarrollador de nivel profesional utiliza CodeWhisperer el AWS kit de herramientas en VS Code o IDE. JetBrains

Desarrollador de nivel individual (con un IDE de terceros)

El desarrollador de nivel individual no lo usa CodeWhisperer en nombre de un profesional. Por lo tanto, son ellos los que se encargan de su propio acceso. Este desarrollador se autentica con el Builder ID, que no requiere una cuenta. AWS

Desarrollador integrado en la consola

Un desarrollador integrado en la consola usa AWS Cloud 9, Lambda, Sagemaker Studio AWS Glue o Studio CodeWhisperer dentro de la consola. AWS Este desarrollador inicia sesión como un usuario creado en IAM (no en el IAM Identity Center). Normalmente, este desarrollador usa su cuenta personal. AWS El propietario de esta cuenta también puede actuar como el propio administrador. En ese caso, es posible que haya creado él mismo el usuario de IAM para desarrolladores integrado en la consola y haya iniciado sesión como usuario root (no se recomienda) o, como práctica recomendada, un usuario que actúa como administrador general de AWS cuentas.

Ejemplos de código

Temas

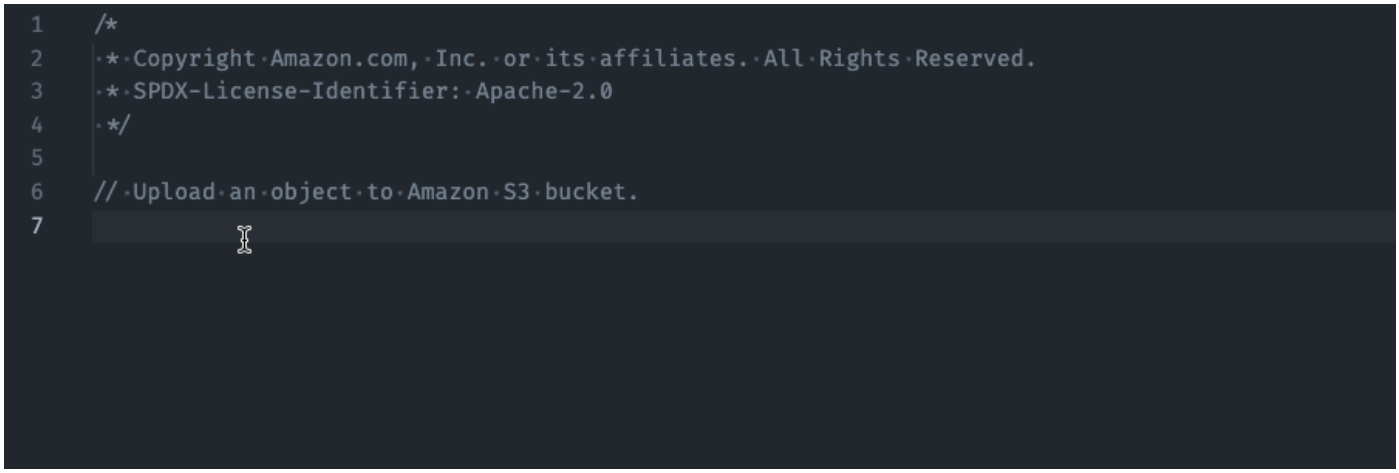
- Finalización de código de línea única
- Generación de funciones completas
- Finalización de bloques
- Finalización de Docstring, JSDoc y Javadoc
- L: recomendaciones ine-by-line

Finalización de código de línea única

Cuando empiezas a escribir líneas de código individuales, CodeWhisperer hace sugerencias basadas en tus entradas actuales y anteriores.

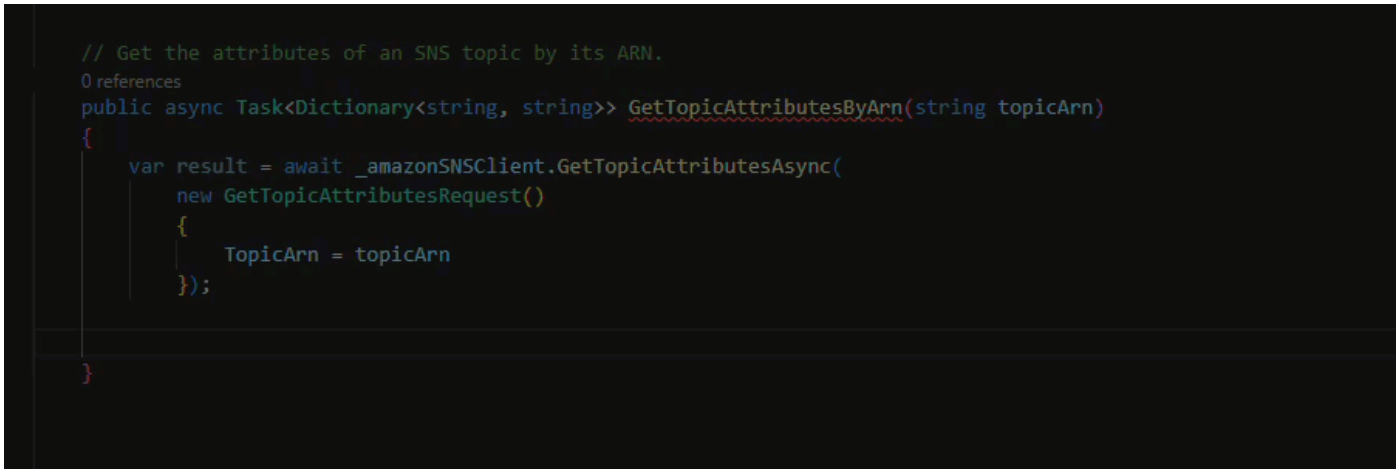
AWS Toolkit for Visual Studio Code

En este ejemplo, al usar JavaScript VS Code, CodeWhisperer se completa una línea de código que comienza el desarrollador.



En este ejemplo, con TypeScript VS Code, el usuario introduce un comentario completo y, a continuación, CodeWhisperer proporciona el código que lo acompaña.

En este ejemplo, CodeWhisperer proporciona una recomendación de una sola línea basada en un comentario, utilizando C# y VS Code.



AWS Toolkit for JetBrains

En la imagen siguiente, utilizando un script de shell escrito en IntelliJ CodeWhisperer , se ofrecen recomendaciones sobre cómo completar una sola línea de código.

Lambda

Cuando empiezas a escribir líneas de código individuales, CodeWhisperer hace sugerencias basadas en tus entradas actuales y anteriores. En la imagen de abajo, un usuario ha empezado a definir una variable para un cliente de Amazon S3. En base a esto CodeWhisperer , sugiere una forma de completar esta línea de código.

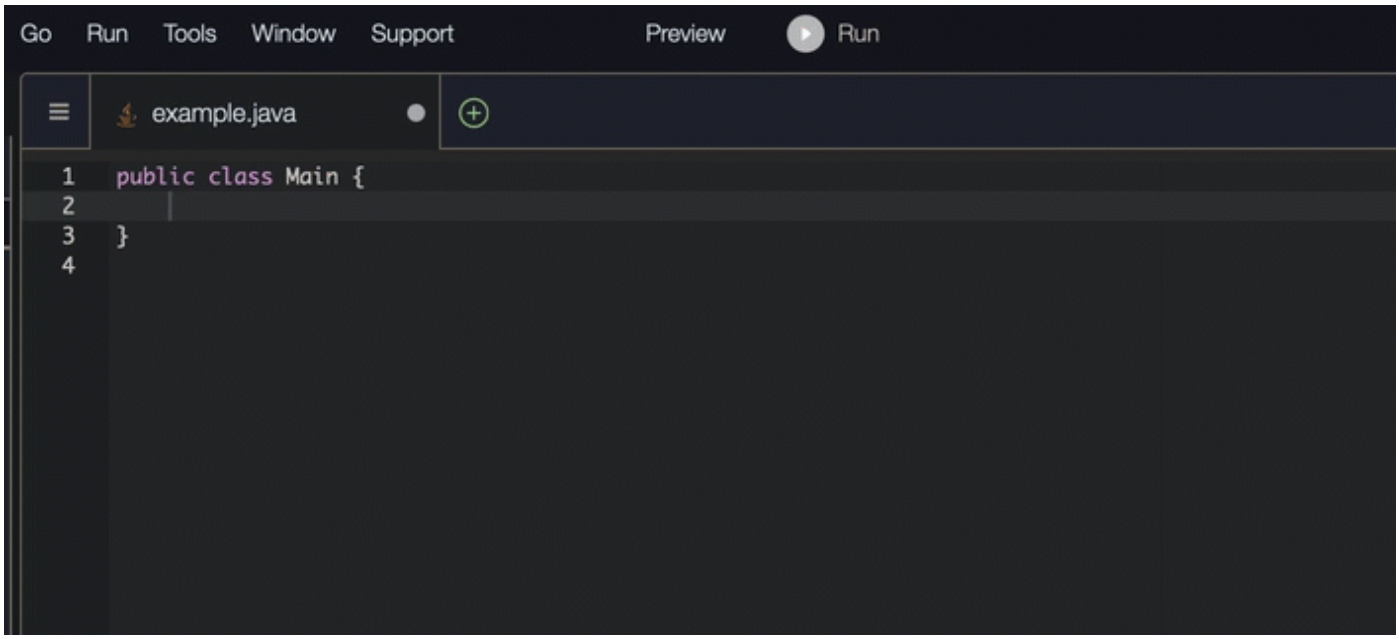
Como otro ejemplo, en la imagen siguiente, un usuario ya ha escrito algún código y ahora quiere enviar un mensaje a una cola de Amazon SQS. CodeWhisperer sugiere una forma de completar esta última línea de código.

AWS Cloud9

Cuando empiece a escribir líneas de código individuales, CodeWhisperer hace sugerencias en función de sus entradas actuales y anteriores.

En el siguiente ejemplo, en Java, un usuario introduce la cadena `public` en una clase existente.

En función de la entrada, CodeWhisperer genera una sugerencia para la firma del método principal.



SageMaker Studio

En este ejemplo, con Python y SageMaker Studio, se CodeWhisperer recomienda una sola línea de código, según el comentario del desarrollador.

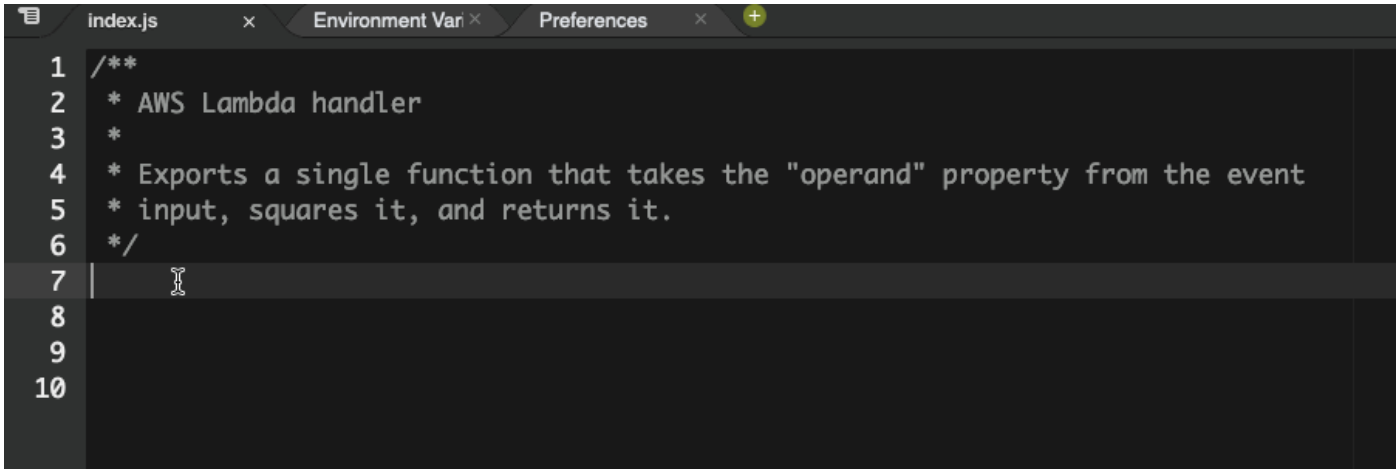
Generación de funciones completas

CodeWhisperer puede generar una función completa a partir de un comentario que hayas escrito. Al terminar, su comentario CodeWhisperer sugerirá una firma de función. Si aceptas la sugerencia, el cursor pasará CodeWhisperer automáticamente a la siguiente parte de la función y realizará

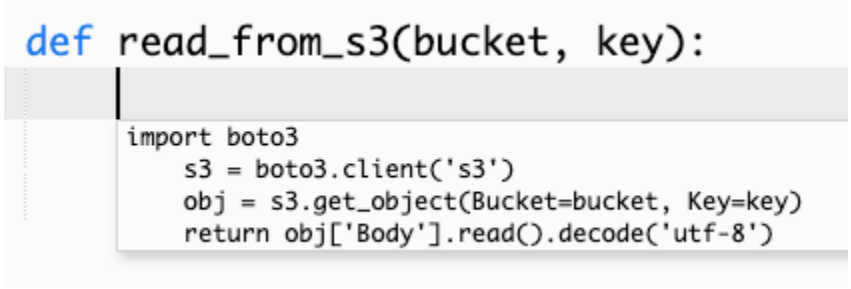
una sugerencia. Aunque introduzcas un comentario o una línea de código adicional entre las sugerencias, CodeWhisperer se refactorizará en función de lo que introduzcas.

Lambda

En el siguiente ejemplo, con JavaScript Lambda, el usuario genera y, a continuación, edita una función completa en función de un conjunto de comentarios.



En la siguiente imagen, un usuario ha escrito una firma de función para leer un archivo de Amazon S3. Amazon sugiere CodeWhisperer entonces una implementación completa del `read_from_s3` método.



> **Note**
>
> A veces, como en el ejemplo anterior, CodeWhisperer incluye `import` declaraciones como parte de sus sugerencias. Como práctica recomendada, mueva manualmente estas declaraciones de `import` en la parte superior de su archivo.

Como otro ejemplo, en la siguiente imagen, un usuario ha escrito una firma de función. CodeWhisperer luego sugiere una implementación completa del `quicksort` método.

```
def quicksort(a):
    if len(a) <= 1:
        return a
    else:
        pivot = a[0]
        less = [i for i in a[1:] if i <= pivot]
        greater = [i for i in a[1:] if i > pivot]
        return quicksort(less) + [pivot] + quicksort(greater)
```

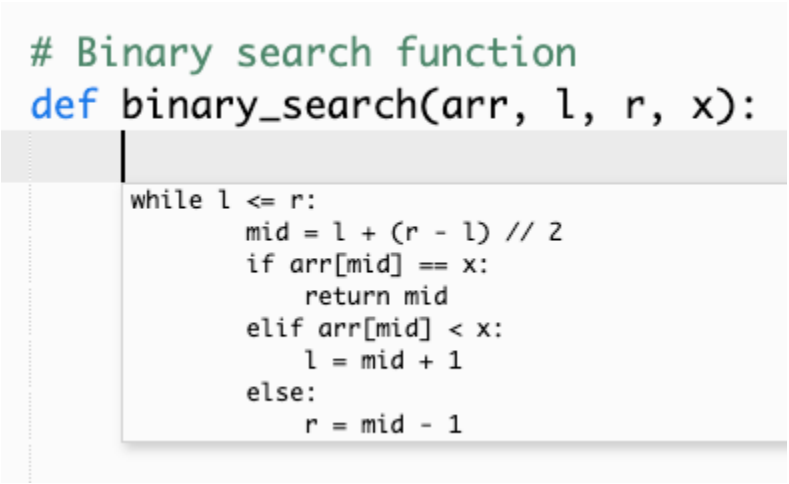
CodeWhisperer tiene en cuenta los fragmentos de código anteriores al hacer sugerencias. En la siguiente imagen, el usuario del ejemplo anterior ha aceptado la implementación sugerida para `quicksort` anterior. A continuación, el usuario escribe otra firma de función para un método genérico`sort`. CodeWhisperer luego sugiere una implementación basada en lo que ya se ha escrito.

```
def quicksort(a):
    if len(a) <= 1:
        return a
    else:
        pivot = a[0]
        less = [i for i in a[1:] if i <= pivot]
        greater = [i for i in a[1:] if i > pivot]
        return quicksort(less) + [pivot] + quicksort(greater)

def sort(a):
    return quicksort(a)
```

En la siguiente imagen, un usuario ha escrito un comentario. Según este comentario, CodeWhisperer sugiere una firma de función.

```
# Binary search function
def binary_search(arr, l, r, x):
```

En la imagen siguiente, el usuario del ejemplo anterior ha aceptado la firma de función sugerida. CodeWhisperer puede entonces sugerir una implementación completa de la `binary_search` función.

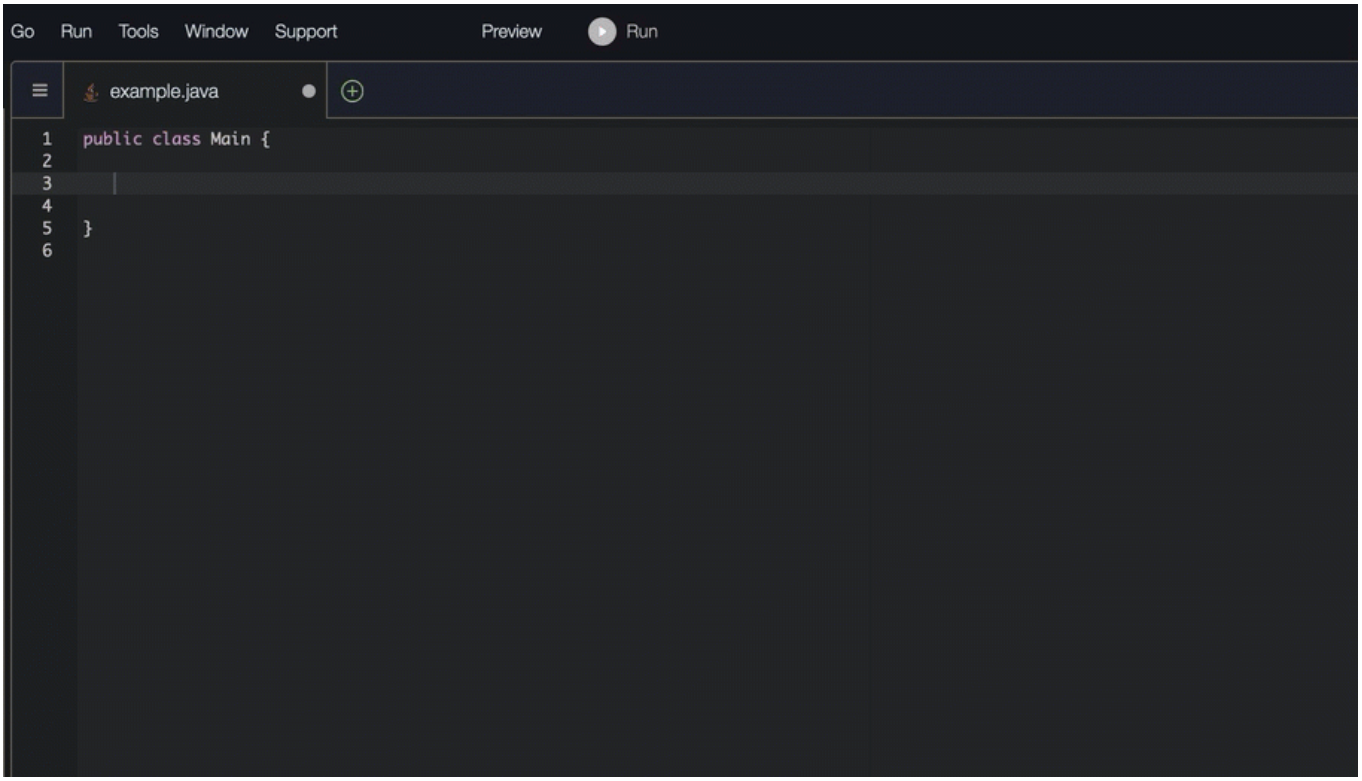


AWS Cloud9

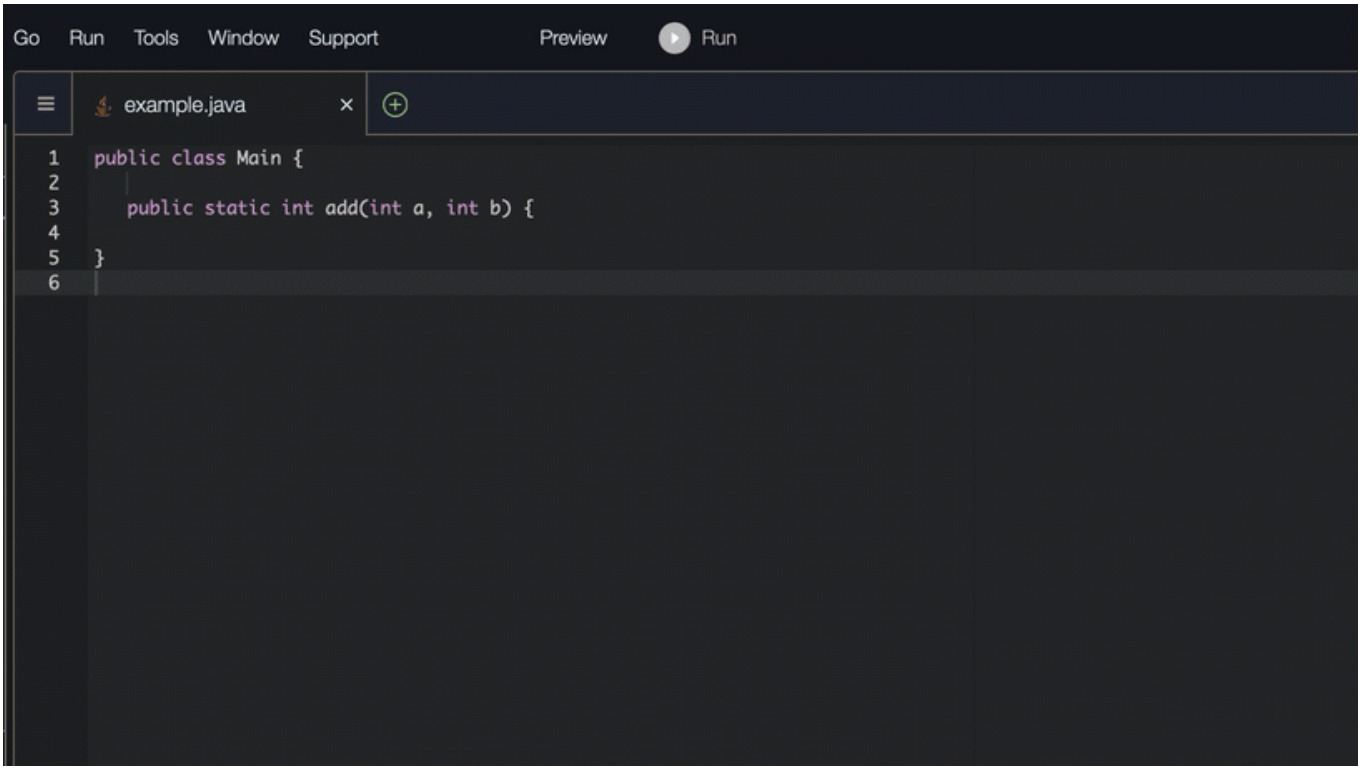
La siguiente lista contiene ejemplos de cómo CodeWhisperer hacer sugerencias y cómo avanzar en todo el proceso de creación de una función.

1. En el siguiente ejemplo, en Java, un usuario introduce un comentario. CodeWhisperer sugiere una firma de función.

   Una vez que el usuario acepta esa sugerencia, CodeWhisperer sugiere el cuerpo de una función.



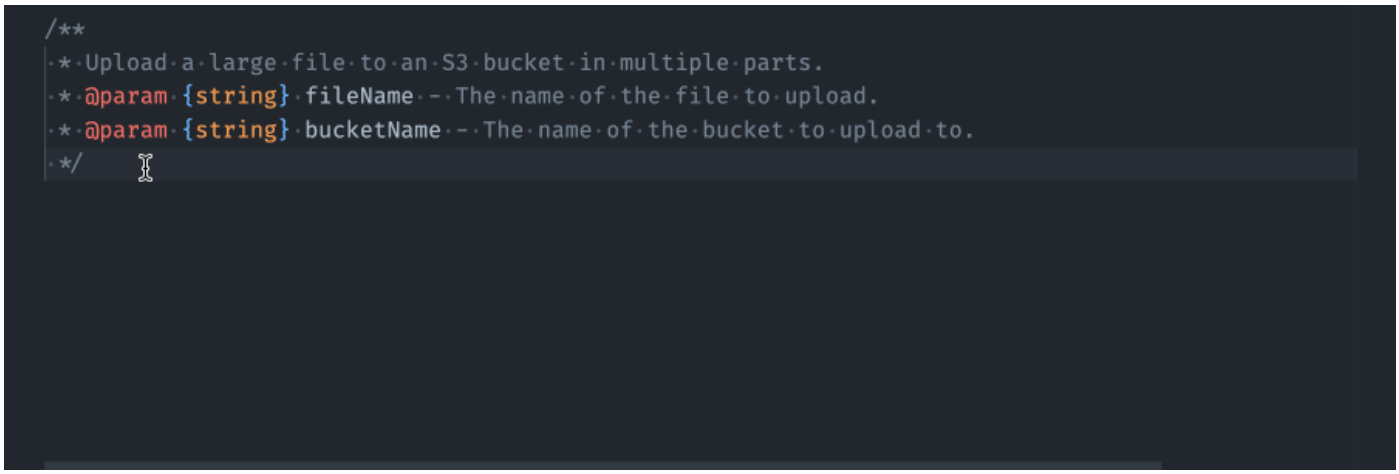
2. En la imagen siguiente, un usuario introduce un comentario en el cuerpo de la función antes de aceptar una sugerencia CodeWhisperer. En la siguiente línea, CodeWhisperer genera una sugerencia basada en el comentario.



AWS Toolkit for Visual Studio Code

En el siguiente ejemplo, con C# y VS Code, se CodeWhisperer recomienda una función completa.

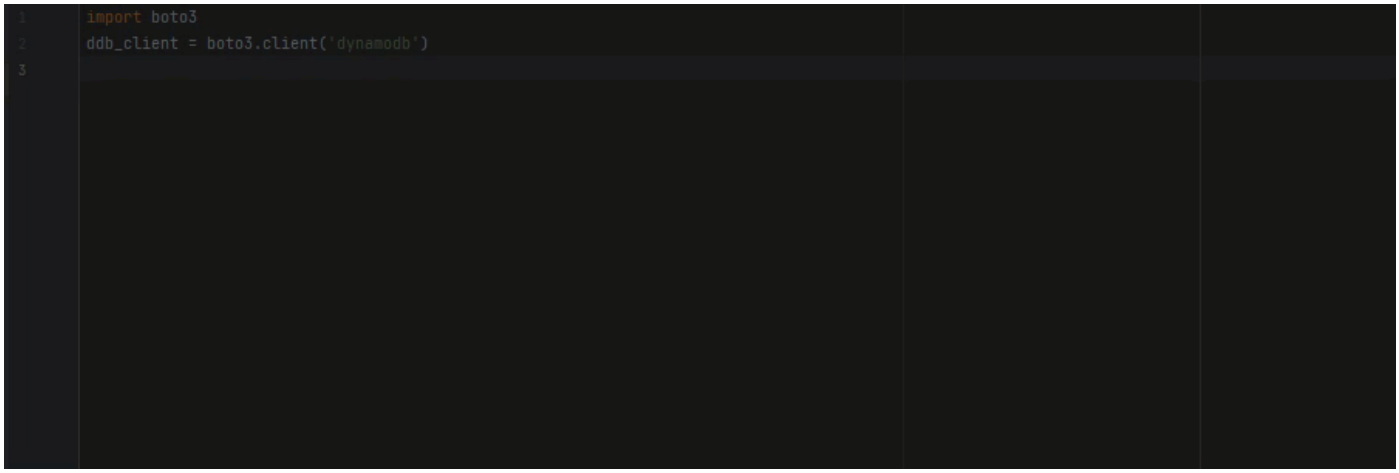
En el siguiente ejemplo, al usar TypeScript VS Code, se CodeWhisperer genera una función basada en las cadenas de documentación del usuario.



AWS Toolkit for JetBrains

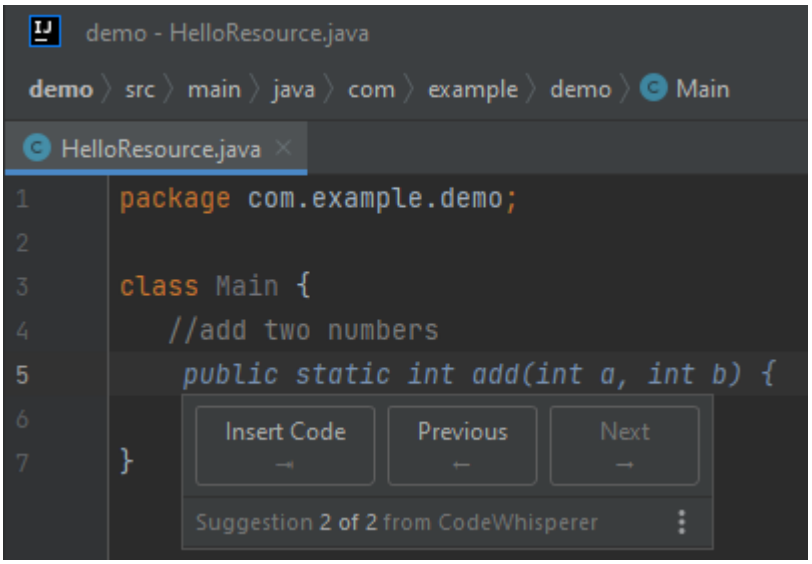
CodeWhisperer puede generar una función completa a partir de un comentario que haya escrito. Cuando termines tu comentario, te CodeWhisperer sugerirá una firma de función. Si aceptas la sugerencia, CodeWhisperer automáticamente pasa el cursor a la siguiente parte de la función y realiza una sugerencia. Aunque introduzcas un comentario o una línea de código adicional entre las sugerencias, CodeWhisperer se refactorizará en función de lo que introduzcas.

En el siguiente ejemplo, al usar Python en Pycharm, se CodeWhisperer genera una función completa y la prueba unitaria correspondiente.



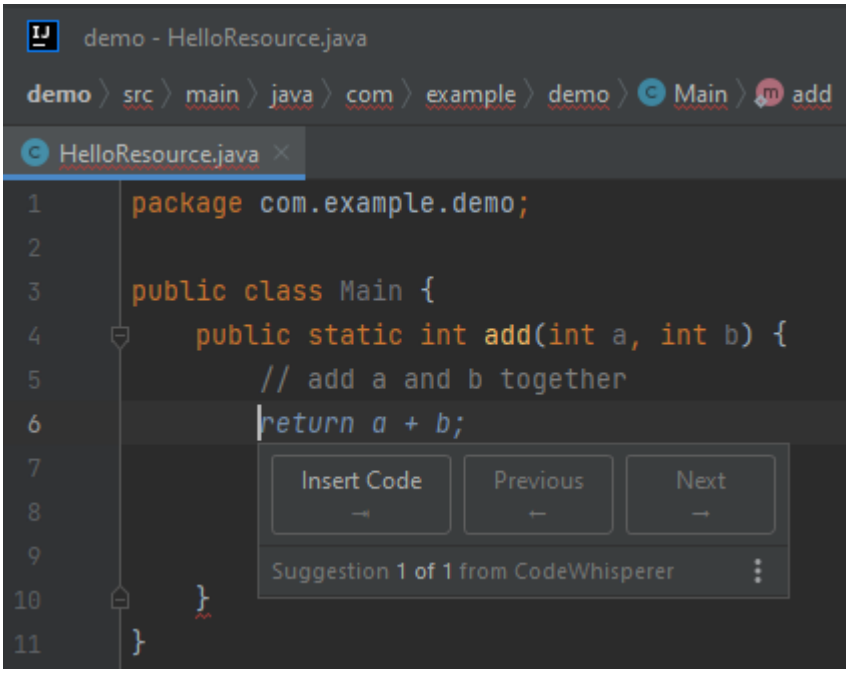
La siguiente lista contiene ejemplos de cómo se CodeWhisperer hacen sugerencias y se avanza a lo largo de todo el proceso de creación de una función.

1. En la siguiente imagen de abajo, un usuario ha escrito un comentario. La firma de la función, situada debajo del comentario, es una sugerencia de CodeWhisperer.



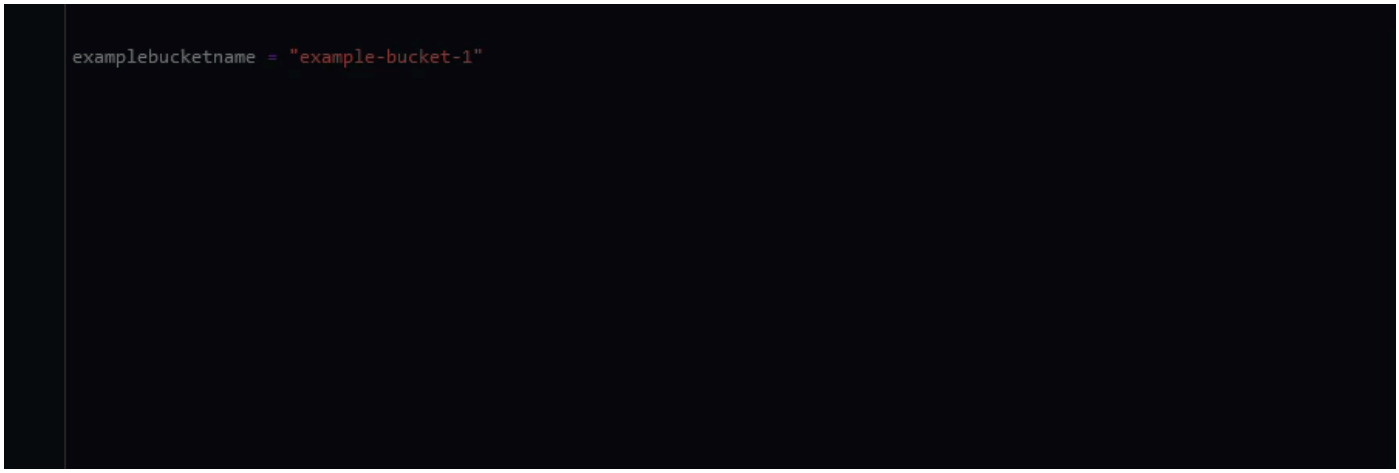
2. En la imagen siguiente, el usuario ha aceptado la CodeWhisperer sugerencia de una firma de función. Al aceptar la sugerencia, el cursor avanzó automáticamente y CodeWhisperer se hizo una nueva sugerencia para el cuerpo de la función.

3. En la siguiente imagen, un usuario introduce un comentario en el cuerpo de la función antes de aceptar una sugerencia CodeWhisperer. En la siguiente línea, CodeWhisperer ha generado una nueva sugerencia basada en el contenido del comentario.



SageMaker Studio

En este ejemplo, con Python y SageMaker Studio, se CodeWhisperer recomienda una función completa después de que el usuario escriba parte de la firma.

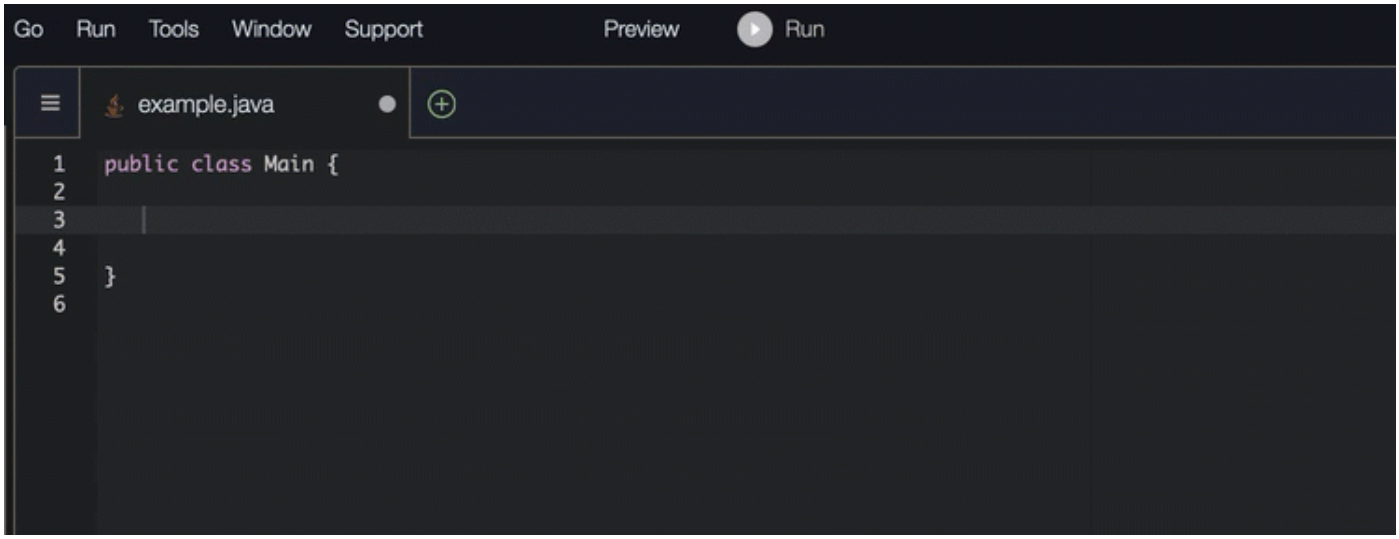


Finalización de bloques

La finalización de bloques se utiliza para completar su bloques de código de `if/for/while/try`.

AWS Cloud9

En el siguiente ejemplo, en Java, un usuario introduce la firma de una instrucción de `if`. El cuerpo de la declaración es una sugerencia de CodeWhisperer.



AWS Toolkit for Visual Studio Code

En la imagen de abajo, utilizando TypeScript VS Code, se CodeWhisperer recomienda una forma de completar la función.

AWS Toolkit for JetBrains

En la imagen de abajo, un usuario ha escrito la firma de una instrucción `if`. El cuerpo de la declaración `System.out.println("negative");` es una sugerencia de CodeWhisperer.

SageMaker Studio

En este ejemplo, con Python y SageMaker Studio, se CodeWhisperer recomienda un bloque de código en función del contexto.

```
examplebucketname = "example-bucket-1"


def print_bucket_contents(bucket_name):
    '''
    Print the contents of a bucket.
    '''
    print(f"Printing bucket contents for bucket {bucket_name}")
    for obj in s3.Bucket(bucket_name).objects.all():
        print(obj)
```

Finalización de Docstring, JSDoc y Javadoc

Visual Studio Code

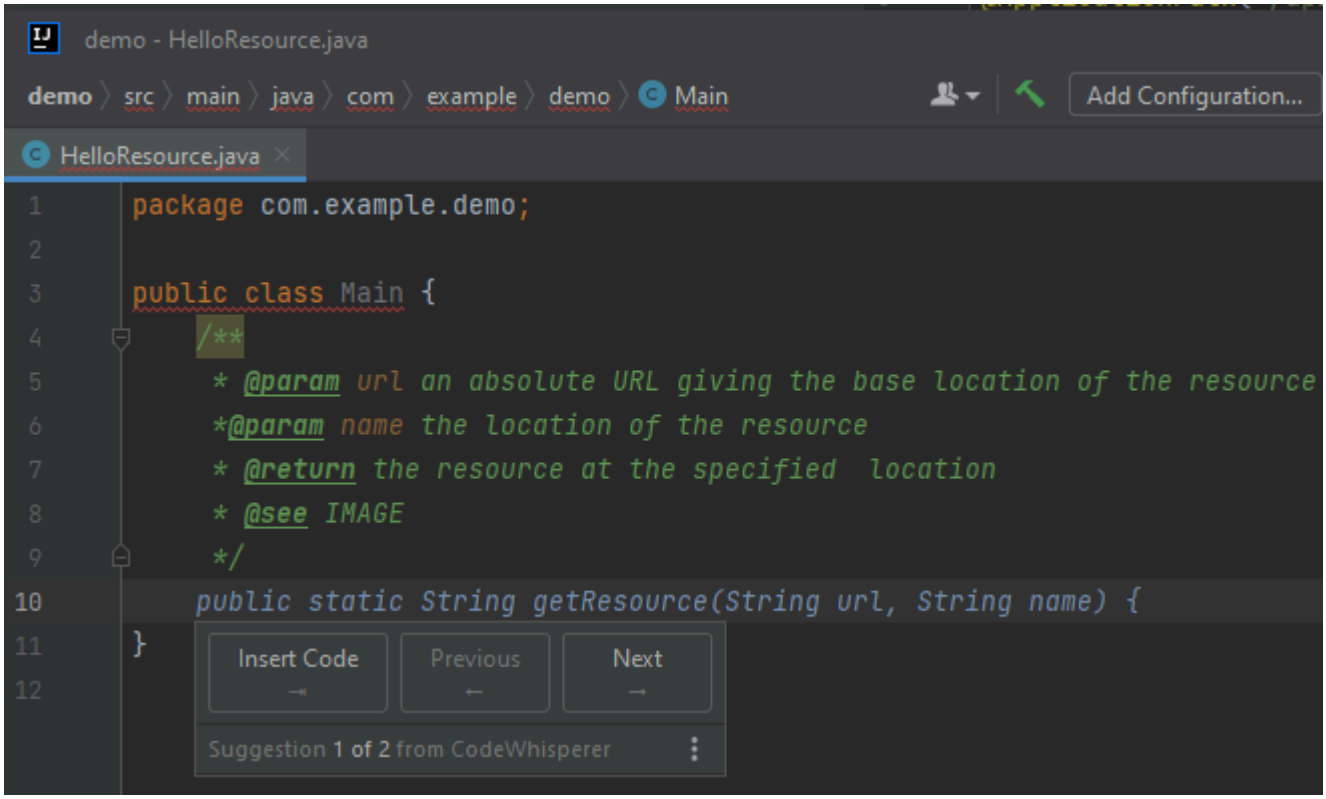
En este ejemplo, si se utiliza Javascript en VS Code, CodeWhisperer se rellenan los parámetros de JSDoc en función de las constantes existentes.

```
import {PutObjectCommand, S3Client} from "@aws-sdk/client-s3";

const client = new S3Client({});

/**
 *
 */
export const putObject = async (bucketName, key, body) => {
  const params = {
    Bucket: bucketName,
    Key: key,
    Body: body,
  };
  return client.send(new PutObjectCommand(params));
```

AWS Toolkit for JetBrains

El siguiente ejemplo es una adaptación de un ejemplo en el sitio web de Oracle.

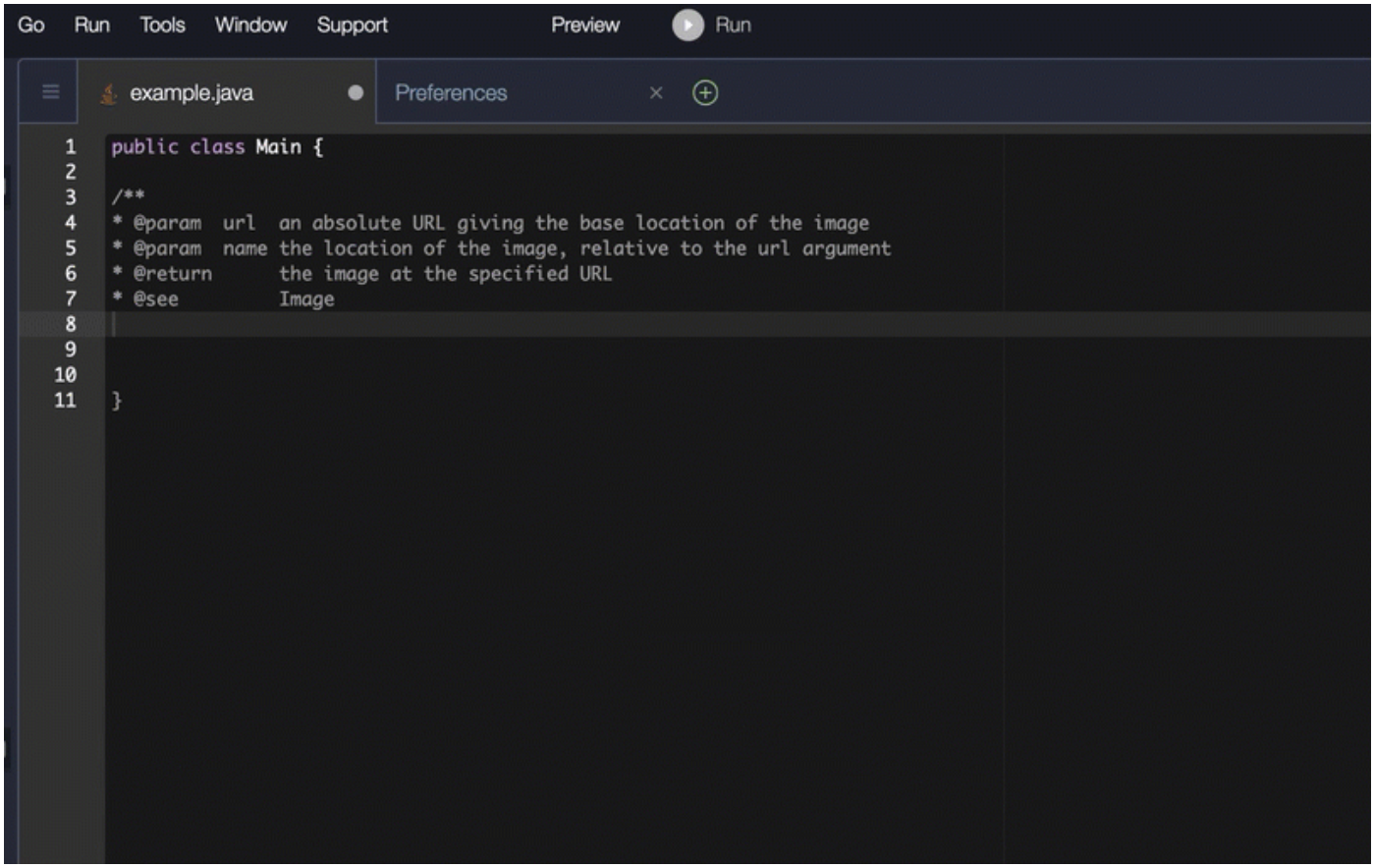
En la imagen siguiente, el usuario ha introducido una cadena de documentos. CodeWhisperer ha sugerido una función para completar la cadena de documentos.



AWS Cloud9

El siguiente ejemplo es una adaptación de un ejemplo en el sitio web de Oracle.

En el siguiente ejemplo, en Java, el usuario introduce una cadena de documentación. CodeWhisperer sugiere una función para procesar la cadena de documentos.



SageMaker Studio

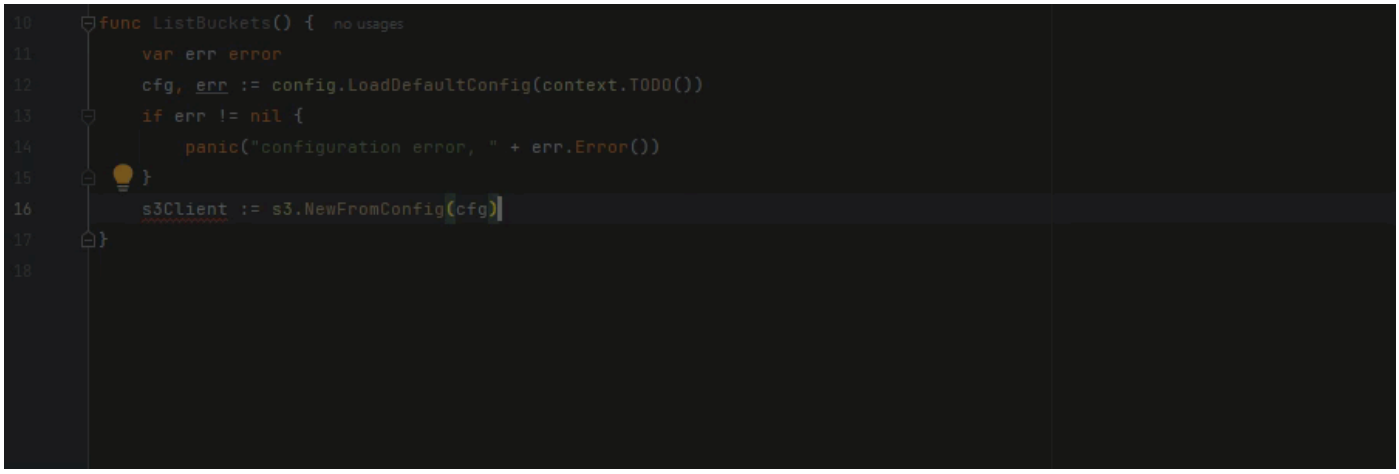
En este ejemplo, con Python y SageMaker Studio, se CodeWhisperer recomienda una cadena de documentos basada en el contexto circundante.

L: recomendaciones ine-by-line

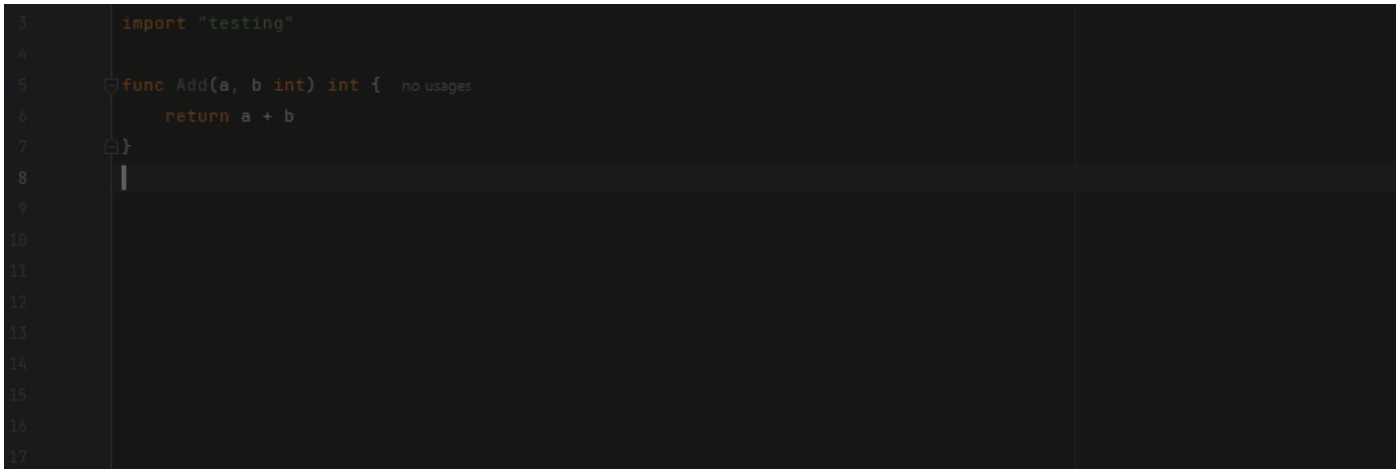
Según su caso de uso, es CodeWhisperer posible que no pueda generar un bloque de funciones completo en una sola recomendación. Sin embargo, aún CodeWhisperer puede proporcionar line-by-line recomendaciones.

JetBrains

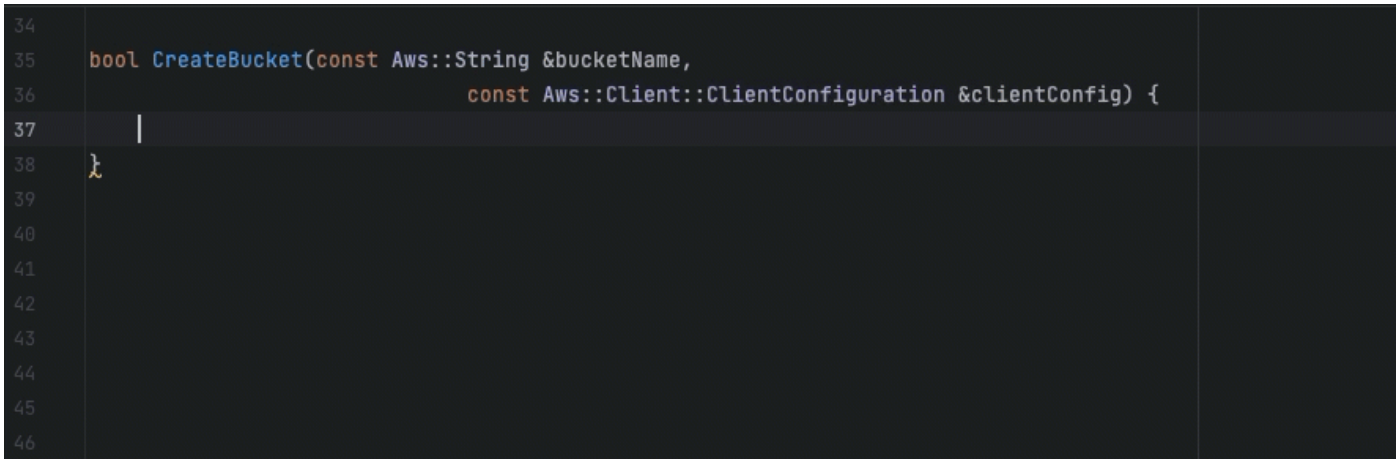
En este ejemplo GoLand, el uso de Go and CodeWhisperer proporciona line-by-line recomendaciones.



Este es otro ejemplo de line-by-line recomendaciones con Go y GoLand, esta vez, con una prueba unitaria.

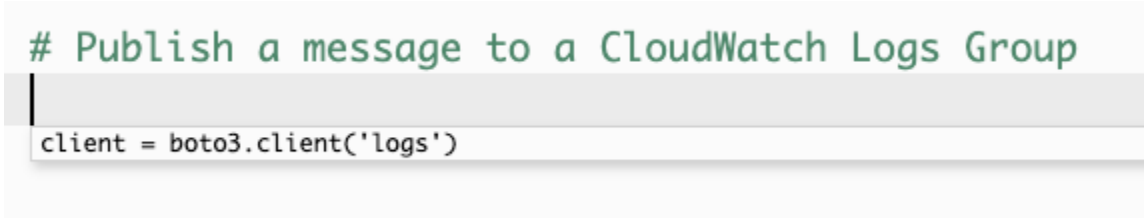


En este ejemplo, CodeWhisperer proporciona line-by-line recomendaciones mediante el uso de C ++ y CLion.

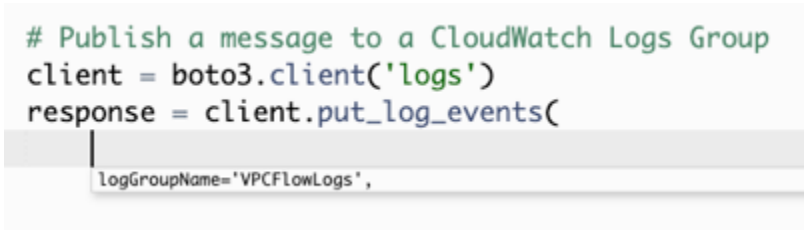


Lambda

En la siguiente imagen, el cliente ha escrito un comentario inicial en el que indica que quiere publicar un mensaje en un grupo de Amazon CloudWatch Logs. Dado este contexto, CodeWhisperer solo puede sugerir el código de inicialización del cliente en su primera recomendación, como se muestra en la siguiente imagen.



Sin embargo, si el usuario sigue solicitando line-by-line recomendaciones, CodeWhisperer también seguirá sugiriendo líneas de código basadas en lo que ya está escrito.



> **Note**
>
> En el ejemplo anterior, `VPCFlowLogs` puede que no sea el valor constante correcto. A medida que CodeWhisperer haga sugerencias, recuerde cambiar el nombre de las constantes según sea necesario.

CodeWhisperer eventualmente puede completar todo el bloque de código, como se muestra en la siguiente imagen.

SageMaker Studio

En este ejemplo, con Python y SageMaker Studio, se CodeWhisperer proporcionan recomendaciones, línea por línea.

Facturación para CodeWhisperer

En esta página se describen los diferentes niveles de CodeWhisperer uso desde el punto de vista de la facturación.

Nivel personal

El nivel personal es gratuito y fácil de configurar, pero no incluye los beneficios de la administración de licencias organizativa.

Si los utilizas CodeWhisperer en el nivel individual, entonces:

- Se usa CodeWhisperer con el AWS kit de herramientas en VS Code o JetBrains, o con JupyterLab.
- Se autentica con el ID del creador.
- Se controla la propia configuración del rastreador de referencias.
- Tiene acceso a la generación de código para todos los lenguajes compatibles.
- De forma predeterminada, compartes datos de fragmentos de código con AWS. Puede desactivar esto en la configuración del IDE.
- De forma predeterminada, compartes los datos de telemetría con. AWS Puede desactivar esto en la configuración del IDE.
- Puede realizar hasta 50 análisis de seguridad al mes.

Nivel profesional

El nivel profesional incluye un cargo por las características adicionales. Su empleador paga la factura a través de la cuenta de su empresa AWS .

> **Note**
>
> La característica de personalizaciones, que se encuentra en versión preliminar, es gratuita actualmente. Los precios estarán disponibles según la disponibilidad general.

El nivel profesional ofrece capacidades administrativas a las organizaciones que desean permitir que sus desarrolladores las utilicen CodeWhisperer. En el nivel profesional, la organización faculta

al CodeWhisperer administrador para gestionar de forma centralizada a qué desarrolladores de la organización deberían tener acceso CodeWhisperer. El CodeWhisperer administrador también establece políticas a nivel organizativo, por ejemplo, si los desarrolladores pueden recibir recomendaciones de código similares a las de los datos de formación de código abierto.

Si lo utilizas CodeWhisperer a nivel profesional, entonces:

- Se usa CodeWhisperer con el AWS kit de herramientas en VS Code o JetBrains.
- Se autentica con las credenciales configuradas por el administrador del Centro de Identidad de IAM de la AWS cuenta de su empresa en el Centro de Identidad de IAM.
- No utilice ID de creador.
- El administrador controla la configuración del rastreador de referencias.
- Tiene acceso a la generación de código para todos los lenguajes compatibles.
- No comparte datos de fragmentos de código con. AWS
- De forma predeterminada, compartes los datos de telemetría con. AWS Puede desactivar esto en la configuración del IDE.
- Puede realizar hasta 500 análisis de seguridad al mes.

Para obtener información detallada sobre los precios, consulta la página de CodeWhisperer precios.

> **Note**
>
> Incluso si el mismo usuario actúa como CodeWhisperer desarrollador en dos cuentas diferentes de la misma organización, a tu organización solo se le facturará por ese usuario una vez por ciclo de facturación.

Facturación correspondiente a CodeWhisperer cuando se utiliza con servicios incluidos en la consola AWS

Los siguientes servicios funcionan CodeWhisperer desde dentro de la AWS consola (a diferencia de un IDE de terceros):

- AWS Cloud9
- AWS Lambda

- SageMaker Estudio
- AWS Glue Estudio

Si utilizas alguno CodeWhisperer de esos servicios, entonces:

- No lo está utilizando CodeWhisperer con el AWS kit de herramientas ni en VS Code ni JetBrains.
- Para autenticarse, inicie sesión directamente en la AWS consola con las credenciales de IAM configuradas por el administrador del IAM Identity Center de la AWS cuenta de su empresa. (Si utiliza una AWS cuenta personal, puede configurar esas credenciales usted mismo).
- No utilice ID de creador.
- Su uso no conlleva ningún cargo adicional CodeWhisperer.
- No puede ejecutar escaneos de seguridad CodeWhisperer relacionados desde dentro AWS Cloud9 de Lambda, SageMaker Studio o AWS Glue Studio Notebook.

Facturación de las personalizaciones CodeWhisperer

En el nivel profesional, los usuarios pueden aprovechar la nueva capacidad de CodeWhisperer personalización (en versión preliminar), que permite a las organizaciones personalizar CodeWhisperer para generar recomendaciones más relevantes al conocer las bibliotecas, las API, las clases o los métodos internos de la organización.

Durante la vista previa, puede usar la capacidad de personalización para crear hasta ocho personalizaciones basadas en las bases de código internas. Pueden mantener activas hasta dos personalizaciones de código al mismo tiempo, de forma gratuita. Los precios estarán disponibles según la disponibilidad general

Supervisión de Amazon CodeWhisperer

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon CodeWhisperer y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de monitoreo para observar CodeWhisperer, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puedes CloudWatch hacer un seguimiento del número de veces que se CodeWhisperer ha invocado en tu cuenta o del número de usuarios activos a diario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

  > **Note**
  >
  > CloudWatch no se puede usar para monitorear la actividad en el nivel individual, ya que no requiere una AWS cuenta.

Monitorización CodeWhisperer con Amazon CloudWatch

Puede monitorizar el CodeWhisperer uso CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se guardan durante 15 meses, para que pueda acceder a la información histórica y obtener una mejor perspectiva de CodeWhisperer su rendimiento. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El CodeWhisperer servicio informa de las siguientes métricas en el espacio de `AWS/CodeWhisperer` nombres.

Dimensiones	Métrica	Caso de uso o explicación
Recuento	Invocaciones	Desea determinar cuántas invocaciones se han contado a lo largo del tiempo.
UserCount	DailyActiveUserTrend	Desea determinar la cantidad de usuarios activos por día.
SubscriptionUserCount	SubscriptionCount	Desea determinar el número de usuarios con suscripciones de pago.
UniqueUserCount	MonthlyActiveUniqueUsers	Desea determinar el número de usuarios que están activos en un mes determinado.
ProgrammingLanguage, SuggestionState, CompletionType	GeneratedLineCount	Desea determinar el número de líneas generadas por. CodeWhisperer
ProgrammingLanguage, SuggestionState, CompletionType	SuggestionReferenceCount	Desea determinar el número de recomendaciones desencadenadas con las referencias que se han realizado.
ProgrammingLanguage	CodeScanCount	Desea determinar el número de análisis de código que se han realizado.

Dimensiones	Métrica	Caso de uso o explicación
ProgrammingLanguage	TotalCharacterCount	El número de caracteres del archivo, incluidas todas las sugerencias de CodeWhisperer.
ProgrammingLanguage	CodeWhispererCharacterCount	El número de caracteres generado por CodeWhisperer.

Para agregar las invocaciones, utilice la estadística Sum.

Para agregar DailyActiveUserTrend, use la estadística de suma y use «1 día» como período.

Para agregar SubscriptionCount, utilice la estadística de suma.

Para agregar, MonthlyActiveUniqueUsers utilice la estadística de suma y utilice «30 días» como período.

Seguimiento CodeWhisperer del uso en toda la organización

Su empresa puede operar con muchas AWS cuentas diferentes que forman parte de una AWS organización. En ese caso, es posible que desee crear una CodeWhisperer instancia independiente para cada una de sus AWS cuentas. Luego, puedes asignar un CodeWhisperer administrador diferente y un conjunto diferente (o superpuesto) de desarrolladores a cada cuenta.

Cuando un CodeWhisperer administrador vea el panel, solo verá información sobre la cuenta a la que se le ha asignado.

La facturación del uso CodeWhisperer profesional es por AWS organización. Si el mismo desarrollador utiliza el servicio CodeWhisperer en varias cuentas de la misma organización, solo se te facturará el puesto que ocupe en la primera cuenta en la que utilice el servicio.

Compartir sus datos con AWS

Cuando los utilice CodeWhisperer, AWS podrá, con fines de mejora del servicio, almacenar datos sobre su uso y contenido. En esta página, se explica cómo desactivar compartir esos datos.

Los datos que se AWS pueden recopilar CodeWhisperer incluyen su telemetría del lado del cliente y su contenido.

Tu contenido incluye las partes del código que se CodeWhisperer utilizan para generar sugerencias, así como el contenido de las propias sugerencias. A nivel profesional y para el desarrollo en consolas, CodeWhisperer no recopila tu contenido con fines de mejora del servicio. El desarrollo en consola incluye el desarrollo en Amazon SageMaker Studio, AWS Glue Studio, AWS Lambda consola y AWS Cloud9. El nivel profesional, en este contexto, incluye las características de chat de código, desarrollo de características y transformación de código de Amazon Q.

La telemetría del cliente cuantifica el uso del servicio. Por ejemplo, AWS puede hacer un seguimiento de si aceptas o rechazas una recomendación. La telemetría del cliente no contiene el código real ni información de identificación personal (PII), como la dirección IP.

Desactivación del envío de la telemetría del cliente

Toolkit for Visual Studio

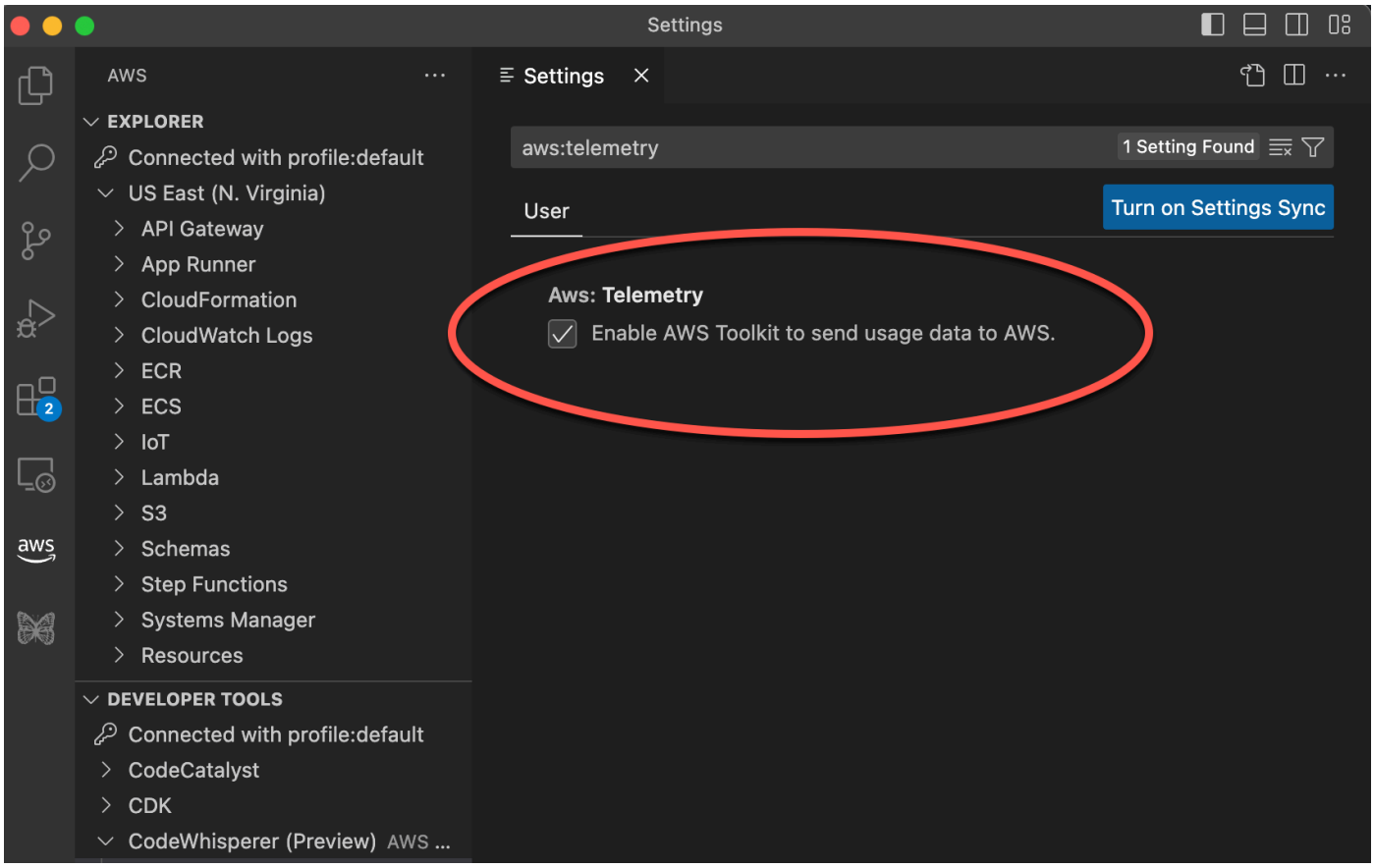
Para desactivar compartir los datos de telemetría en Toolkit para Visual Studio, utilice este procedimiento:

1. En Herramientas, seleccione Opciones.
2. Seleccione kit de herramientas de AWS .
3. En Uso del kit de herramientas, quite la selección de la casilla.

> **Note**
>
> Esta es una decisión que cada desarrollador debe tomar dentro de su propio IDE. Si la utilizas CodeWhisperer como parte de una empresa, tu administrador no podrá cambiar esta configuración por ti.

AWS Toolkit for Visual Studio Code

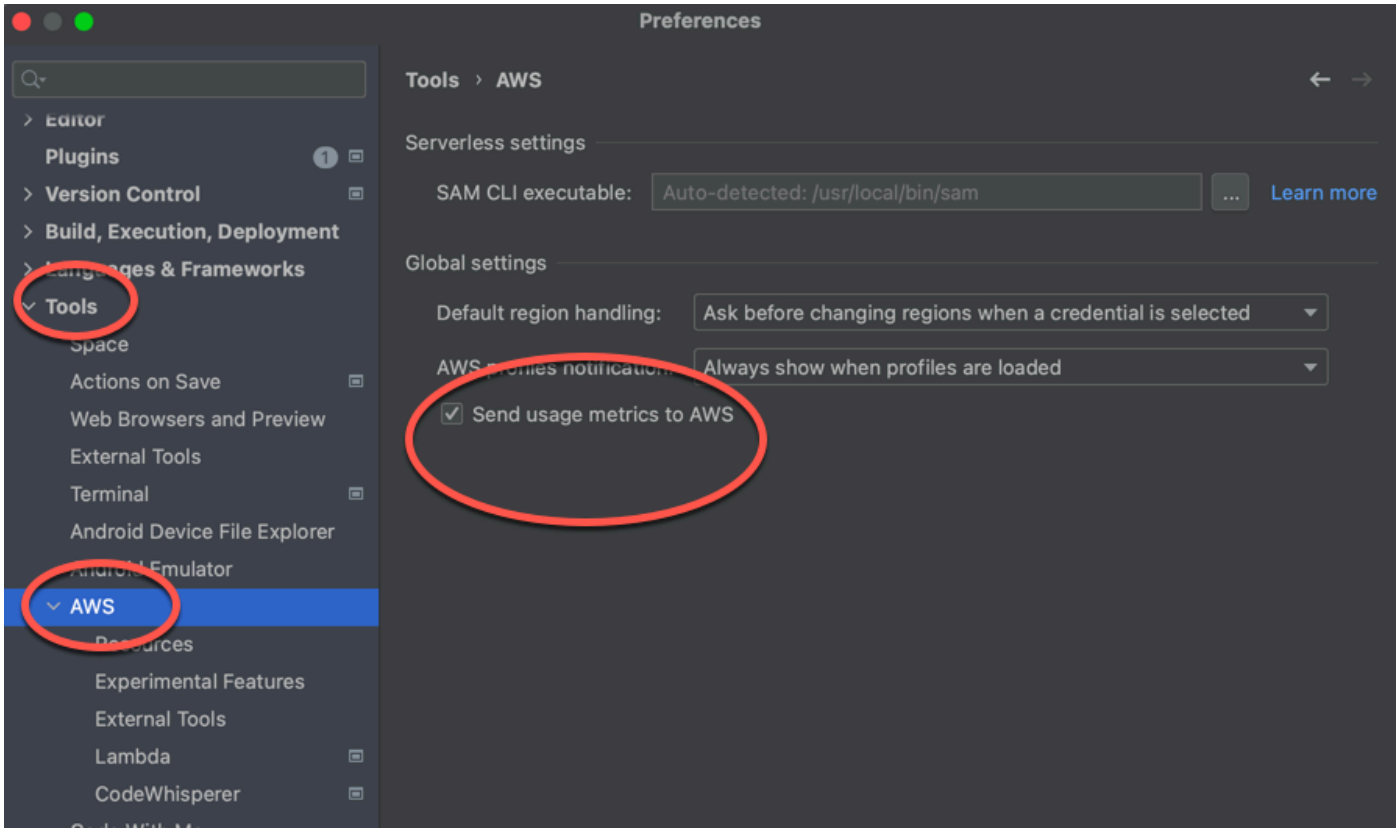
1. En VS Code, elige el AWS logotipo en el lateral de la ventana. Se abrirá el panel de AWS .
2. En Herramientas para desarrolladores, selecciona el icono con forma de engranaje situado junto a CodeWhisperer.
3. Si utiliza espacios de trabajo de VS Code, cambie a la subpestaña de espacio de trabajo. En VS Code, la configuración del espacio de trabajo invalida la configuración del usuario.
4. En la pestaña Configuración, busque aws:telemetry.
5. Desmarque la casilla.



> **Note**
>
> Esta es una decisión que cada desarrollador debe tomar dentro de su propio IDE. Si lo utilizas CodeWhisperer como parte de una empresa, tu administrador no podrá cambiar esta configuración por ti.

AWS Toolkit for JetBrains

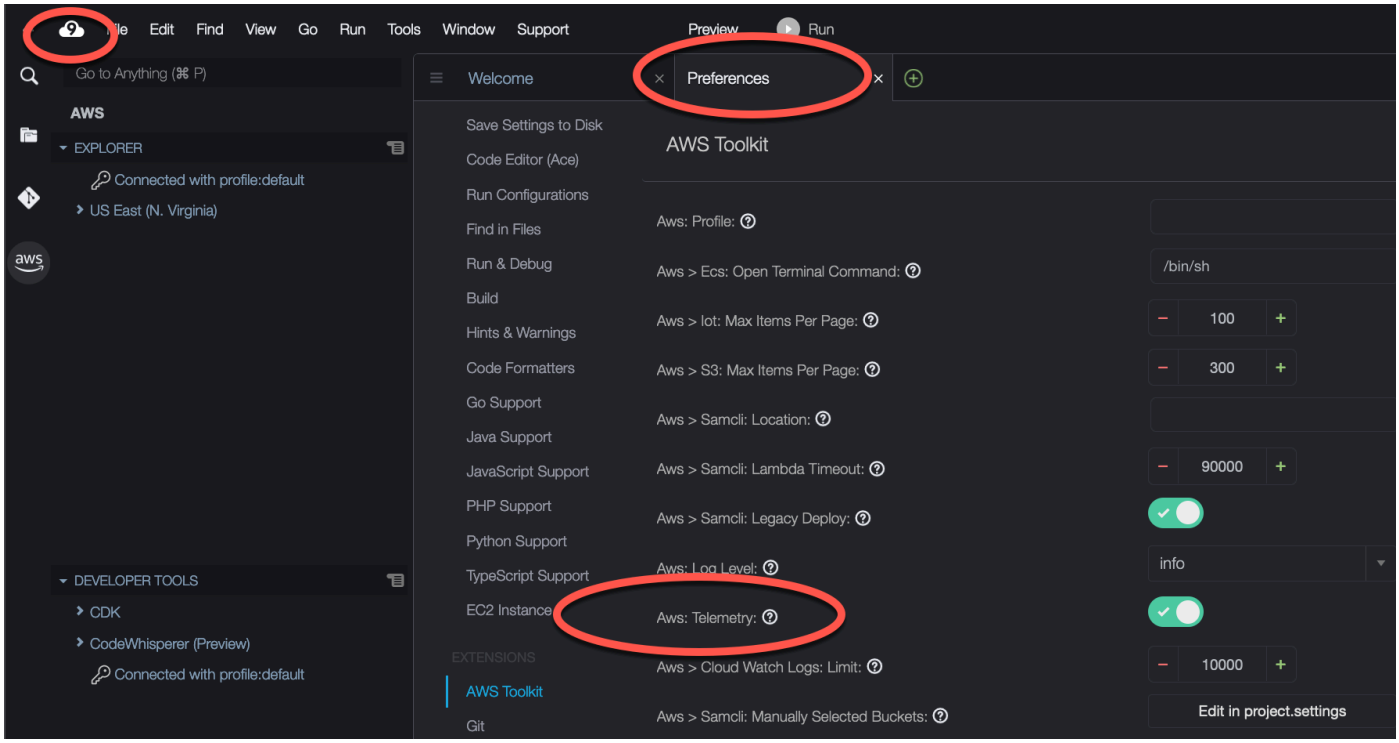
1. En JetBrains, seleccione el logotipo del AWS kit de herramientas en el lateral de la ventana. Se abrirá el AWS panel.
2. Cerca del encabezado del kit de herramientas de AWS , elija el icono de engranaje.
3. En el menú emergente, elija Mostrar configuración de AWS .
4. En la ventana de preferencias, en Herramientas -> AWS, junto a Enviar métricas de uso a AWS, desmarca la casilla.



> **Note**
>
> Esta es una decisión que cada desarrollador debe tomar dentro de su propio IDE. Si lo utilizas CodeWhisperer como parte de una empresa, tu administrador no podrá cambiar esta configuración por ti.

AWS Cloud 9

1. Desde tu IDE de AWS Cloud 9, selecciona el logotipo de AWS Cloud 9 en la parte superior de la ventana y, a continuación, selecciona Preferencias.
2. En la pestaña Preferencias, elija kit de herramientas de AWS .
3. Junto a AWS: telemetría del cliente, coloque el interruptor en la posición de apagado.



> **Note**
>
> Esta configuración determina si compartes o no la telemetría del lado del cliente de AWS Cloud 9 en general, no solo para ti. CodeWhisperer

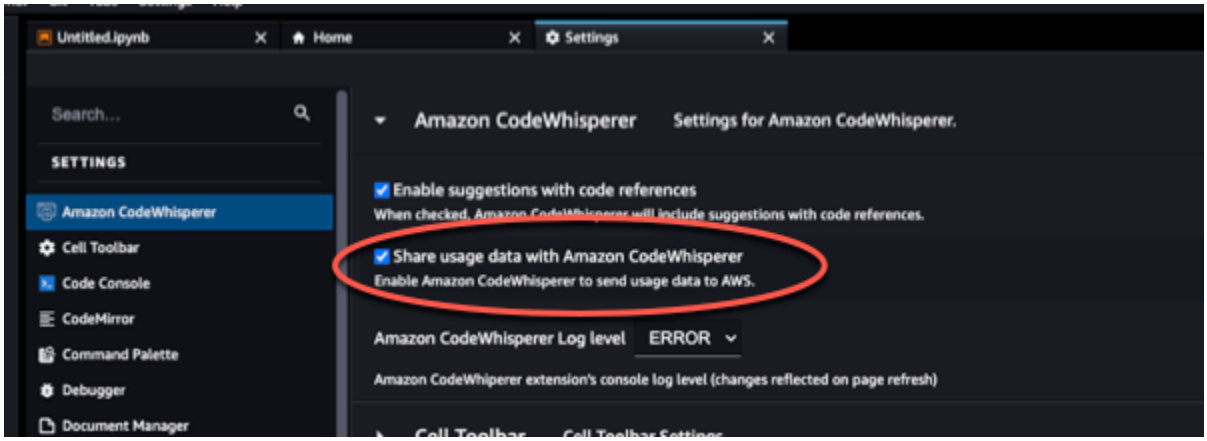
Lambda

Cuando se utiliza CodeWhisperer con Lambda, CodeWhisperer no comparte la telemetría del lado del cliente con. AWS

SageMaker Studio

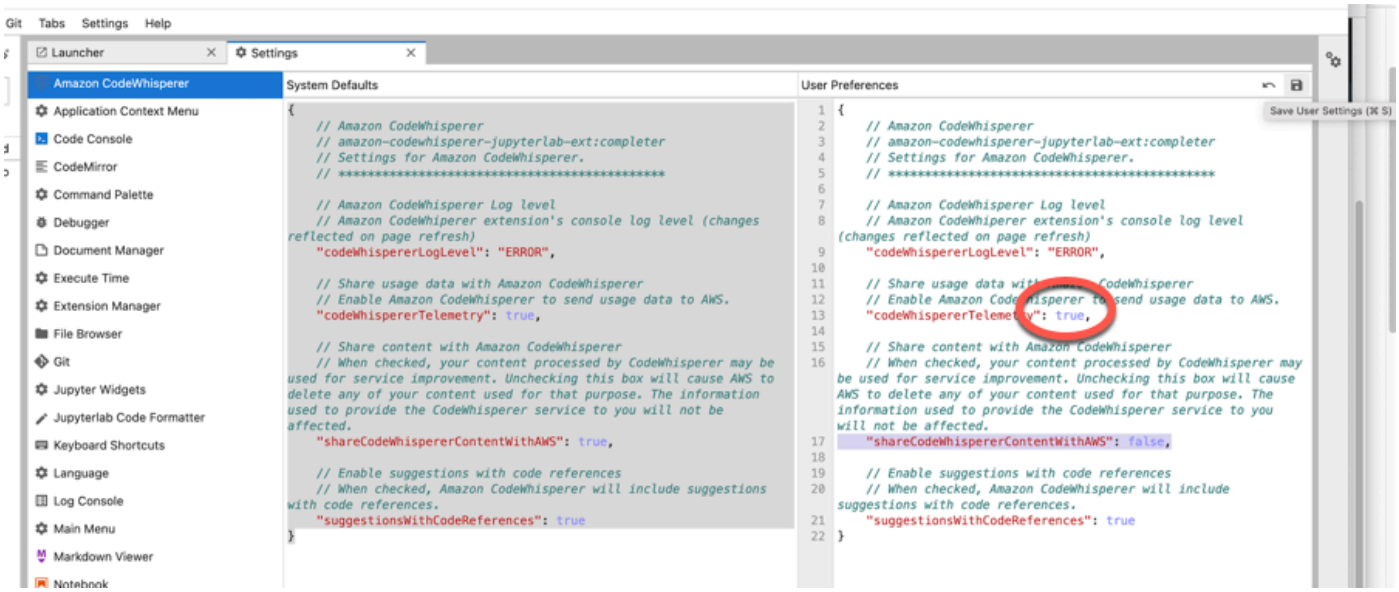
1. En la parte superior de la ventana de Studio, selecciona Configuración SageMaker .

2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. En el CodeWhisperer menú desplegable Amazon, selecciona o desmarca la casilla situada junto a Compartir datos de uso con Amazon. CodeWhisperer



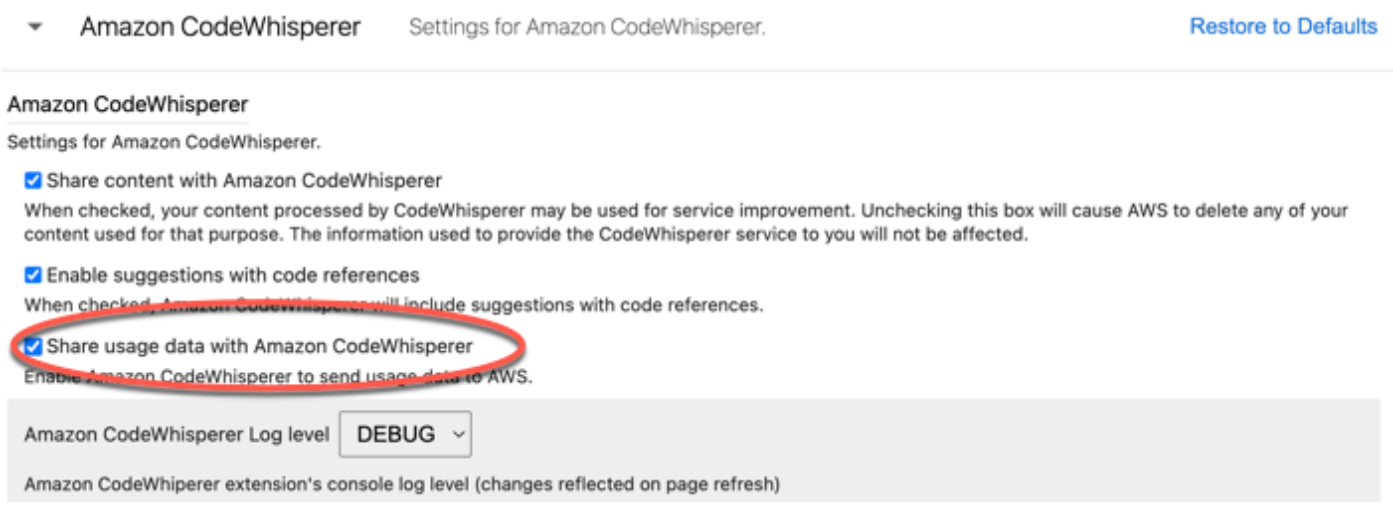
Amazon EMR Studio

1. En la parte superior de la ventana de Amazon EMR Studio, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. Selecciona Amazon CodeWhisperer en el menú desplegable. Defina el valor `codeWhispererTelemetry` de verdadero o falso.



JupyterLab

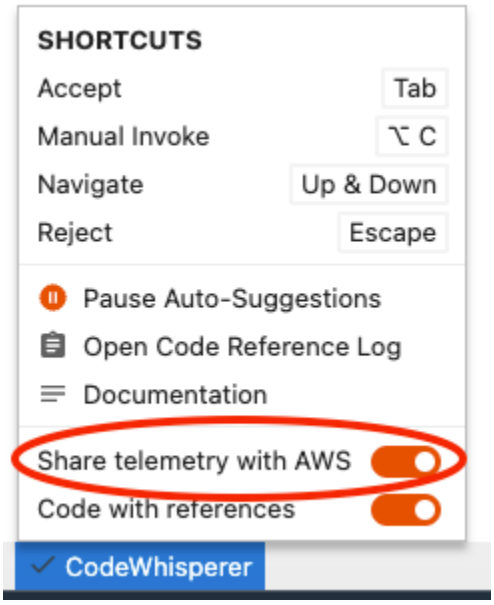
1. En la parte superior de la JupyterLab ventana, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. En el CodeWhisperer menú desplegable Amazon, selecciona o desmarca la casilla situada junto a Compartir datos de uso con Amazon. CodeWhisperer



AWS Glue Studio Notebook

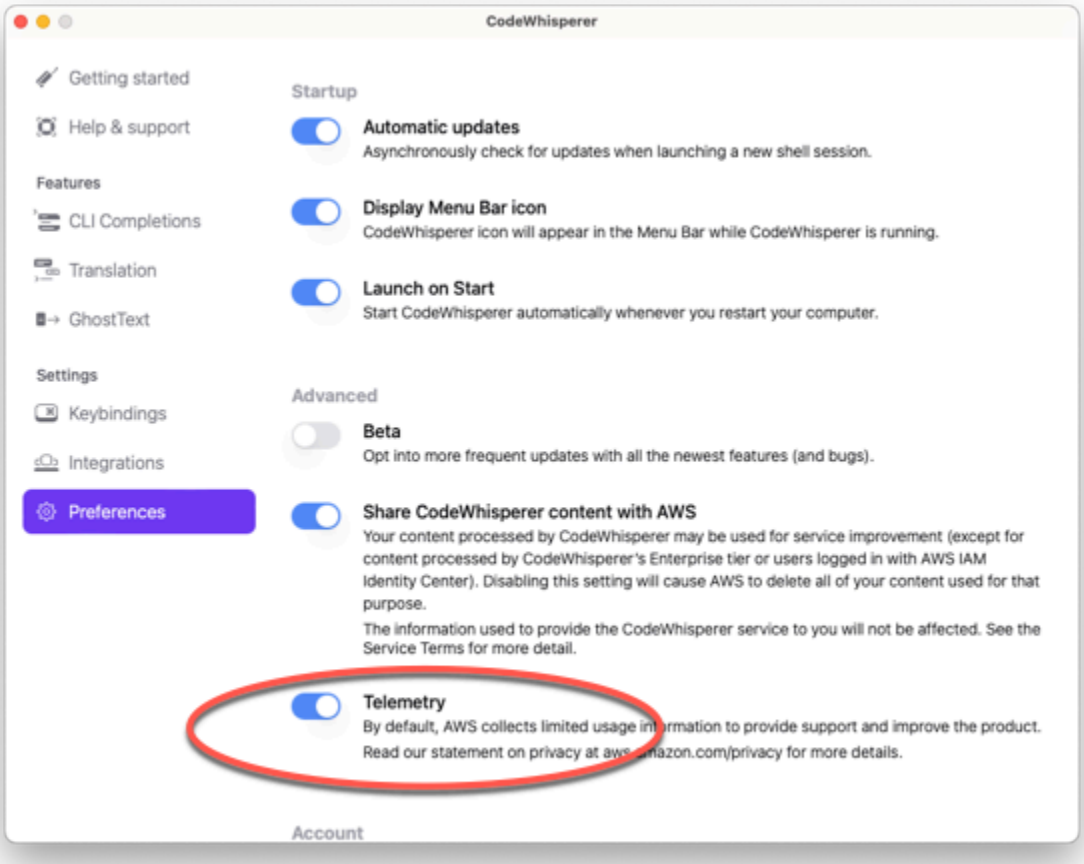
1. Selecciona la opción en la parte inferior de la ventana de AWS Glue Studio Notebook. CodeWhisperer
2. En el menú emergente, active el interruptor situado junto a Compartir telemetría con AWS.

> **Note**
>
> La pausa en el uso compartido de la telemetría del lado del cliente solo será válida mientras dure el Studio Notebook actual. AWS Glue



Command line

En la herramienta de línea de comandos, en Preferencias, conmute la telemetría.



Cancelación del uso compartido del contenido

Toolkit for Visual Studio

En el nivel profesional, CodeWhisperer no recopila tu contenido.

En el nivel personal, para desactivar el uso compartido del contenido en Visual Studio, utilice el siguiente procedimiento.

Abre el menú de CodeWhisperer opciones de dos maneras:

- Selecciona el CodeWhisperer icono del borde de la ventana y, a continuación, selecciona Opciones...
- Ve a Herramientas -> Opciones -> AWS Kit de herramientas -> CodeWhisperer

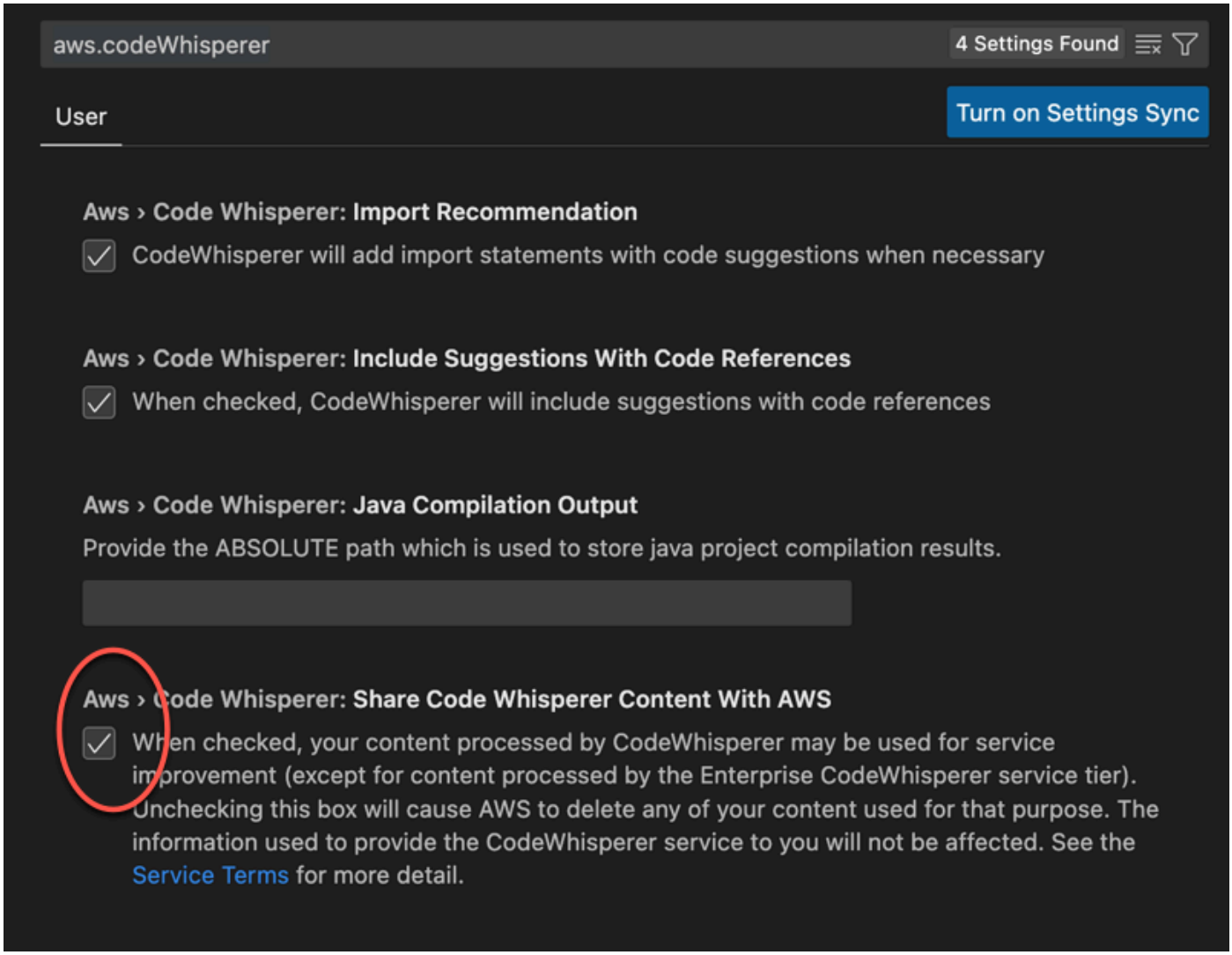
A continuación, cambia la opción Compartir CodeWhisperer contenido AWS a Verdadero o Falso.

AWS Toolkit for Visual Studio Code

En el nivel profesional, CodeWhisperer no recopila tu contenido.

En el nivel personal, para desactivar el uso compartido del contenido en VS Code, utilice el siguiente procedimiento.

1. En VS Code, elige el AWS logotipo en el lateral de la ventana. Se abrirá el panel de AWS .
2. En Herramientas para desarrolladores, selecciona el icono con forma de engranaje situado junto a CodeWhisperer.
3. Si utiliza espacios de trabajo de VS Code, cambie a la subpestaña de espacio de trabajo. En VS Code, la configuración del espacio de trabajo invalida la configuración del usuario.
4. Desmarca la casilla situada junto a Compartir CodeWhisperer contenido con AWS.



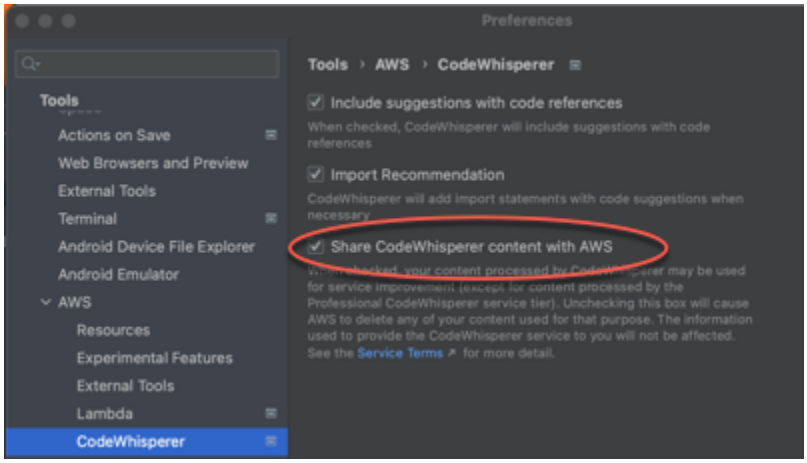
AWS Toolkit for JetBrains

En el nivel profesional, CodeWhisperer no recopila tu contenido.

Para optar por no compartir CodeWhisperer datos JetBrains, utilice el siguiente procedimiento.

1. Asegúrese de utilizar la última versión de ambos JetBrains y del AWS kit de herramientas.
2. En JetBrains, abre Preferencias (en un Mac, estará en Configuración).
3. En la ventana de preferencias, en Herramientas, en AWS, selecciona CodeWhisperer.

   El panel de CodeWhisperer preferencias se abrirá a la derecha.
4. En el panel de CodeWhisperer preferencias, deselecciona Compartir CodeWhisperer contenido con AWS.



AWS Cloud 9

Cuando lo usas CodeWhisperer con AWS Cloud 9, CodeWhisperer no comparte tu contenido con AWS.

> **Note**
>
> La configuración de AWS Cloud 9 contiene un interruptor para compartir CodeWhisperer contenido. AWS Pero ese conmutador no funciona.

Lambda

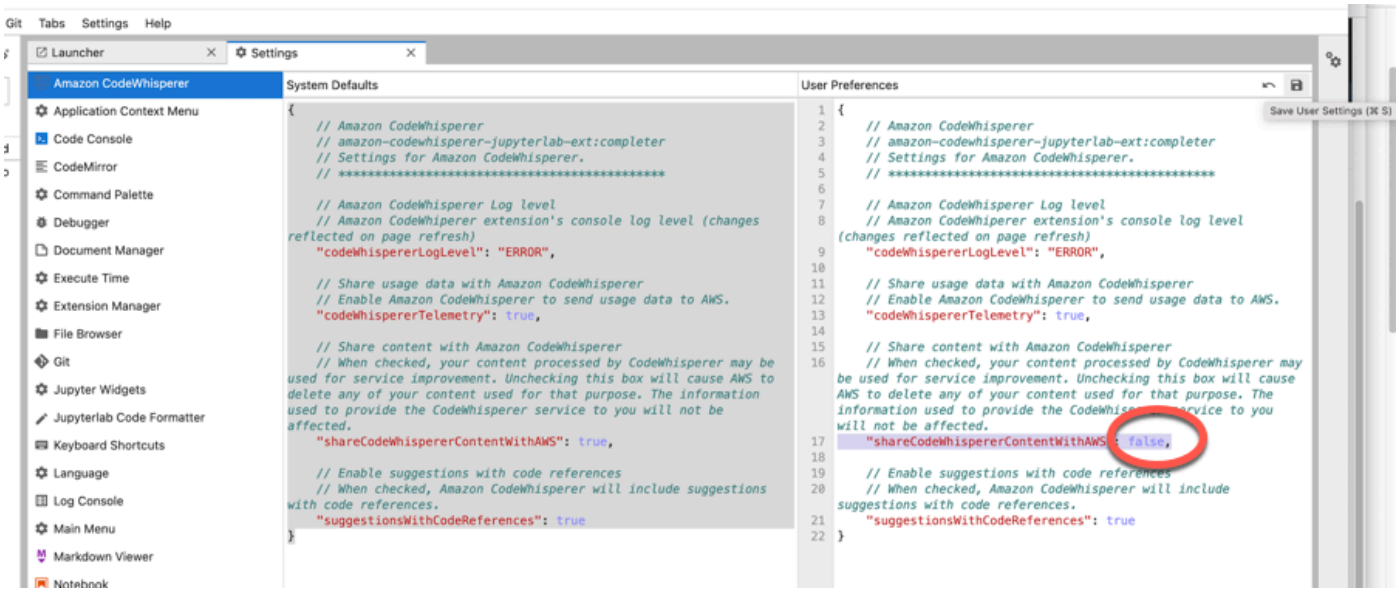
Cuando lo usa CodeWhisperer con Lambda, CodeWhisperer no comparte su contenido con. AWS

SageMaker Studio

Cuando lo usa CodeWhisperer con SageMaker Studio, CodeWhisperer no comparte su contenido con AWS.

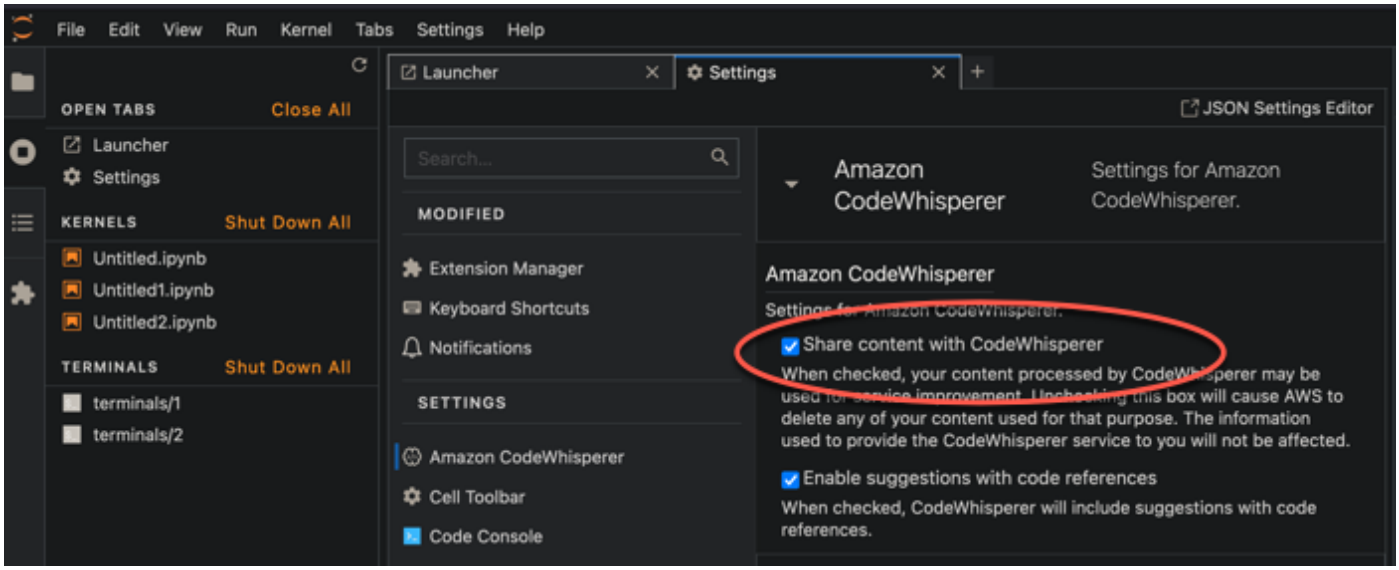
Amazon EMR Studio

1. En la parte superior de la ventana de Amazon EMR Studio, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. Selecciona Amazon CodeWhisperer en el menú desplegable. Defina el valor `shareCodedeWhispererContentWithAWS` de verdadero o falso.



JupyterLab

1. En la parte superior de la JupyterLab ventana, selecciona Configuración.
2. En el menú desplegable de ajustes, elija Editor de ajustes avanzados.
3. En el CodeWhisperer menú desplegable Amazon, selecciona o desmarca la casilla situada junto a Compartir contenido con Amazon. CodeWhisperer

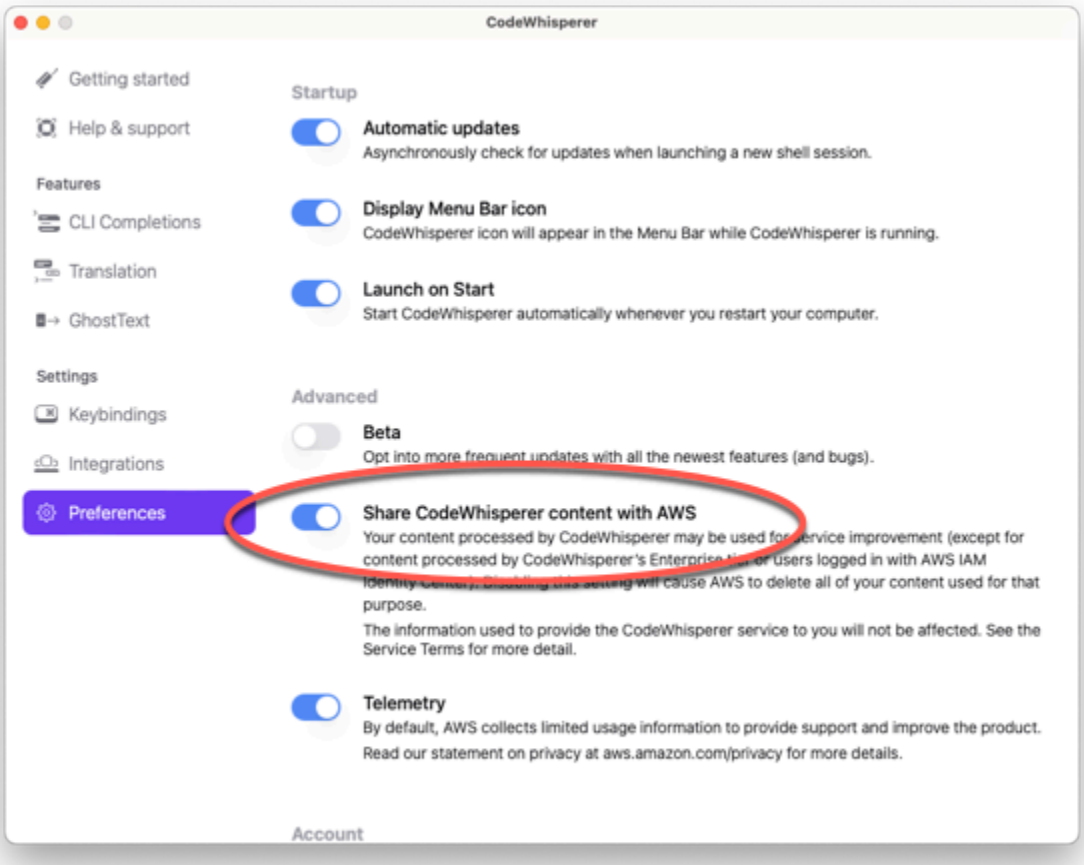


AWS Glue Studio Notebook

Cuando lo usas CodeWhisperer con AWS Glue Studio Notebook, CodeWhisperer no comparte tu contenido con. AWS

Command line

En la herramienta de línea de comandos, en Preferencias, selecciona Compartir CodeWhisperer contenido con AWS.



Cuotas para Amazon CodeWhisperer

CodeWhisperer no mantiene ninguna cuota de servicio.

Para obtener más información sobre las diferencias de uso disponibles por nivel de servicio, consulte ???.

Seguridad en Amazon CodeWhisperer

> **Note**
>
> La CodeWhisperer infraestructura está ubicada en el este de EE. UU. (Virginia del Norte).

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon CodeWhisperer, consulta AWS Servicios en el ámbito de aplicación por programa de conformidad AWS .
- Seguridad en la nube: tu responsabilidad viene determinada por el AWS servicio que utilices. También eres responsable de otros factores, como la confidencialidad de tus datos, los requisitos de tu empresa y las leyes AWS y reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza CodeWhisperer. Los siguientes temas muestran cómo configurarlo CodeWhisperer para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus CodeWhisperer recursos.

> **Note**

Temas

- Resiliencia en Amazon CodeWhisperer
- Análisis y gestión de vulnerabilidades en Amazon CodeWhisperer

- Las mejores prácticas de seguridad administrativa con IAM Identity Center y CodeWhisperer
- Protección de datos para Amazon CodeWhisperer
- Validación de conformidad para Amazon CodeWhisperer
- Mejores prácticas de seguridad en Amazon CodeWhisperer
- Seguridad de la infraestructura en Amazon CodeWhisperer
- Identity and Access Management para Amazon CodeWhisperer
- Amazon CodeWhisperer y puntos de enlace de VPC de interfaz () AWS PrivateLink

Resiliencia en Amazon CodeWhisperer

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global. AWS

Además de la infraestructura AWS global, CodeWhisperer ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Análisis y gestión de vulnerabilidades en Amazon CodeWhisperer

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Las mejores prácticas de seguridad administrativa con IAM Identity Center y CodeWhisperer

En esta sección se describen algunas sugerencias para simplificar sus decisiones de seguridad al administrar el Centro de identidades de IAM en relación con. CodeWhisperer

- Active la MFA en el usuario raíz de la consola de administración y también en el proveedor de identidades externo.
- Si utiliza un entorno de varias cuentas, configure la administración delegada.
- Utilice un origen de identidades existente y actívelo la primera vez que se utilice IAM Identity Center.
- Delegue permisos administrativos a un usuario concreto.
- Cree un conjunto de permisos administrativos.
- Utilice las políticas de control de servicios (SCP) para controlar qué aplicaciones pueden acceder a la información en qué cuentas de AWS Organizations.
- Cree un límite de permisos.

Para obtener más información, consulte la Guía del usuario del IAM Identity Center.

Protección de datos para Amazon CodeWhisperer

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Amazon CodeWhisperer. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se basa toda la AWS nube. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación del blog AWS Modelo de responsabilidad compartida de y RGPDAWS en el blog de seguridad de .

Con fines de protección de datos, le recomendamos que proteja las credenciales de las AWS cuentas y configure cuentas de usuario individuales con ellas AWS Identity and Access Management. De esta manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes maneras:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.

- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que le ayuden a detectar y proteger los datos personales almacenados en Amazon Simple Storage Service.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información acerca de los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2

Recomendamos encarecidamente que nunca ingrese información confidencial, como direcciones de correo electrónico de los clientes, en variables. Esto incluye cuando trabaja con CodeWhisperer u otros AWS servicios mediante la consola, la API o AWS los SDK. AWS CLI

AWS CloudTrail y CodeWhisperer las API

CodeWhisperer envía eventos a CloudTrail. Las llamadas a la API son:

- CreateProfile
- DeleteProfile
- ListProfiles
- UpdateProfile
- GenerateRecommendations
- GetCodeAnalysis
- ListCodeAnalysisFindings
- StartCodeAnalysis
- CreateUploadUrl
- GenerateCompletions
- CreateCustomization
- DeleteCustomization
- ListCustomizations
- ListCustomizationVersions
- UpdateCustomization
- GetCustomization

Sus datos no se iniciarán sesión CloudTrail. Esto incluye tanto su contenido como la telemetría del lado del cliente.

Para obtener más información sobre cómo se puede llamar a estas API desde la consola y los permisos de IAM relacionados, consulte ???.

Para obtener explicaciones de las API específicas, consulte ???.

Cifrado de datos en Amazon CodeWhisperer

El cifrado es una parte importante de la CodeWhisperer seguridad. Los datos en tránsito y en reposo se cifran de forma predeterminada como parte de Amazon CodeWhisperer y no requieren que hagas nada.

- Cifrado de datos en reposo: de forma predeterminada, los datos recopilados por CodeWhisperer se almacenan mediante Amazon Simple Storage Service y Amazon DynamoDB. Los datos se cifran utilizando sus capacidades de data-at-rest cifrado con una clave propia AWS.

  Sin embargo, los usuarios empresariales tienen la opción de cifrar los datos mediante una AWS KMS key.
- Cifrado de los datos en tránsito: todas las comunicaciones entre los clientes CodeWhisperer y CodeWhisperer sus dependencias internas están protegidas mediante TLS (Transport Layer Security) para cifrar los datos en tránsito. Todos los CodeWhisperer puntos finales utilizan certificados SHA-256 gestionados por. AWS Private Certificate AuthorityPara obtener más información, consulte ¿Qué es? AWS Private CA en la Guía AWS Private CA del usuario.

Protección de datos y CodeWhisperer personalizaciones

Al crear una personalización, AWS protege los archivos de código.

CodeWhisperer carga sus archivos en un bucket de Amazon S3 CodeWhisperer propiedad de Amazon S3. Sus archivos se cifran en tránsito con HTTPS y TLS. Se cifran en reposo mediante una AWS KMS clave, proporcionada por usted o, si no la proporciona, por AWS. Una vez creada la personalización, elimina AWS permanentemente los datos del depósito y los purga de la memoria.

Las personalizaciones están completamente aisladas unas de otras dentro de la cuenta. También están aisladas de los datos de otros clientes.

Solo los usuarios especificados por el CodeWhisperer administrador tienen acceso a cualquier personalización específica. Y antes de que el CodeWhisperer administrador pueda especificar qué usuarios pueden acceder a qué personalizaciones, debe autorizarle el permiso para hacerlo.

Validación de conformidad para Amazon CodeWhisperer

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Mejores prácticas de seguridad en Amazon CodeWhisperer

Para obtener información sobre las prácticas recomendadas en materia de seguridad administrativa, consulte Las mejores prácticas de seguridad administrativa con IAM Identity Center y CodeWhisperer.

Para obtener información sobre las prácticas recomendadas en materia de seguridad de infraestructura, consulte Seguridad de la infraestructura en Amazon CodeWhisperer.

Seguridad de la infraestructura en Amazon CodeWhisperer

Como servicio gestionado, Amazon CodeWhisperer está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a CodeWhisperer través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Identity and Access Management para Amazon CodeWhisperer

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. CodeWhisperer La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo CodeWhisperer funciona Amazon con IAM
- Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer
- AWS políticas gestionadas para Amazon CodeWhisperer
- Solución de problemas de CodeWhisperer identidad y acceso a Amazon
- Uso de roles vinculados a servicios de CodeWhisperer

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. CodeWhisperer

Usuario del servicio: si utiliza el CodeWhisperer servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más CodeWhisperer funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función en CodeWhisperer, consulteSolución de problemas de CodeWhisperer identidad y acceso a Amazon.

Administrador de servicios: si está a cargo de CodeWhisperer los recursos de su empresa, probablemente tenga acceso total a ellos CodeWhisperer. Su trabajo consiste en determinar a qué CodeWhisperer funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM CodeWhisperer, consulteCómo CodeWhisperer funciona Amazon con IAM.

Administrador de IAM: si es administrador de IAM, puede que desee obtener más información sobre cómo redactar políticas para administrar el acceso. CodeWhisperer Para ver ejemplos de políticas CodeWhisperer basadas en la identidad que puede usar en IAM, consulte. Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información,

consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso.

Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal

de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder

permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad

y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo CodeWhisperer funciona Amazon con IAM

Antes de utilizar IAM para gestionar el acceso CodeWhisperer, infórmate sobre las funciones de IAM disponibles. CodeWhisperer

Funciones de IAM que puedes usar con Amazon CodeWhisperer

Característica de IAM	CodeWhisperer soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Parcial
Recursos de políticas	No
Claves de condición de política (específicas del servicio)	No
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo CodeWhisperer funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para CodeWhisperer

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué

condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para CodeWhisperer

Para ver ejemplos de políticas CodeWhisperer basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

Políticas basadas en recursos incluidas CodeWhisperer

Compatibilidad con las políticas basadas en recursos	Sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a

una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para CodeWhisperer

Admite acciones de política	Parcial

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de CodeWhisperer acciones, consulta Acciones definidas por Amazon CodeWhisperer en la Referencia de autorización de servicio.

Las acciones políticas CodeWhisperer utilizan el siguiente prefijo antes de la acción:

```
codewhisperer
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "codewhisperer:action1",
      "codewhisperer:action2"
         ]
```

Para ver ejemplos de políticas CodeWhisperer basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

Recursos de políticas para CodeWhisperer

Admite recursos de políticas	No

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de CodeWhisperer recursos y sus ARN, consulte Recursos definidos por Amazon CodeWhisperer en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon. CodeWhisperer

Para ver ejemplos de políticas CodeWhisperer basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

Claves de condición de la política para CodeWhisperer

Admite claves de condición de políticas específicas del servicio	No

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de CodeWhisperer estado, consulta Claves de estado de Amazon CodeWhisperer en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon CodeWhisperer.

Para ver ejemplos de políticas CodeWhisperer basadas en la identidad, consulte. Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

ACL en CodeWhisperer

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con CodeWhisperer

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con CodeWhisperer

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para CodeWhisperer

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para CodeWhisperer

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir CodeWhisperer la funcionalidad. Edite las funciones de servicio solo cuando se CodeWhisperer proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para CodeWhisperer

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon CodeWhisperer

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar CodeWhisperer recursos. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por CodeWhisperer, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon CodeWhisperer en la Referencia de autorización de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de CodeWhisperer
- Permisos necesarios para la CodeWhisperer consola
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear CodeWhisperer recursos de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus

políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de CodeWhisperer

Para acceder a la CodeWhisperer consola de Amazon, debes tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los CodeWhisperer recursos de tu cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Permisos necesarios para la CodeWhisperer consola

La CodeWhisperer consola utiliza las siguientes acciones de API.

- susurrador de códigos: CreateProfile
- susurrador de códigos: ListProfiles
- susurrador de códigos: UpdateProfile
- susurrador de códigos: DeleteProfile

Las acciones CreateProfile, ListProfiles UpdateProfile, y DeleteProfile API no están pensadas para que las invoques tu código. Por lo tanto, estas acciones de la API no se incluyen en la AWS CLI ni en AWS los SDK.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la AWS CLI API o. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para Amazon CodeWhisperer

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSServiceRoleForCodeWhispererPolicy

Esta política AWS gestionada concede los permisos que normalmente se necesitan para usar Amazon CodeWhisperer. La política se añade a la AWSServiceRoleForCodeWhisperer que se crea cuando te incorporas a CodeWhisperer.

No puedes asociarte AWSServiceRoleForCodeWhispererPolicy a tus entidades de IAM. Esta política está asociada a un rol vinculado al servicio que te permite CodeWhisperer realizar acciones en tu nombre. Para obtener más información, consulte Uso de roles vinculados a servicios de CodeWhisperer.

Esta política otorga permisos de *`administrador`* que permiten escanear los artefactos de código por motivos de seguridad y recopilar métricas de uso para realizar un seguimiento de la facturación.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `cloudwatch`— Permite a los directores publicar las métricas de uso CloudWatch para la facturación o el uso. Esto es necesario para que puedas hacer un seguimiento del uso que haces de la entrada CodeWhisperer . CloudWatch

- `codeguru-security`— Permite a los directores cargar artefactos de código, realizar escaneos de código y enumerar los hallazgos del escaneo de código con Amazon. CodeGuru Esto es necesario para CodeWhisperer poder realizar un análisis de seguridad del código desde los IDE JetBrains y los IDE de Visual Studio Code.
- `sso`— Permite a los directores recuperar todos los detalles de la CodeWhisperer aplicación tal como se muestran en el Centro de identidades de IAM. Esto es necesario para poder facturar el uso CodeWhisperer.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListMembersInGroup"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sso:ListProfileAssociations",
                 "sso:ListProfiles",
                 "sso:ListDirectoryAssociations",
                 "sso:DescribeRegisteredRegions",
                 "sso:GetProfile",
                 "sso:GetManagedApplicationInstance",
                 "sso:DescribeApplication"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codeguru-security:CreateUploadUrl"
            ],
            "Resource": [
```

```
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "codeguru-security:CreateScan",
                "codeguru-security:GetScan",
                "codeguru-security:ListFindings",
                "codeguru-security:GetFindings"
            ],
            "Resource": [
                "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/CodeWhisperer"
                    ]
                }
            }
        }
    ]
}
```

Para ver esta política en el contexto de otras políticas AWS gestionadas, consulte AWSServiceRoleForCodeWhispererPolicy.

CodeWhisperer actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas CodeWhisperer desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del CodeWhisperer documento.

Cambio	Descripción	Fecha
Actualizado AWSServiceRoleForCodeWhispererPolicy	Se agregó un DescribeApplication permiso, que le permite recuperar información sobre CodeWhisperer.	29 de marzo de 2024
Actualizado AWSServiceRoleForCodeWhispererPolicy	GetFindings Añadidos y GetManagedApplicationInstance permisos. GetFindings los permisos simplifican las interacciones entre servicios, pero no afectan a su experiencia con el servicio. GetManagedApplicationInstance evita que se le facture por las instancias de CodeWhisperer aplicaciones deshabilitadas.	19 de junio de 2023
Actualizado AWSServiceRoleForCodeWhispererPolicy	Se han agregado permisos para obtener información de usuarios y grupos con fines de facturación.	31 de mayo de 2023
AWSServiceRoleForCodeWhispererPolicy: política nueva	Se agregó una nueva política que CodeWhisperer permite llamar CloudWatch y CodeGuru en tu nombre. Esta política se añade a la AWSServiceRoleForCodeWhisperer que se crea cuando te incorporas a Amazon CodeWhisperer.	29 de marzo de 2023

Cambio	Descripción	Fecha
CodeWhisperer comenzó a rastrear los cambios	CodeWhisperer comenzó a rastrear los cambios de sus políticas AWS gestionadas.	29 de marzo de 2023

Solución de problemas de CodeWhisperer identidad y acceso a Amazon

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas más comunes que puedes encontrar al trabajar con un CodeWhisperer IAM.

Temas

- No estoy autorizado a realizar ninguna acción en CodeWhisperer
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis CodeWhisperer recursos

No estoy autorizado a realizar ninguna acción en CodeWhisperer

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `codewhisperer:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 codewhisperer:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `codewhisperer:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferirle CodeWhisperer una función.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en ella. CodeWhisperer Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis CodeWhisperer recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si CodeWhisperer es compatible con estas funciones, consulteCómo CodeWhisperer funciona Amazon con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles vinculados a servicios de CodeWhisperer

Amazon CodeWhisperer usa roles AWS Identity and Access Management vinculados a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. CodeWhisperer Los roles vinculados al servicio están predefinidos CodeWhisperer e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración CodeWhisperer , ya que no es necesario añadir manualmente los permisos necesarios. CodeWhisperer define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo CodeWhisperer puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus CodeWhisperer recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Información sobre AWS políticas gestionadas para Amazon CodeWhisperer.

Permisos de rol vinculados al servicio para CodeWhisperer

CodeWhisperer usa el rol vinculado al servicio denominado AWSServiceRoleForCodeWhisperer: este rol otorga permisos para acceder CodeWhisperer a los datos de tu cuenta a fin de calcular la facturación, proporciona acceso para crear y acceder a informes de seguridad en Amazon CodeGuru y emite datos a... CloudWatch

El rol AWSServiceRoleForCodeWhisperer vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `codewhisperer.amazonaws.com`

La política de permisos de roles denominada AWSServiceRoleForCodeWhispererPolicy permite CodeWhisperer realizar las siguientes acciones en los recursos especificados:

- Acción: `cloudwatch:PutMetricData` en `AWS/CodeWhisperer CloudWatch namespace`
- Acción: `codeguru-security:CreateUploadUrl` en `*`
- Acción: `codeguru-security:CreateScan` en `arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*`
- Acción: `codeguru-security:GetScan` en `arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*`
- Acción: `codeguru-security:ListFindings` en `arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*`
- Acción: `sso:ListProfiles` en `*`
- Acción: `sso:ListProfileAssociations` en `*`
- Acción: `sso-directory:ListMembersInGroup` en `*`
- Acción: `sso:ListDirectoryAssociations` en `*`
- Acción: `sso:DescribeRegisteredRegions` en `*`
- Acción: `sso:GetProfile` en `*`
- Acción: `sso:DescribeApplication` en `*`

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para CodeWhisperer

No necesita crear manualmente un rol vinculado a servicios. Al configurarlo CodeWhisperer en AWS Management Console, CodeWhisperer crea el rol vinculado al servicio para usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al actualizar la configuración, vuelve a CodeWhisperer crear el rol vinculado al servicio para usted.

Puede utilizar la consola de IAM o la CLI de AWS para crear un rol vinculado a servicios con el nombre de servicios `codewhisperer.amazonaws.com`. Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para CodeWhisperer

CodeWhisperer no permite editar el rol vinculado al AWSServiceRoleForCodeWhisperer servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para CodeWhisperer

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el CodeWhisperer servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForCodeWhisperer servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados al servicio CodeWhisperer

CodeWhisperer no admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio esté disponible. Puede usar el AWSServiceRoleForCodeWhisperer rol en las siguientes regiones. Para obtener más información, consulte Puntos de conexión y Regiones de AWS.

Nombre de la región	Identidad de la región	Support en CodeWhisperer
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	No
Oeste de EE. UU. (Norte de California)	us-west-1	No
Oeste de EE. UU. (Oregón)	us-west-2	No
África (Ciudad del Cabo)	af-south-1	No
Asia-Pacífico (Hong Kong)	ap-east-1	No
Asia-Pacífico (Yakarta)	ap-southeast-3	No
Asia-Pacífico (Bombay)	ap-south-1	No
Asia Pacífico (Osaka)	ap-northeast-3	No
Asia Pacífico (Seúl)	ap-northeast-2	No
Asia Pacífico (Singapur)	ap-southeast-1	No
Asia Pacífico (Sídney)	ap-southeast-2	No
Asia Pacífico (Tokio)	ap-northeast-1	No
Canadá (centro)	ca-central-1	No
Europa (Fráncfort)	eu-central-1	No
Europa (Irlanda)	eu-west-1	No
Europa (Londres)	eu-west-2	No
Europa (Milán)	eu-south-1	No
Europa (París)	eu-west-3	No
Europa (Estocolmo)	eu-north-1	No

Nombre de la región	Identidad de la región	Support en CodeWhisperer
Medio Oriente (Baréin)	me-south-1	No
Medio Oriente (EAU)	me-central-1	No
América del Sur (São Paulo)	sa-east-1	No
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	No
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	No

Amazon CodeWhisperer y puntos de enlace de VPC de interfaz () AWS PrivateLink

Puede establecer una conexión privada entre su VPC y Amazon CodeWhisperer mediante la creación de un punto de enlace de VPC de interfaz. Los puntos de enlace de la interfaz funcionan con una tecnología que le permite acceder de forma privada a CodeWhisperer las API sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. AWS PrivateLink Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con CodeWhisperer las API. El tráfico entre tu VPC y CodeWhisperer no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Interface VPC Endpoints (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

> **Note**
>
> CodeWhisperer no admite políticas de puntos finales.

Consideraciones sobre los puntos CodeWhisperer finales de VPC

Antes de configurar un punto de enlace de VPC de interfaz CodeWhisperer, asegúrese de revisar las propiedades y limitaciones del punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

CodeWhisperer admite realizar llamadas a todas sus acciones de API desde su VPC, en el contexto de los servicios que están configurados para funcionar con ellos. CodeWhisperer

Requisitos previos

Antes de comenzar cualquiera de los procedimientos siguientes, asegúrese de que dispone de lo siguiente:

- Una AWS cuenta con los permisos adecuados para crear y configurar los recursos.
- Una VPC ya creada en su cuenta. AWS
- Familiaridad con AWS los servicios, especialmente Amazon CodeWhisperer VPC y.

Creación de un punto de conexión de VPC de interfaz para CodeWhisperer

Puede crear un punto de enlace de VPC para el CodeWhisperer servicio mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto final de VPC para CodeWhisperer usar el siguiente nombre de servicio:

- com.amazonaws.*region*.codewhisperer

Si habilita DNS privado para el punto de conexión, puede realizar solicitudes a la API para CodeWhisperer usando su nombre de DNS predeterminado para la región, por ejemplo `codewhisperer.us-east-1.amazonaws.com`.

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Utilizar un ordenador local para conectarse a un punto final CodeWhisperer

En esta sección se describe el proceso de usar un equipo local al que conectarse a CodeWhisperer través de un AWS PrivateLink punto final de la AWS VPC.

1. Cree una conexión de VPN entre el dispositivo en las instalaciones y la VPC.
2. Cree un punto final de VPC de interfaz para. CodeWhisperer
3. Configure un punto de conexión entrante de Amazon Route 53. Esto le permitirá utilizar el nombre DNS de su CodeWhisperer terminal desde su dispositivo local.

Uso de un IDE integrado en la consola para conectarse a un punto final CodeWhisperer

En esta sección se describe el proceso de uso de un IDE integrado en la consola para conectarse a un CodeWhisperer punto final.

En este contexto, un IDE integrado en la consola es un IDE al que se accede desde la AWS consola y al que se autentica con IAM. Algunos ejemplos son SageMaker Studio AWS Cloud9 y Studio. AWS Glue

1. Cree un punto final de VPC de interfaz para. CodeWhisperer
2. Configúrelo CodeWhisperer con el IDE integrado en la consola.
   - AWS Cloud9
   - SageMaker Estudio
   - AWS Glue Estudio
3. Configure el IDE para usar el CodeWhisperer punto final.
   - AWS Cloud9
   - SageMaker Estudio
   - AWS Glue Estudio

Conexión CodeWhisperer mediante un IDE AWS PrivateLink de terceros en una instancia de Amazon EC2

En esta sección, se explica el proceso de instalación de un entorno de desarrollo integrado (IDE) de terceros, como Visual Studio Code o JetBrains en una instancia de Amazon EC2, y de configurarlo para que se conecte a CodeWhisperer él. AWS PrivateLink

1. Cree un punto final de VPC de interfaz para. CodeWhisperer
2. Lance una instancia de Amazon EC2 en la subred deseada dentro de la VPC. Puede elegir una imagen de máquina de Amazon (AMI) que sea compatible con el IDE de terceros. Por ejemplo, puede seleccionar una AMI de Amazon Linux 2.
3. Conéctese a la instancia de Amazon EC2.
4. Instale y configure el IDE (Visual Studio Code o JetBrains).

5. Instale el AWS kit de herramientas mediante uno de los siguientes procedimientos:

   - Instalación del AWS kit de herramientas para. JetBrains
   - Instalación del AWS Toolkit for Visual Studio Code.

6. Configure el IDE para conectarse mediante AWS PrivateLink.

   - Conexiones de red en Visual Studio Code
   - JetBrains desarrollo remoto

Historial de documentos de la Guía CodeWhisperer del usuario

En la siguiente tabla se describen las versiones de la documentación de CodeWhisperer.

Cambio	Descripción	Fecha
Fusión con Amazon Q Developer	CodeWhisperer ahora forma parte de Amazon Q Developer .	30 de abril de 2024
DescribeApplication permiso añadido	La función vinculada al servicio y la política AWSServiceRoleForCodeWhispererPolicy gestionada se han actualizado para incluir el DescribeApplication permiso sso:, que permite recuperar información sobre. CodeWhisperer	29 de marzo de 2024
Instrucciones de configuración actualizadas JupyterLab	Se JuptyerLab han actualizado y aclarado los procedimientos de configuración CodeWhisperer con.	6 de marzo de 2024
Instrucciones genéricas para la integración con otros servicios	Una nueva sección proporciona la política de IAM básica necesaria para su uso CodeWhisperer en el contexto de otros servicios, en general.	6 de marzo de 2024
Política de administrador CodeWhisperer profesional actualizada	Se agregaron permisos a la política de administrador CodeWhisperer profesional: sso: CreateManagedApplicationInstance y codewhisp	5 de marzo de 2024

	erer:. CreateProfile Estos permisos son necesarios para crear un CodeWhisperer perfil en una cuenta que no sea de administración.	
Uso compartido de datos con Amazon EMR Studio	La página de intercambio de datos contiene informaci ón sobre cómo compartir contenido y datos de telemetrí a con Amazon EMR Studio.	7 de febrero de 2024
Se necesitan más permisos de panel	El acceso al panel de personalizaciones requiere permisos adicionales. Además, cuando no CodeWhisperer se utilice durante dos semanas, el panel tendrá un aspecto diferente.	26 de enero de 2024
Soporte de escaneo de seguridad para Ruby y Go	La función de escaneo de seguridad es compatible con Ruby y Go. Además, la sección de análisis de seguridad también se ha actualizado significativamente para mayor claridad.	12 de enero de 2024
Compatibilidad de Visual Studio con C y C++	La integración de Visual Studio (en versión preliminar) funciona con C y C++, además de con C#.	13 de diciembre de 2023
AWS CDK apoyo	CodeWhisperer es compatibl e AWS CDK con TypeScript y Python.	13 de diciembre de 2023

Proceso de incorporación del kit de herramientas simplificado	La descripción del procedimiento para empezar a utilizar VS CodeWhisperer Code e JetBrains IDEs se ha simplificado considerablemente.	28 de noviembre de 2023
Autenticación de Amazon Q	Para poder utilizar algunas funciones de Amazon Q, debes autenticarte con CodeWhisperer Professional.	28 de noviembre de 2023
Compatibilidad de Visual Studio	CodeWhisperer funciona con Visual Studio.	26 de noviembre de 2023
Compatibilidad de grupos con personalización	Puede agregar grupos de usuarios a una personalización.	26 de noviembre de 2023
Compatibilidad de análisis de seguridad para más lenguajes y marcos	Puede ejecutar un análisis de seguridad en el código escrito en C# TypeScript, Terraform o el AWS CDK. AWS CloudFormation	26 de noviembre de 2023
Nuevos permisos para mostrar las versiones de personalización	Si utiliza personalizaciones, debe añadirlas `codewhisperer:ListCustomizationVersions` a la política de personalización asociada a su CodeWhisperer función de administrador.	26 de noviembre de 2023
Actualizaciones de paneles	El panel muestra la tasa de aceptación y se puede filtrar por lenguaje de programación.	26 de noviembre de 2023

Personalización del control de versiones	Puede actualizar las personalizaciones mediante la creación de versiones nuevas.	26 de noviembre de 2023
Compatibilidad de generación de código para más lenguajes	Compatibilidad de lenguajes para JSON (AWS CloudFormation), YAML (AWS CloudFormation) y HCL (Terraform).	26 de noviembre de 2023
Corrección de código asistida	Tras ejecutar un análisis de seguridad, CodeWhisperer puede ayudarle a corregir el código.	26 de noviembre de 2023
Command line	Puede usarlo CodeWhisperer en la línea de comandos.	20 de noviembre de 2023
Integración de Amazon EMR	Integración con Amazon EMR.	17 de noviembre de 2023
Registros de personalización y mensajes de error de la consola	Puede exportar los mensajes de registro sobre las personalizaciones y, en una tabla, se proporciona información que le ayudará a solucionar los mensajes de error relacionados con la consola.	13 de noviembre de 2023
JupyterLab soporte para la versión 4	Ahora se admite la integración con la JupyterLabversión 4.	7 de noviembre de 2023
Personalizaciones	Puedes entrenar con tu propia CodeWhisperer base de código.	17 de octubre de 2023

Más compatibilidad con Go, SQL, PHP, Rust y Kotlin	Go, SQL, PHP, Rust y Kotlin ahora están incluidos en la lista de lenguajes “más compatibles”.	13 de octubre de 2023
Cuentas de miembros	Ahora puedes configurarla CodeWhisperer en más de una cuenta dentro de tu organización.	12 de septiembre de 2023
Panel	Hay un panel disponible para los administradores de nivel profesional.	8 de septiembre de 2023
AWS PrivateLink integration	Puede establecer una conexión privada entre su VPC y crear un punto final de CodeWhisperer la VPC de interfaz.	26 de julio de 2023
AWS Glue integration	Puede utilizarla CodeWhisperer con AWS Glue Studio Notebook.	26 de julio de 2023
Políticas administrada actualizada	Añadido GetFindings y GetManagedApplicationInstance.	28 de junio de 2023
Se han agregado permisos a la política para los administradores	Se agregaron nuevos permisos relacionados iamadmin: ListRolesByPrincipal y precios:GetProducts, necesarios para CodeWhisperer la administración.	27 de junio de 2023

Las cuentas que no son de administración ahora se pueden administrar CodeWhisperer	AWS recomienda que el CodeWhisperer Centro de Identidad de IAM se administre a través de una cuenta que no sea de administración. Además, se agregó un nuevo permiso relacionado, sso: necesario para la ListApplicationInstances administración. CodeWhisperer	12 de junio de 2023
Se agregaron llamadas a la API para ser rastreadas con AWS CloudTrail	Ahora se puede realizar un seguimiento de las siguientes API CloudTrail: DeleteProfile GetCodeAnalysis,, ListCodeAnalysisFindings, StartCodeAnalysis, CreateUploadUrl, GenerateCompletions.	6 de junio de 2023
Cambio a rol vinculado al servicio	Se agregaron permisos para obtener información de usuarios y grupos con fines de facturación mediante la actualización AWSServiceRoleForCodeWhispererPolicy, que está asociada a la función vinculada al servicio.	30 de mayo de 2023
Se agregaron dos CloudWatch métricas de Amazon	Se agregaron suscripciones y CloudWatch métricas MonthlyActiveUniqueUsers como métricas.	30 de mayo de 2023
Amazon SageMaker Studio y JupyterLab soporte	Se agregaron secciones que explican la configuración de la integración con SageMaker Studio y JupyterLab.	9 de mayo de 2023

Nuevo rol vinculado a servicio	Se agregó sso: ListDirectoryAssociations como un rol vinculado a un servicio.	1 de mayo de 2023
Capítulo de monitoreo	Se agregó información sobre el monitoreo con. CodeWhisperer CloudWatch	24 de abril de 2023
Análisis de seguridad de varios archivos	La sección de análisis de seguridad se ha actualizado para aclarar que un análisis puede incluir más de un archivo.	20 de abril de 2023
Restricciones basadas en la región	La sección de CodeWhisperer administradores se ha actualizado para aclarar la situación específica en la que se deben tomar medidas en una región en particular.	19 de abril de 2023
API útiles	Se ha agregado la sección de API útiles a las acciones del usuario. Aunque CodeWhisperer no tiene una API pública, estas llamadas a la API pueden resultar útiles en el contexto de la creación o edición de políticas de IAM.	13 de abril de 2023
Tipos de usuarios	Se ha añadido el capítulo sobre los tipos de usuarios para ayudar a aclarar cuáles son las distintas personas que lo utilizan de distintas CodeWhisperer maneras.	13 de abril de 2023

Configuración	Parte del contenido pasó de introducción a configuración. Las instrucciones de configuración para los administradores se dividen en tres partes: usuario root, administrador de la AWS cuenta y CodeWhisperer administrador.	13 de abril de 2023
Roles vinculados al servicio	Se ha agregado información acerca de los roles vinculados a servicios.	13 de abril de 2023
Contenido de seguridad	Se ha agregado contenido nuevo para aclarar los problemas de seguridad relacionados con CodeWhisperer. Esta actualización incluye la adición de la sección Identity and Access Management, así como la seguridad de la infraestructura, la validación del cumplimiento, las prácticas recomendadas de seguridad, la seguridad de la infraestructura y las actualizaciones de la sección de protección de datos.	13 de abril de 2023
Cuotas	El capítulo de cuotas se ha actualizado para aclarar que CodeWhisperer no mantiene ninguna cuota.	13 de abril de 2023

Lenguajes compatibles	La sección de soporte lingüísti co se ha actualizado para incluir los idiomas que ya están disponibles para el público en CodeWhisperer general.	13 de abril de 2023
Capturas de pantalla de IDE	Se han actualizado varias capturas de pantalla para reflejar el aspecto de la CodeWhisperer interfaz incluida en el AWS kit de herramientas cuando ya no CodeWhisperer estaba en versión preliminar.	13 de abril de 2023
Características	Se han incorporado las siguientes secciones al capítulo de características: acciones del usuario, compatibilidad de lenguajes , sugerencias de pausas, análisis de seguridad y referencias de código.	13 de abril de 2023
Capturas de pantalla de desactivación de datos	Las capturas de pantalla de la sección «exclusión voluntaria» del capítulo sobre el intercamb io de datos se han actualiza do para reflejar la CodeWhisp erer configuración actual de VS Code y. JetBrains	13 de abril de 2023

Facturación	Se ha agregado el capítulo de facturación para proporcionar información sobre cómo se le puede cobrar por su uso. CodeWhisperer	13 de abril de 2023
Versión inicial	Versión inicial de la Guía CodeWhisperer del usuario. Algunos materiales incluidos aquí estaban disponibles anteriormente en otras guías.	21 de febrero de 2023
Nueva política: AWSServiceRoleForAmazonCodeWhisperer	Se agregó una nueva política que CodeWhisperer permite llamar CloudWatch y CodeGuru en tu nombre.	17 de febrero de 2023