



Guía de referencia

# AWS SDKs y herramientas



# AWS SDKsy herramientas: Guía de referencia

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

---

# Table of Contents

AWS SDKs Guía de referencia de herramientas y herramientas .....	1
Recursos para desarrolladores .....	3
Kit de herramientas: notificación telemétrica .....	3
Configuración .....	5
Archivos compartidos <code>config</code> y <code>credentials</code> .....	6
Perfiles .....	6
Formato del archivo de configuración .....	8
Formato del archivo de credenciales .....	11
Ubicación de los archivos compartidos .....	12
Resolución del directorio principal .....	13
Cambie la ubicación predeterminada de estos archivos .....	13
Variables de entorno .....	14
Cómo configurar las variables de entorno .....	15
Configuración de variables de entorno sin servidor .....	16
Propiedades del sistema JVM .....	17
¿Cómo configurar las propiedades del sistema JVM .....	17
Autenticación y acceso .....	19
ID de creador de AWS .....	21
IAM Autenticación en el Centro .....	21
Configure el acceso mediante programación mediante IAM Identity Center .....	22
Comprender la autenticación del Centro de identidades de IAM .....	25
Funciones de IAM en cualquier lugar .....	30
Paso 1: Configurar las Funciones de IAM en cualquier lugar .....	30
Paso 2: Utilice las funciones de IAM en cualquier lugar .....	30
Asumir un rol .....	32
Asume cualquier rol IAM .....	32
Asume un rol (web) .....	34
Cómo federar con identidad web u OpenID Connect .....	34
AWS claves de acceso .....	36
Use credenciales a corto plazo. ....	36
Use credenciales a largo plazo. ....	36
Credenciales a corto plazo .....	38
Credenciales a largo plazo .....	39
IAM roles para EC2 instancias .....	43

Crear un rol de IAM .....	43
Lanza una EC2 instancia de Amazon y especifica tu IAM rol .....	43
Conectarse a la EC2 instancia .....	44
Ejecuta la aplicación en la instancia EC2 .....	44
Referencia de configuración .....	46
Cómo crear clientes de servicio .....	46
Prioridad de los ajustes .....	46
Páginas de configuración .....	48
Lista de ajustes de archivos Config .....	49
Lista de ajustes de archivos Credentials .....	53
Lista de variables de entorno .....	54
JVMlista de propiedades del sistema .....	58
Proveedores de credenciales estandarizadas .....	61
Comprenda la cadena de proveedores de credenciales .....	61
SDK-cadenas de proveedores de credenciales específicas y específicas de cada herramienta .....	63
AWS claves de acceso .....	64
Asumir el rol de proveedor .....	67
Proveedor de contenedores .....	74
IAMProveedor del centro de identidad .....	77
IMDSproveedor .....	84
Proveedor del proceso .....	88
Características estandarizadas .....	93
Puntos de enlace basados en cuentas .....	94
Application ID .....	96
Metadatos de EC2 instancias de Amazon .....	98
Puntos de acceso de Amazon S3 .....	100
Puntos de acceso multirregión de Amazon S3 .....	103
Región de AWS .....	105
AWS STS Puntos finales regionales .....	108
Pila doble y puntos finales FIPS .....	113
Detección de puntos de conexión .....	115
Configuración general .....	118
IMDScliente .....	121
Comportamiento de los reintentos .....	124
Compresión de solicitudes .....	131

---

Puntos de conexión específicos del servicio .....	133
Valores predeterminados de configuración inteligente .....	183
Tiempo de ejecución común .....	189
CRTdependencias .....	190
Política de mantenimiento .....	191
Información general .....	191
Control de versiones .....	191
Ciclo de vida de las versiones principales del .....	191
Ciclo de vida de .....	192
Métodos de comunicación .....	193
Compatibilidad de versiones .....	194
Historial de documentos .....	197
Glosario de AWS .....	200
.....	cci

# AWS SDKs Guía de referencia de herramientas y herramientas

Muchas SDKs herramientas comparten alguna funcionalidad común, ya sea a través de especificaciones de diseño compartidas o de una biblioteca compartida.

Esta guía incluye información sobre:

- [Configuración](#)— Cómo utilizar los `credentials` archivos `config` y variables de entorno compartidos para configurar sus AWS SDKs propias herramientas.
- [Autenticación y acceso](#)— Establece cómo se autentica tu código o herramienta AWS cuando desarrollas con Servicios de AWS ellos.
- [Referencia de configuración](#): referencia para todos los ajustes estandarizados disponibles para la autenticación y la configuración.
- [AWS Bibliotecas Common Runtime \(CRT\)](#)— Descripción general de las bibliotecas compartidas de AWS Common Runtime (CRT) que están disponibles para casi todos SDKs.
- [AWS Política de mantenimiento de SDK y herramientas](#) cubre la política de mantenimiento y el control de versiones de los kits y herramientas de desarrollo de AWS software (SDKs), incluidos los dispositivos móviles y el Internet de las cosas (IoT) SDKs, y sus dependencias subyacentes.

Esta guía de referencia AWS SDKs y las herramientas pretenden ser una base de información aplicable a múltiples SDKs herramientas. La guía específica de la herramienta SDK o herramienta que esté utilizando debe utilizarse además de cualquier información que se presente aquí. Las siguientes son las herramientas SDK y herramientas que incluyen secciones de material relevantes en esta guía:

Si utiliza:	Las secciones relevantes de esta guía para usted son:
<ul style="list-style-type: none"> <li>• ¿Alguna herramienta SDK o herramienta</li> </ul>	<a href="#">AWS Política de mantenimiento de SDK y herramientas</a>
<ul style="list-style-type: none"> <li>• <a href="#">AWS Cloud9</a></li> <li>• <a href="#">AWS CDK</a></li> <li>• <a href="#">AWS Toolkit for Azure DevOps</a></li> </ul>	<a href="#">Configuración</a>  <a href="#">Autenticación y acceso</a>

Si utiliza:	Las secciones relevantes de esta guía para usted son:
<ul style="list-style-type: none"><li>• <a href="#">AWS Toolkit for JetBrains</a></li><li>• <a href="#">AWS Toolkit for Visual Studio</a></li><li>• <a href="#">AWS Toolkit for Visual Studio Code</a></li><li>• <a href="#">AWS Serverless Application Model</a></li> <li>• <a href="#">AWS CodeArtifact</a></li><li>• <a href="#">AWS CodeBuild</a></li><li>• <a href="#">Amazon CodeCatalyst</a></li><li>• <a href="#">AWS CodeCommit</a></li><li>• <a href="#">AWS CodeDeploy</a></li><li>• <a href="#">AWS CodePipeline</a></li></ul>	<a href="#">AWS Política de mantenimiento de SDK y herramientas</a>
<ul style="list-style-type: none"><li>• <a href="#">AWS CLI</a></li><li>• <a href="#">AWS SDK for C++</a></li><li>• <a href="#">AWS SDK for Go</a></li><li>• <a href="#">AWS SDK for Java</a></li><li>• <a href="#">AWS SDK for JavaScript</a></li><li>• <a href="#">AWS SDK para Kotlin</a></li><li>• <a href="#">AWS SDK for .NET</a></li><li>• <a href="#">AWS SDK for PHP</a></li><li>• <a href="#">AWS SDK for Python (Boto3)</a></li><li>• <a href="#">AWS SDK for Ruby</a></li><li>• <a href="#">AWS SDK para Rust</a></li><li>• <a href="#">AWS SDK para Swift</a></li><li>• <a href="#">AWS Tools for Windows PowerShell</a></li></ul>	<a href="#">Configuración</a>  <a href="#">Autenticación y acceso</a>  <a href="#">Referencia de configuración</a>  <a href="#">AWS Bibliotecas Common Runtime (CRT)</a>  <a href="#">AWS Política de mantenimiento de SDK y herramientas</a>  <a href="#">AWS SDKs y compatibilidad con las versiones de Tools</a>

## Recursos para desarrolladores

Para obtener una descripción general de las herramientas que pueden ayudarle a desarrollar aplicaciones AWS, consulte [Herramientas sobre las que construir AWS](#). Para obtener más información sobre el soporte, consulte el [Centro de conocimiento de AWS](#).

Amazon Q Developer es un asistente conversacional generativo basado en inteligencia artificial que puede ayudarle a comprender, crear, ampliar y operar aplicaciones. AWS Para acelerar su desarrollo AWS, el modelo que impulsa Amazon Q se complementa con AWS contenido de alta calidad para producir respuestas más completas, procesables y referenciadas. Para obtener más información, consulte [¿Qué es Amazon Q Developer?](#) en la Guía del usuario de Amazon Q Developer.

### Kit de herramientas: notificación telemétrica

AWS Los kits de herramientas del entorno de desarrollo integrado (IDE) son complementos y extensiones que permiten el acceso a AWS los servicios de su empresa. IDE IDE Los complementos y extensiones de Amazon Q permiten la asistencia generativa de IA en su IDE. Para obtener información detallada sobre cada uno de los IDE kits de herramientas, consulte las guías de usuario del kit de herramientas de la tabla anterior. Para obtener más información sobre el uso de Amazon Q en su entorno IDE, consulte el IDE tema [Uso de Amazon Q en la](#) guía para desarrolladores de Amazon Q.

AWS IDE Los kits de herramientas y Amazon Q pueden recopilar y almacenar datos de telemetría del lado del cliente para fundamentar las decisiones sobre futuras versiones de Toolkit AWS y Amazon Q. Los datos recopilados cuantifican su uso del AWS kit de herramientas y Amazon Q.

Para obtener más información sobre los datos de telemetría recopilados en todos los kits de AWS IDE herramientas y Amazon Q, consulte el [commonDefinitions.json en el repositorio](#) de Github. `aws-toolkit-common`

Para obtener información detallada sobre los datos de telemetría recopilados por cada uno de los kits de AWS IDE herramientas y las extensiones de Amazon Q, consulte los documentos de recursos en los siguientes AWS repositorios del kit de herramientas: GitHub

- [AWS Kit de herramientas de Visual Studio con Amazon Q](#)
- [AWS Toolkit for Visual Studio Code y la extensión Amazon Q para VS Code](#)
- [AWS Toolkit for JetBrains y el complemento Amazon Q para JetBrains](#)
- [Amazon Q para Eclipse](#)

Algunos AWS servicios a los que se puede acceder en los AWS kits de herramientas pueden recopilar datos de telemetría adicionales del lado del cliente. Para obtener información detallada sobre el tipo de datos que recopila cada AWS servicio individual, consulte el tema de la [AWS documentación correspondiente](#) al servicio específico que le interese.

# Configuración

Con AWS los SDK y otras herramientas para AWS desarrolladores, como AWS Command Line Interface (AWS CLI), puedes interactuar con las API de AWS servicio. Sin embargo, antes de intentarlo, debes configurar el SDK o la herramienta con la información necesaria para realizar la operación solicitada.

La información incluye los siguientes elementos:

- Información de credenciales que identifica quién llama a la API. Las credenciales se utilizan para cifrar la solicitud a los AWS servidores. Con esta información, AWS confirma su identidad y puede recuperar las políticas de permisos asociadas a la misma. Luego, puede determinar qué acciones puedes realizar.
- Otros detalles de configuración que se utilizan para indicar al SDK AWS CLI o al software cómo procesar la solicitud, dónde enviarla (a qué punto final del AWS servicio) y cómo interpretar o mostrar la respuesta.

Cada SDK o herramienta admite varias fuentes que puede utilizar para proporcionar las credenciales y la información de configuración necesarias. Algunas fuentes son exclusivas del SDK o la herramienta, y debes consultar la documentación de esa herramienta o SDK para obtener más información sobre cómo usar ese método.

Sin embargo, la mayoría de AWS los SDK y las herramientas admiten configuraciones comunes procedentes de dos fuentes principales (además del propio código):

- [Archivos de AWS configuración y credenciales compartidos](#): los `credentials` archivos `config` AND compartidos son la forma más común de especificar la autenticación y la configuración de un AWS SDK o una herramienta. Usa estos archivos para almacenar la configuración que pueden usar tus herramientas y aplicaciones. Los ajustes de los archivos compartidos `config` y `credentials` están asociados a un perfil específico. Con varios perfiles, puede crear diferentes opciones de configuración para aplicarlas en diferentes escenarios. Cuando utilizas una AWS herramienta para invocar un comando o un SDK para invocar una AWS API, puedes especificar qué perfil y, por lo tanto, qué ajustes de configuración quieres usar para esa acción. Uno de los perfiles se denomina perfil `default` y se utiliza automáticamente cuando no especifica explícitamente un perfil que se va a utilizar. La configuración que puede almacenar en estos archivos se documenta en esta guía de referencia.

- [Variables de entorno](#): algunas de las configuraciones también se pueden almacenar en las variables de entorno del sistema operativo. Aunque solo puede tener un conjunto de variables de entorno en vigor a la vez, se modifican fácilmente de forma dinámica a medida que se ejecuta el programa y cambian sus requisitos.

Temas adicionales en esta sección

- [Archivos config y credentials compartidos](#)
- [Ubicación de los archivos config y credentials compartidos](#)
- [Compatibilidad con variables de entorno](#)
- [Soporte de propiedades del sistema JVM](#)

## Archivos **config** y **credentials** compartidos

Los `credentials` archivos AWS `config` y `compartidos` contienen un conjunto de perfiles. Un perfil es un conjunto de parámetros de configuración, en pares clave-valor, que utilizan AWS Command Line Interface (AWS CLI) AWS SDKs, `the` y otras herramientas. Los valores de configuración se adjuntan a un perfil para configurar algún aspecto de la SDK /tool cuando se utiliza ese perfil. Estos archivos se «comparten», ya que los valores se aplican a cualquier aplicación o proceso o SDKs al entorno local del usuario.

Tanto los archivos `compartidos config` como `credentials` los archivos son archivos de texto sin formato que contienen solo ASCII caracteres (codificados en UTF -8). Adoptan la forma de lo que generalmente se denomina [INI](#) archivos.

## Perfiles

Los ajustes de los archivos `compartidos config` y `credentials` están asociados a un perfil específico. Se pueden definir varios perfiles en el archivo para crear diferentes configuraciones de configuración y aplicarlas en diferentes entornos de desarrollo.

El `[default]` perfil contiene los valores que utiliza una operación SDK o herramienta si no se especifica un perfil con nombre específico. También puede crear perfiles independientes a los que pueda hacer referencia de forma explícita por su nombre. Cada perfil puede usar diferentes configuraciones y valores según lo necesite la aplicación y el escenario.

**Note**

[default] es simplemente un perfil sin nombre. Este perfil recibe su nombre default porque es el perfil predeterminado que utiliza SDK si el usuario no especifica ningún perfil. No proporciona valores predeterminados heredados a otros perfiles. Si establece algo en el [default] perfil y no lo establece en un perfil con nombre, el valor no se establece cuando usa el perfil con nombre.

## Establece un perfil con nombre

El [default] perfil y varios perfiles con nombre pueden existir en el mismo archivo. Usa la siguiente configuración para seleccionar qué configuración de perfil usará tu herramienta SDK o tu herramienta al ejecutar el código. Los perfiles también se pueden seleccionar dentro del código o por comando cuando se trabaja con el AWS CLI.

Configure esta funcionalidad mediante una de las siguientes opciones:

### **AWS\_PROFILE**- variable de entorno

Cuando esta variable de entorno se establece en un perfil con nombre o «predeterminado», todos los SDK códigos y AWS CLI comandos utilizan la configuración de ese perfil.

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_PROFILE="my_default_profile_name";
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_PROFILE "my_default_profile_name"
```

### **aws.profile**- propiedad JVM del sistema

SDK para Kotlin on the JVM y SDK para Java 2.x, puede [establecer la propiedad del aws.profile sistema](#). Cuando SDK crea un cliente de servicio, utiliza la configuración del perfil indicado, a menos que la configuración se anule en el código. La versión 1.x SDK para Java no admite esta propiedad del sistema.

**Note**

Si su aplicación está en un servidor que ejecuta varias aplicaciones, le recomendamos que utilice siempre perfiles con nombre en lugar del perfil predeterminado. El perfil predeterminado lo recoge automáticamente cualquier AWS aplicación del entorno y lo comparte entre ellas. Por lo tanto, si otra persona actualiza el perfil predeterminado de su aplicación, puede afectar involuntariamente a los demás. Para evitar esto, defina un perfil con nombre en el `config` archivo compartido y, a continuación, utilice ese perfil con nombre en su aplicación configurándolo en su código. Puede usar la variable de entorno o la propiedad JVM del sistema para establecer el perfil con nombre si sabe que su ámbito solo afecta a su aplicación.

## Formato del archivo de configuración

El archivo `config` está organizado en secciones. Una sección es una colección con nombre de configuraciones y continúa hasta que se encuentra otra línea de definición de sección.

El archivo `config` es un archivo de texto sin formato que utiliza el formato siguiente:

- Todas las entradas de una sección adoptan el formato general de `setting-name=value`.
- Las líneas se pueden comentar si se inician con un carácter de almohadilla (`#`).

### Tipo de sección

La definición de una sección es una línea que aplica un nombre a un conjunto de ajustes. Las líneas de definición de sección comienzan y terminan con corchetes (`[ ]`). Dentro de los corchetes, hay un identificador de tipo de sección y un nombre personalizado para la sección. Puede utilizar letras, números, guiones (`-`) y guiones bajos (`_`), pero no espacios.

Tipo de sección: **default**

Ejemplo de línea de definición de sección: `[default]`

`[default]` es el único perfil que no requiere el identificador de `profile` sección.

En el siguiente ejemplo, se muestra un archivo `config` con un perfil `[default]`. Establece la configuración [region](#). Todos los ajustes que siguen esta línea, hasta que se encuentre otra definición de sección, forman parte de este perfil.

```
[default]
#Full line comment, this text is ignored.
region = us-east-2
```

Tipo de sección: **profile**

Ejemplo de línea de definición de sección: [profile *dev*]

La línea de definición de la `profile` sección es una agrupación de configuraciones con nombre que se puede aplicar a diferentes escenarios de desarrollo. Para conocer mejor los perfiles con nombre, consulte la sección anterior sobre Perfiles.

El siguiente ejemplo muestra un `config` archivo con una línea de definición de `profile` sección y un perfil con nombre denominado `foo`. Todos los ajustes que siguen esta línea, hasta que se encuentre otra definición de sección, forman parte de este perfil con nombre.

```
[profile foo]
...settings...
```

Algunas configuraciones tienen su propio grupo anidado de subconfiguraciones, como la configuración `s3` y las subconfiguraciones del siguiente ejemplo. Para asociar los subajustes al grupo, indéntelos con uno o más espacios.

```
[profile test]
region = us-west-2
s3 =
    max_concurrent_requests=10
    max_queue_size=1000
```

Tipo de sección: **sso-session**

Ejemplo de línea de definición de sección: [sso-session *my-sso*]

La línea de definición de la `sso-session` sección indica un grupo de ajustes que se utilizan para configurar un perfil a fin de resolver AWS las credenciales AWS IAM Identity Center. Para obtener más información sobre la configuración de la autenticación de inicio de sesión único, consulte [IAMAutenticación de Identity Center para su SDK herramienta](#). Un perfil está vinculado a una sección `sso-session` mediante un par clave-valor en el que `sso-session` es la clave y el nombre de la sección `sso-session` es el valor, como `sso-session = <name-of-sso-session-section>`.

En el siguiente ejemplo, se configura un perfil que obtendrá AWS credenciales a corto plazo para el IAM rol «SampleRole» de la cuenta «111122223333» mediante un token de «my-sso». La sección «my-sso» sso-session se menciona en la sección profile por su nombre mediante la clave sso-session.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

Tipo de sección: **services**

Ejemplo de línea de definición de sección: [services dev]

#### Note

La services sección admite personalizaciones de terminales específicas del servicio y solo está disponible en las herramientas que incluyen esta función. SDKs Para ver si esta función está disponible para sus terminales SDK, consulte [Compatibilidad con AWS SDKs](#) los puntos finales específicos del servicio.

La línea de definición de la services sección indica un grupo de ajustes que configuran puntos de enlace personalizados para las solicitudes. Servicio de AWS Un perfil está vinculado a una sección services mediante un par clave-valor en el que services es la clave y el nombre de la sección services es el valor, como services = <name-of-services-section>.

Además, la services sección está separada en subsecciones por <SERVICE> = líneas, donde <SERVICE> está la Servicio de AWS clave identificadora. El Servicio de AWS identificador se basa en el del API modelo, sustituyendo todos los espacios serviceId por guiones bajos y minúsculas todas las letras. Para obtener una lista de todas las claves de identificación de servicio que se van a utilizar en la sección de services, consulte [Identificadores de punto de conexión específicos del servicio](#). La clave del identificador del servicio va seguida de configuraciones anidadas, cada una en su propia línea y marcada con dos espacios.

En el siguiente ejemplo, se utiliza una definición de `services` para configurar el punto de conexión que se utilizará únicamente en las solicitudes realizadas únicamente al servicio Amazon DynamoDB. La sección "local-dynamodb" de `services` se menciona en la sección `profile` por su nombre mediante la clave `services`. La clave de Servicio de AWS identificación es. `dynamodb` La subsección de Amazon DynamoDB servicio comienza en la línea `dynamodb =`. Todas las líneas inmediatamente siguientes que estén sangradas se incluyen en esa subsección y se aplican a ese servicio.

```
[profile dev]
services = local-dynamodb

[services local-dynamodb]
dynamodb =
  endpoint_url = http://localhost:8000
```

Para obtener más información sobre la configuración de punto de conexión, consulte [Puntos de conexión específicos del servicio](#).

## Formato del archivo de credenciales

Por lo general, las reglas del archivo `credentials` son idénticas a las del archivo `config`, con la salvedad de que las secciones del perfil no comienzan por la palabra "profile". Utilice únicamente el propio nombre del perfil entre corchetes. El siguiente ejemplo muestra un `credentials` archivo con una sección de perfil con nombre denominada `foo`.

```
[foo]
...credential settings...
```

En el `credentials` archivo solo se pueden almacenar las siguientes configuraciones que se consideran «secretas» o confidenciales: `aws_access_key_id`, `aws_secret_access_key`, `yaws_session_token`. Si bien estas configuraciones también se pueden colocar en el `config` archivo compartido, le recomendamos que mantenga estos valores confidenciales en un `credentials` archivo independiente. De esta forma, puede proporcionar permisos independientes para cada archivo, si es necesario.

En el siguiente ejemplo, se muestra un archivo `credentials` con un perfil `[default]`. Establece la `aws_access_key_id` configuración `aws_session_token` global [y la](#) configuración global. `aws_secret_access_key`



## Resolución del directorio principal

~solo se utiliza para la resolución del directorio principal cuando:

- Inicia la ruta
- Va seguido inmediatamente por un separador específico de la plataforma / o por uno específico. En Windows, ~/ ~\ ambos se resuelven en el directorio principal.

Al determinar el directorio principal, se comprueban las siguientes variables:

- (Todas las plataformas) La variable de entorno HOME
- (Plataformas Windows) La variable de entorno USERPROFILE
- (Plataformas Windows) La concatenación de las variables de HOMEDRIVE HOMEPath entorno () \$HOMEDRIVE\$HOMEPATH
- (Opcional según el SDK o la herramienta) Una función o variable de resolución de la ruta de inicio específica del SDK o de la herramienta

Cuando sea posible, si el directorio principal de un usuario se especifica al principio de la ruta (por ejemplo, ~username/), se resuelve en el directorio principal del nombre de usuario solicitado (por ejemplo, /home/username/.aws/config).

## Cambie la ubicación predeterminada de estos archivos

Puedes usar cualquiera de las siguientes opciones para anular el lugar desde el que el SDK o la herramienta cargan estos archivos.

### Utilización de variables de entorno

Se pueden configurar las siguientes variables de entorno para cambiar la ubicación o el nombre de estos archivos del valor predeterminado a un valor personalizado:

- Variable de entorno de archivo config: **AWS\_CONFIG\_FILE**
- Variable de entorno de archivo credentials: **AWS\_SHARED\_CREDENTIALS\_FILE**

## Linux/macOS

Puede especificar una ubicación alternativa ejecutando los siguientes comandos de [export](#) en Linux o macOS.

```
$ export AWS_CONFIG_FILE=/some/file/path/on/the/system/config-file-name
$ export AWS_SHARED_CREDENTIALS_FILE=/some/other/file/path/on/the/system/
credentials-file-name
```

## Windows

Puede especificar una ubicación alternativa ejecutando los siguientes comandos de [setx](#) en Windows.

```
C:\> setx AWS_CONFIG_FILE c:\some\file\path\on\the\system\config-file-name
C:\> setx AWS_SHARED_CREDENTIALS_FILE c:\some\other\file\path\on\the\system
\credentials-file-name
```

Para obtener más información sobre la configuración del sistema mediante variables de entorno, consulte [Compatibilidad con variables de entorno](#).

## Utilice las propiedades del sistema JVM

Para el SDK para Kotlin que se ejecuta en la JVM y para el SDK para Java 2.x, puedes configurar las siguientes propiedades del sistema JVM para cambiar la ubicación o el nombre de estos archivos del valor predeterminado a uno personalizado:

- configpropiedad del sistema JVM del archivo: **aws.configFile**
- Variable de entorno de archivo `credentials`: **aws.sharedCredentialsFile**

Para obtener instrucciones sobre cómo configurar las propiedades del sistema JVM, consulte [the section called “¿Cómo configurar las propiedades del sistema JVM”](#). El SDK for Java 1.x no admite estas propiedades del sistema.

## Compatibilidad con variables de entorno

Las variables de entorno constituyen otro mecanismo para especificar opciones de configuración y credenciales, y pueden ser útiles para crear scripts o configurar temporalmente un perfil con

nombre como la opción predeterminada. Para ver la lista de variables de entorno compatibles con la mayoría de SDKs, consulte [Lista de variables de entorno](#).

### Prioridad de las opciones

- Si especifica una configuración mediante su variable de entorno, anulará cualquier valor cargado desde un perfil en los `credentials` archivos AWS config AND compartidos.
- Si especifica una configuración mediante un parámetro de la línea de AWS CLI comandos, anulará cualquier valor de la variable de entorno correspondiente o de un perfil del archivo de configuración.

## Cómo configurar las variables de entorno

En los siguientes ejemplos se muestra cómo se pueden configurar las variables de entorno para el usuario predeterminado.

Linux, macOS, or Unix

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
$ export
AWS_SESSION_TOKEN=AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
$ export AWS_REGION=us-west-2
```

La configuración de la variable de entorno cambia el valor usado hasta el final de su sesión del intérprete de comandos o hasta que otorgue a la variable un valor diferente. Puede hacer que las variables persistan en sesiones futuras configurándolas en el script de startup del intérprete de comandos.

Windows Command Prompt

```
C:\> setx AWS_ACCESS_KEY_ID AKIAIOSFODNN7EXAMPLE
C:\> setx AWS_SECRET_ACCESS_KEY wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
C:\> setx
AWS_SESSION_TOKEN AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
C:\> setx AWS_REGION us-west-2
```

El uso de `set` para configurar una variable de entorno cambia el valor usado hasta que finalice la sesión de símbolo del sistema actual o hasta que otorgue a la variable un valor diferente. El uso

de [setx](#) para establecer una variable de entorno cambia el valor usado en la sesión de símbolo del sistema actual y en todas las sesiones de símbolo del sistema que cree después de ejecutar el comando. La operación no afecta a otros comandos del shell que ya se están ejecutando en el momento de ejecutar el comando.

## PowerShell

```
PS C:\> $Env:AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
PS C:\> $Env:AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
PS C:\>
\> $Env:AWS_SESSION_TOKEN="AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40L"
PS C:\> $Env:AWS_REGION="us-west-2"
```

Si establece una variable de entorno en la PowerShell línea de comandos, como se muestra en los ejemplos anteriores, guardará el valor únicamente durante la sesión actual. Para que la configuración de la variable de entorno sea persistente en todas las sesiones PowerShell y en las de Command Prompt, guárdela mediante la aplicación Sistema del Panel de control. Como alternativa, puede configurar la variable para todas las PowerShell sesiones futuras añadiéndola a su PowerShell perfil. Consulte la [PowerShell documentación](#) para obtener más información sobre cómo almacenar variables de entorno o cómo conservarlas en todas las sesiones.

## Configuración de variables de entorno sin servidor

Si utiliza una arquitectura sin servidor para el desarrollo, tiene otras opciones para configurar las variables de entorno. En función del contenedor, puede usar diferentes estrategias para que el código que se ejecute en esos contenedores pueda ver las variables de entorno y acceder a ellas, de forma similar a lo que ocurre en los entornos que no son de nube.

Por ejemplo, con AWS Lambda, puede configurar directamente las variables de entorno. Para obtener más información, consulte [Uso de variables de AWS Lambda entorno](#) en la Guía para AWS Lambda desarrolladores.

En Serverless Framework, a menudo puede establecer variables de SDK entorno en el `serverless.yml` archivo con la clave del proveedor en la configuración del entorno. Para obtener información sobre el archivo `serverless.yml`, consulte la [configuración general de las funciones](#) en la documentación de Serverless Framework.

Independientemente del mecanismo que utilice para establecer las variables de entorno del contenedor, hay algunas que están reservadas por el contenedor, como las documentadas

para Lambda en las variables de [entorno de tiempo de ejecución definidas](#). Consulte siempre la documentación oficial del contenedor que utilice para determinar cómo se tratan las variables de entorno y si hay alguna restricción.

## Soporte de propiedades del sistema JVM

[Las propiedades del sistema JVM](#) proporcionan otra forma de especificar las opciones de configuración y las credenciales de los SDK que se ejecutan en la JVM, como el y el. AWS SDK for Java AWS SDK para Kotlin [Para obtener una lista de las propiedades del sistema JVM compatibles con los SDK, consulte la referencia de configuración.](#)

### Prioridad de las opciones

- Si especifica una configuración mediante su propiedad de sistema JVM, anulará cualquier valor que se encuentre en las variables de entorno o que se cargue desde un perfil en los archivos `config` y `credentials` AWS compartidos.
- Si especifica una configuración mediante su variable de entorno, anulará cualquier valor cargado desde un perfil en los `credentials` archivos `config` y AWS compartidos.

## ¿Cómo configurar las propiedades del sistema JVM

Puede configurar las propiedades del sistema JVM de varias maneras.

### En la línea de comandos

Establezca las propiedades del sistema JVM en la línea de comandos al invocar el `java` comando mediante el conmutador. `-D` El siguiente comando lo configura Región de AWS globalmente para todos los clientes del servicio, a menos que se anule explícitamente el valor del código.

```
java -Daws.region=us-east-1 -jar <your_application.jar> <other_arguments>
```

Si necesita configurar varias propiedades del sistema JVM, especifique el `-D` conmutador varias veces.

### Con una variable de entorno

Si no puede acceder a la línea de comandos para invocar la JVM y ejecutar la aplicación, puede usar la variable de `JAVA_TOOL_OPTIONS` entorno para configurar las opciones de la línea de comandos.

Este enfoque resulta útil en situaciones como la ejecución de una AWS Lambda función en el entorno de ejecución de Java o la ejecución de código en una JVM integrada.

En el siguiente ejemplo, se configura Región de AWS globalmente para todos los clientes del servicio, a menos que se anule explícitamente el valor del código.

Linux, macOS, or Unix

```
$ export JAVA_TOOL_OPTIONS="-Daws.region=us-east-1"
```

La configuración de la variable de entorno cambia el valor usado hasta el final de su sesión del intérprete de comandos o hasta que otorgue a la variable un valor diferente. Puede hacer que las variables persistan en sesiones futuras configurándolas en el script de startup del intérprete de comandos.

Windows Command Prompt

```
C:\> setx JAVA_TOOL_OPTIONS -Daws.region=us-east-1
```

El uso de [set](#) para configurar una variable de entorno cambia el valor usado hasta que finalice la sesión de Símbolo del Sistema actual o hasta que otorgue a la variable un valor diferente. El uso de [setx](#) para establecer una variable de entorno cambia el valor usado en la sesión de Símbolo del Sistema actual y en todas las sesiones de Símbolo del Sistema que cree después de ejecutar el comando. La operación no afecta a otros comandos del shell que ya se están ejecutando en el momento de ejecutar el comando.

## En tiempo de ejecución

También puede establecer las propiedades del sistema JVM en tiempo de ejecución en el código mediante el `System.setProperty` método que se muestra en el siguiente ejemplo.

```
System.setProperty("aws.region", "us-east-1");
```

### Important

Establezca las propiedades del sistema JVM antes de inicializar los clientes del servicio del SDK; de lo contrario, los clientes del servicio podrían utilizar otros valores.

# Autenticación y acceso

Debe establecer cómo se autentica su código AWS cuando desarrolla con Servicios de AWS. Puede configurar el acceso programático a AWS los recursos de diferentes maneras, según el entorno y el AWS acceso del que disponga.

Opciones de autenticación para el código que se ejecuta de forma local (no interna en AWS)

- [IAM Autenticación de Identity Center para su SDK herramienta](#)— Como práctica recomendada de seguridad, le recomendamos que utilice AWS Organizations IAM Identity Center para gestionar el acceso en todos sus Cuentas de AWS dispositivos. Puede crear usuarios en Microsoft Active Directory AWS IAM Identity Center, usar un proveedor de identidades (IdP) SAML 2.0 o federar individualmente su IdP a. Cuentas de AWS Para comprobar si su región es compatible con IAM Identity Center, consulte los [AWS IAM Identity Center puntos finales y](#) las cuotas en. Referencia general de Amazon Web Services
- [Funciones de IAM en cualquier lugar](#)— Puede utilizar IAM Roles Anywhere para obtener credenciales de seguridad temporales IAM para cargas de trabajo, como servidores, contenedores y aplicaciones que se ejecutan fuera de él. AWS Para usar IAM Roles Anywhere, tus cargas de trabajo deben usar certificados X.509.
- [Asume un rol con AWS credenciales](#)— Puedes asumir un IAM rol para acceder temporalmente a AWS recursos a los que de otro modo no tendrías acceso.
- [AWS claves de acceso](#)— Otras opciones que podrían resultar menos prácticas o que podrían aumentar el riesgo de seguridad de sus AWS recursos.

Opciones de autenticación para el código que se ejecuta en un AWS entorno

Si el código se ejecuta AWS, las credenciales se pueden poner automáticamente a disposición de la aplicación. Por ejemplo, si su aplicación está alojada en Amazon Elastic Compute Cloud y hay un IAM rol asociado a ese recurso, las credenciales estarán disponibles automáticamente para su aplicación. Del mismo modo, si utilizas Amazon ECS o EKS contenedores de Amazon, el código que se ejecuta dentro del contenedor a través de la cadena de proveedores de credenciales del IAM rol puede obtener automáticamente las SDK credenciales configuradas para el rol.

- [Uso de IAM roles para EC2 instancias de Amazon](#)— Usa IAM roles para ejecutar tu aplicación de forma segura en una EC2 instancia de Amazon.

- Puede interactuar mediante programación mediante el AWS uso de IAM Identity Center de las siguientes maneras:
  - Se utiliza [AWS CloudShell](#) para ejecutar AWS CLI comandos desde la consola.
  - Si quieres probar un espacio de colaboración basado en la nube para equipos de desarrollo de software, considera usar [Amazon CodeCatalyst](#).

Autenticación a través de un proveedor de identidades basado en web, aplicaciones web móviles o basadas en cliente

Si va a crear aplicaciones móviles o aplicaciones web basadas en clientes a las que es necesario acceder AWS, cree su aplicación de manera que solicite credenciales de AWS seguridad temporales de forma dinámica mediante la federación de identidades web.

Con la federación de identidades web no necesita crear código de inicio de sesión personalizado ni administrar sus propias identidades de usuario. En su lugar, los usuarios de la aplicación pueden iniciar sesión con un proveedor de identidad externo (IdP) conocido, como Login with Amazon, Facebook, Google o cualquier otro IdP compatible con OpenID Connect (OIDC). Pueden recibir un token de autenticación y, a continuación, cambiarlo por credenciales de seguridad temporales en AWS ese mapa por un IAM rol con permisos para usar sus recursos. Cuenta de AWS

Para obtener información sobre cómo configurar esto para su SDK herramienta, consulte [Asume un rol con identidad web o OpenID Connect](#).

Para aplicaciones móviles, le recomendamos que utilice Amazon Cognito. Amazon Cognito actúa como agente de identidades y realiza gran parte del trabajo de federación por usted. Para obtener más información, consulte [Uso de Amazon Cognito para aplicaciones móviles](#) en la Guía del IAM usuario.

Más información sobre la administración de acceso

La guía del IAM usuario contiene la siguiente información sobre cómo controlar de forma segura el acceso a AWS los recursos:

- [IAM identidades \(usuarios, grupos de usuarios y roles\)](#): comprenda los conceptos básicos de las identidades en AWS.
- [Prácticas recomendadas de seguridad en IAM](#): recomendaciones de seguridad que se deben seguir al desarrollar AWS aplicaciones de acuerdo con el modelo de [responsabilidad compartida](#).

Referencia general de Amazon Web Services tiene los conceptos básicos sobre lo siguiente:

- [Comprender y obtener sus AWS credenciales](#): acceda a las principales opciones y prácticas de administración tanto para el acceso mediante consola como mediante programación.

## ID de creador de AWS

ID de creador de AWS Complementa cualquier Cuentas de AWS cosa que ya tengas o quieras crear. Si bien a Cuenta de AWS actúa como contenedor de los AWS recursos que usted crea y proporciona un límite de seguridad para esos recursos, usted lo ID de creador de AWS representa como individuo. Puedes iniciar sesión con tu cuenta ID de creador de AWS para acceder a herramientas y servicios para desarrolladores, como Amazon CodeWhisperer y Amazon CodeCatalyst.

- [Inicia ID de creador de AWS sesión con](#) la Guía del AWS Sign-In usuario: aprende a crear y usar una ID de creador de AWS y descubre qué te proporciona el Builder ID.
- [Autenticación con CodeWhisperer un ID de constructor](#) en la guía del CodeWhisperer usuario: aprenda a utilizar CodeWhisperer un ID de creador de AWS. AWS Toolkit
- [CodeCatalyst conceptos: ID de creador de AWS](#) en la Guía del CodeCatalyst usuario de Amazon: aprenda cómo se CodeCatalyst usa un ID de creador de AWS.

## IAM Autenticación de Identity Center para su SDK herramienta

AWS IAM Identity Center es el método recomendado para proporcionar AWS credenciales cuando se desarrolla en un servicio que no es AWS informático. Por ejemplo, sería algo así como su entorno de desarrollo local. Si estás desarrollando en un AWS recurso, como Amazon Elastic Compute Cloud (AmazonEC2) o AWS Cloud9, te recomendamos que obtengas las credenciales de ese servicio en su lugar.

En este tutorial, establecerá el acceso al IAM Identity Center y lo configurará para su SDK herramienta mediante el portal de AWS acceso y el AWS CLI.

- El portal de AWS acceso es la ubicación web en la que se inicia sesión manualmente en el IAM Identity Center. El formato de URL es `d-xxxxxxxxxx.awsapps.com/start` *o* `your_subdomain.awsapps.com/start`. Al iniciar sesión en el portal de AWS acceso, puede ver Cuentas de AWS los roles que se han configurado para ese usuario. Este procedimiento utiliza el portal de AWS acceso para obtener los valores de configuración que necesita para el proceso de autenticación SDK /tool.

- **AWS CLI** Se utiliza para configurar su SDK herramienta para que utilice la autenticación del Centro de IAM Identidad para API las llamadas realizadas con su código. Este proceso único actualiza el AWS config archivo compartido, que luego es utilizado por la herramienta SDK o al ejecutar el código.

## Configure el acceso mediante programación mediante IAM Identity Center

### Paso 1: establecer el acceso y seleccionar el conjunto de permisos adecuado

Si aún no ha activado IAM Identity Center, consulte [Habilitar IAM Identity Center](#) en la Guía del AWS IAM Identity Center usuario.

Elija uno de los siguientes métodos para acceder a sus AWS credenciales.

No tengo un acceso establecido a través de IAM Identity Center

1. Añada un usuario y añada permisos administrativos siguiendo el procedimiento para [configurar el acceso de los usuarios con el directorio predeterminado de IAM Identity Center](#) de la Guía del AWS IAM Identity Center usuario.
2. El conjunto de `AdministratorAccess` permisos no debe utilizarse para un desarrollo normal. En su lugar, le recomendamos que utilice el conjunto de `PowerUserAccess` permisos predefinido, a menos que su empresa haya creado un conjunto de permisos personalizado para este fin.

Siga el mismo procedimiento [para configurar el acceso de los usuarios con el directorio predeterminado del Centro de IAM Identidad](#), pero esta vez:

- En lugar de crear el *Admin team* grupo, cree un *Dev team* grupo y sustitúyalo a continuación en las instrucciones.
- Puede usar el usuario existente, pero debe agregarlo al nuevo *Dev team* grupo.
- En lugar de crear el conjunto de *AdministratorAccess* permisos, cree un conjunto de *PowerUserAccess* permisos y sustitúyalo posteriormente en las instrucciones.

Cuando haya terminado, debería disponer de lo siguiente:

- Un `Dev team` grupo.
- Un conjunto de `PowerUserAccess` permisos adjunto al `Dev team` grupo.

- El usuario se ha añadido al Dev team grupo.
3. Salga del portal e inicie sesión de nuevo para ver sus opciones Cuentas de AWS y para `Administrator` o `PowerUserAccess`. Seleccione `PowerUserAccess` cuando trabaje con su herramienta/SDK.

Ya tengo acceso a AWS través de un proveedor de identidad federado administrado por mi empresa (como Microsoft Entra u Okta)

Inicia sesión a AWS través del portal de tu proveedor de identidad. Si el administrador de la nube te ha concedido permisos `PowerUserAccess` (de desarrollador), verás aquellos a los Cuentas de AWS que tienes acceso y tu conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Las implementaciones personalizadas pueden dar lugar a experiencias diferentes, como distintos nombres de conjuntos de permisos. Si no está seguro de qué configuración de permisos debe utilizar, contacte con su equipo de TI para obtener ayuda.

Ya tengo acceso a él a AWS través del portal de AWS acceso gestionado por mi empresa

Inicie sesión a AWS través del portal de AWS acceso. Si su administrador de la nube le ha concedido permisos `PowerUserAccess` (desarrollador), verá las Cuentas de AWS a las que tiene acceso y su conjunto de permisos. Junto al nombre de su conjunto de permisos, verá las opciones para acceder a las cuentas de forma manual o programática mediante ese conjunto de permisos.

Ya tengo acceso a AWS través de un proveedor de identidad personalizado federado administrado por mi empleador

Contacte con su equipo de TI para obtener ayuda.

## Paso 2: Configurar SDKs y usar las herramientas para usar IAM Identity Center

1. En su máquina de desarrollo, instale la versión más reciente de la AWS CLI.
  - a. Consulte [Instalar o actualizar la versión más reciente de la AWS CLI](#) en la Guía del usuario de AWS Command Line Interface .
  - b. (Opcional) Para comprobar que AWS CLI funciona, abra una línea de comandos y ejecute el `aws --version` comando.

2. Inicie sesión en el portal de AWS acceso. Su empleador puede proporcionárselo URL o puede recibirlo por correo electrónico siguiendo el paso 1: Establecer el acceso. Si no es así, busque su portal de AWS acceso URL en el panel de control de <https://console.aws.amazon.com/singlesignon/>.
  - a. En el portal de AWS acceso, en la pestaña Cuentas, seleccione la cuenta individual que desee administrar. Se muestran las funciones de su usuario. Elija las claves de acceso para obtener las credenciales de acceso mediante línea de comandos o mediante programación para el conjunto de permisos correspondiente. Utilice el conjunto de permisos `PowerUserAccess` predefinido o el conjunto de permisos que usted o su empleador hayan creado para aplicar permisos de privilegio mínimo para el desarrollo.
  - b. En el cuadro de diálogo Obtener credenciales, elija MacOS y Linux o Windows, en función del sistema operativo.
  - c. Elija el método de credenciales de IAM Identity Center para obtener los SS0 Region valores `Issuer URL` y valores que necesita para el siguiente paso. Nota: se SS0 Start URL puede usar indistintamente con. `Issuer URL`
3. En la AWS CLI línea de comandos, ejecute el `aws configure sso` comando. Cuando se le solicite, introduzca los valores de configuración que recopiló en el paso anterior. Para obtener más información sobre este AWS CLI comando, consulte [Configurar su perfil con el aws configure sso asistente](#).
  - a. En el mensaje SS0 Start URL, introduzca el valor para el que ha obtenido `Issuer URL`.
  - b. Para el nombre del CLI perfil, le recomendamos que lo introduzca *default* al empezar. Para obtener información sobre cómo configurar perfiles no predeterminados (con nombre) y su variable de entorno asociada, consulte [Perfiles](#).
4. (Opcional) En la AWS CLI línea de comandos, confirme la identidad de la sesión activa ejecutando el `aws sts get-caller-identity` comando. La respuesta debería mostrar el conjunto de permisos de IAM Identity Center que configuró.
5. Si está utilizando un AWS SDK, cree una aplicación para usted SDK en su entorno de desarrollo.
  - a. En el caso de algunos SDKs, es SS00IDC necesario añadir paquetes adicionales a la aplicación antes de poder utilizar la autenticación de IAM Identity Center. SS0 Para obtener más información, consulte su información específica SDK.
  - b. Si anteriormente configuraste el acceso a AWS, revisa tu `AWS credentials` archivo compartido para ver si hay alguno [AWS claves de acceso](#). Debido a la [Comprenda la cadena](#)

[de proveedores de credenciales](#) prioridad, debe eliminar todas las credenciales estáticas antes de que la herramienta SDK o herramienta utilice las credenciales del Centro de IAM Identidad.

Para obtener información detallada sobre cómo las herramientas SDKs y herramientas utilizan y actualizan las credenciales con esta configuración, consulte [Comprender la autenticación del Centro de identidades de IAM](#).

En función de la duración de las sesiones configuradas, el acceso eventualmente caducará y la SDK herramienta detectará un error de autenticación. Para volver a actualizar la sesión del portal de acceso cuando sea necesario, utilice el comando AWS CLI para ejecutar el `aws sso login` comando.

Puede ampliar tanto la duración de la sesión del portal de acceso a IAM Identity Center como la duración de la sesión del conjunto de permisos. Esto prolonga el tiempo que puede ejecutar el código antes de tener que volver a iniciar sesión manualmente con la AWS CLI. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS IAM Identity Center :

- IAM Duración de la sesión de Identity Center: [configure la duración de las sesiones del portal de AWS acceso de sus usuarios](#)
- Duración de la sesión establecida por permisos: [establecer la duración de la sesión](#)

Para obtener más información sobre todos los ajustes SDKs y las herramientas de los proveedores de IAM Identity Center, consulte [IAM Proveedor de credenciales de Identity Center](#) esta guía.

## Comprender la autenticación del Centro de identidades de IAM

### Términos relevantes del Centro de identidades de IAM

Los siguientes términos le ayudan a entender el proceso y la configuración subyacentes en AWS IAM Identity Center. La documentación de las API del SDK de AWS utiliza nombres diferentes a los del Centro de identidades de IAM para algunos de estos conceptos de autenticación. Resulta útil conocer ambos nombres.

En la siguiente tabla, se muestra cómo se relacionan entre sí los nombres alternativos.

Nombre del Centro de identidades de IAM	Nombre de la API del SDK	Descripción
Centro de identidades	sso	Aunque se haya cambiado el nombre de inicio de sesión único de AWS, los espacios de nombres de las API de sso mantendrán su nombre original por motivos de compatibilidad con versiones anteriores. Para más información, consulte <a href="#">Cambiar el nombre del Centro de identidades de IAM</a> en la Guía del usuario de AWS IAM Identity Center.
Consola del Centro de identidades de IAM Consola administrativa		La consola que se utiliza para configurar el inicio de sesión único.
URL del portal de acceso a AWS		Una URL exclusiva de su cuenta del Centro de identidades de IAM, como <code>https://xxx.awsapps.com/start</code> . Inicie sesión en este portal con sus credenciales de inicio de sesión del Centro de identidad de IAM.
Sesión del Portal de Acceso del Centro de identidades de IAM	Sesión de autenticación	Proporciona un token de acceso al portador al intermediario.
Sesión del conjunto de permisos		La sesión de IAM que el SDK usa internamente para realizar

Nombre del Centro de identidades de IAM	Nombre de la API del SDK	Descripción
		las llamadas de Servicio de AWS. En las discusiones informales, es posible que vea que esto se denomina incorrectamente “sesión de roles”.
Credenciales de configuración de permisos	Credenciales de AWS Single Sign-On  credenciales de sigv4	Las credenciales que el SDK utiliza realmente para la mayoría de las llamadas de Servicio de AWS (específicamente, todas las llamadas sigv4 de Servicio de AWS). En las discusiones informales, es posible que veas que esto se denomina incorrectamente “credenciales de roles”.
Proveedor de credenciales del IAM Identity Center	Proveedor de credenciales SSO	Cómo se obtienen las credenciales, como la clase o el módulo que proporciona la funcionalidad.

## Comprenda la resolución de credenciales del SDK para Servicios de AWS

La API del IAM Identity Center intercambia credenciales de token de portador por credenciales sigv4. La mayoría son API sigv4 de Servicios de AWS, con algunas excepciones, como Amazon CodeWhisperer y Amazon CodeCatalyst. A continuación, se describe el proceso de resolución de credenciales para admitir la mayoría de las llamadas de Servicio de AWS mediante el código de la aplicación AWS IAM Identity Center.

### Iniciar una sesión en el portal de acceso a AWS

- Inicie el proceso iniciando sesión con sus credenciales.

- Use el comando de `aws sso login` en el AWS Command Line Interface (AWS CLI). Esto inicia una nueva sesión en el IAM Identity Center si aún no tiene una sesión activa.
- Al iniciar una nueva sesión, recibirá un token de actualización y un token de acceso del IAM Identity Center. El AWS CLI también actualiza un archivo JSON de la caché del SSO con un nuevo token de acceso y un token de actualización, y lo pone a disposición de los SDK para que lo utilicen.
- Si ya tiene una sesión activa, el AWS CLI comando reutiliza la sesión existente y caducará cuando caduque la sesión existente. Para obtener información sobre cómo establecer la duración de una sesión del IAM Identity Center, consulte [Configurar la duración de las sesiones del portal de acceso de los usuarios de AWS](#) en la AWS IAM Identity Center Guía del usuario.
- La duración máxima de la sesión se ha ampliado a 90 días para reducir la necesidad de iniciar sesión con frecuencia.

## Cómo obtiene el SDK las credenciales para las llamadas a Servicio de AWS

Los SDK proporcionan acceso a Servicios de AWS cuando se crea una instancia de un objeto de cliente por servicio. Cuando el perfil seleccionado del archivo compartido de AWS config está configurado para la resolución de credenciales del IAM Identity Center, el IAM Identity Center se utiliza para resolver las credenciales de su aplicación.

- El [proceso de resolución de credenciales](#) se completa durante el tiempo de ejecución cuando se crea un cliente.

Para recuperar las credenciales de las API sigv4 mediante el inicio de sesión único del IAM Identity Center, el SDK utiliza el token de acceso al IAM Identity Center para obtener una sesión de IAM. Esta sesión de IAM se denomina sesión de conjunto de permisos y proporciona a AWS acceso al SDK al asumir un rol de IAM.

- La duración de la sesión del conjunto de permisos se establece independientemente de la duración de la sesión del IAM Identity Center.
  - Para obtener información sobre cómo configurar la duración de la sesión del conjunto de permisos, consulte [Establecer la duración de la sesión](#) en la Guía del usuario de AWS IAM Identity Center.
- Ten en cuenta que las credenciales del conjunto de permisos también se denominan credenciales de AWS y credenciales sigv4 en la mayoría de la documentación de la API del SDK de AWS.

Las credenciales del conjunto de permisos se devuelven de una llamada a [getRoleCredentials](#) de la API del Centro de identidades de IAM al SDK. El objeto cliente del SDK utiliza ese supuesto rol de IAM para realizar llamadas al Servicio de AWS, por ejemplo, pedir a Amazon S3 que incluya los buckets en su cuenta. El objeto de cliente puede seguir funcionando con esas credenciales del conjunto de permisos hasta que caduque la sesión del conjunto de permisos.

### Caducidad y actualización de la sesión

Al utilizar el [SSO configuración del proveedor de tokens](#), el token de acceso por hora obtenido del Centro de identidades de IAM se actualiza automáticamente mediante el token de actualización.

- Si el token de acceso ha caducado cuando el SDK intenta usarlo, el SDK utiliza el token de actualización para intentar obtener un nuevo token de acceso. El Centro de identidades de IAM compara el token de actualización con la duración de la sesión del portal de acceso al Centro de identidades de IAM. Si el token de actualización no ha caducado, el Centro de identidades de IAM responde con otro token de acceso.
- Este token de acceso se puede utilizar para actualizar la sesión del conjunto de permisos de los clientes existentes o para resolver las credenciales de los nuevos clientes.

Sin embargo, si la sesión del portal de acceso del Centro de identidades de IAM ha caducado, no se concede ningún token de acceso nuevo. Por lo tanto, la duración del conjunto de permisos no se puede renovar. Caducará (y se perderá el acceso) cuando se agote el tiempo de espera de la sesión del conjunto de permisos almacenado en caché para los clientes existentes.

Cualquier código que cree un nuevo cliente no se autenticará en cuanto caduque la sesión del Centro de identidades de IAM. Esto se debe a que las credenciales del conjunto de permisos no se almacenan en caché. Su código no podrá crear un nuevo cliente ni completar el proceso de resolución de credenciales hasta que tenga un token de acceso válido.

En resumen, cuando el SDK necesita nuevas credenciales de conjunto de permisos, primero compruebe si hay credenciales válidas y existentes y si las utiliza. Esto se aplica tanto si las credenciales son para un cliente nuevo como para un cliente existente con credenciales caducadas. Si no se encuentran las credenciales o no son válidas, el SDK llama a la API del Centro de identidades de IAM para obtener nuevas credenciales. Para llamar a la API, necesita el token de acceso. Si el token de acceso ha caducado, el SDK utiliza el token de actualización para intentar obtener un nuevo token de acceso del servicio del Centro de identidades de IAM. Este token se concede si la sesión del portal de acceso al IAM Identity Center no ha caducado.

# Funciones de IAM en cualquier lugar

Puede utilizar Funciones de IAM en cualquier lugar para obtener credenciales de seguridad temporales en IAM para cargas de trabajo, como servidores, contenedores y aplicaciones que se ejecutan fuera de AWS. Para utilizar Funciones de IAM en cualquier lugar, sus cargas de trabajo deben utilizar certificados X.509. El administrador de la nube debe proporcionar el certificado y la clave privada necesarios para configurar Funciones de IAM en cualquier lugar como su proveedor de credenciales.

## Paso 1: Configurar las Funciones de IAM en cualquier lugar

Las funciones de IAM en cualquier lugar proporcionan una forma de obtener credenciales temporales para una carga de trabajo o un proceso que se ejecuta fuera de AWS. Se establece un anclaje de confianza con la autoridad de certificación para obtener credenciales temporales para el rol de IAM asociado. El rol establece los permisos que tendrá su carga de trabajo cuando su código se autentique con las Funciones de IAM en cualquier lugar.

Para ver los pasos necesarios para configurar el anclaje de confianza, el rol de IAM y el perfil de Funciones de IAM en cualquier lugar, consulte [Creación de un anclaje de confianza y un perfil en Funciones de AWS Identity and Access Management en cualquier lugar](#) en la Guía del usuario de Funciones de IAM en cualquier lugar.

### Note

Un perfil en la Guía de usuario de Funciones de IAM en cualquier lugar hace referencia a un concepto exclusivo del servicio de Funciones de IAM en cualquier lugar. No está relacionado con los perfiles del archivo compartido AWS config.

## Paso 2: Utilice las funciones de IAM en cualquier lugar

Para obtener credenciales de seguridad temporales de Funciones de IAM en cualquier lugar, utilice la herramienta ayudante de credenciales proporcionada por Funciones de IAM en cualquier lugar. La herramienta de credenciales implementa el proceso de firma de Funciones de IAM en cualquier lugar.

Para obtener instrucciones sobre cómo descargar la herramienta del ayudante de credenciales, consulte [Obtener credenciales de seguridad temporales de Funciones de AWS Identity and Access Management en cualquier lugar](#) en la Guía del usuario de Funciones de IAM en cualquier lugar.

Para utilizar credenciales de seguridad temporales de Funciones de IAM en cualquier lugar con los SDK de AWS y el AWS CLI, puede configurar `credential_process` los ajustes del archivo compartido AWS `config`. Los SDK y AWS CLI son compatibles con un proveedor de credenciales de proceso que se utiliza `credential_process` para autenticarse. A continuación se muestra la estructura general para establecer `credential_process`.

```
credential_process = [path to helper tool] [command] [--parameter1 value] [--parameter2 value] [...]
```

El comando `credential-process` de la herramienta auxiliar devuelve las credenciales temporales en un formato JSON estándar que es compatible con la configuración `credential_process`. Tenga en cuenta que el nombre del comando contiene un guión, pero el nombre de la configuración contiene un guión bajo. El comando requiere los parámetros siguientes:

- `private-key` – La ruta a la clave privada que firmó la solicitud.
- `certificate` – La ruta al certificado.
- `role-arn` – El ARN del rol para el que se van a obtener las credenciales temporales.
- `profile-arn` – El ARN del perfil que proporciona una asignación para el rol especificado.
- `trust-anchor-arn` – El ARN del anclaje de confianza usado para autenticar.

Su administrador de la nube debe proporcionarle el certificado y la clave privada. Los tres valores del ARN se pueden copiar de AWS Management Console. El siguiente ejemplo muestra un archivo compartido `config` que configura la recuperación de credenciales temporales de la herramienta auxiliar.

```
[profile dev]  
credential_process = ./aws_signing_helper credential-process --certificate /  
path/to/certificate --private-key /path/to/private-key --trust-anchor-  
arn arn:aws:rolesanywhere:region:account:trust-anchor/TA_ID --profile-  
arn arn:aws:rolesanywhere:region:account:profile/PROFILE_ID --role-  
arn arn:aws:iam::account:role/ROLE_ID
```

Para ver los parámetros opcionales y los detalles adicionales de las herramientas auxiliares, consulte el [Ayudante de credenciales de las Funciones de IAM en cualquier lugar](#) en GitHub.

Para obtener más información sobre el ajuste de configuración del SDK en sí y el proveedor de credenciales del proceso, consulte [Proveedor de credenciales de proceso](#) en esta guía.

## Asume un rol con AWS credenciales

Para asumir un rol, se utiliza un conjunto de credenciales de seguridad temporales para acceder a los recursos de AWS a los que de otro modo usted no tendría acceso. Las credenciales temporales incluyen un ID de clave de acceso, una clave de acceso secreta y un token de seguridad. Para obtener más información sobre API las solicitudes AWS Security Token Service (AWS STS), consulte [Acciones](#) en la AWS Security Token Service API referencia.

Para configurar su herramienta SDK o su herramienta para que asuma un rol, primero debe crear o identificar el rol específico que desee asumir. IAM los roles se identifican de forma única mediante un rol: Amazon Resource Name ([ARN](#)). Los roles establecen relaciones de confianza con otra entidad. La entidad de confianza que usa el rol puede ser una Servicio de AWS u otra Cuenta de AWS. Para obtener más información sobre IAM los roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

Una vez identificado el IAM rol, si ese rol confía en usted, puede configurar su SDK herramienta para que utilice los permisos que otorga el rol.

### Note

Se AWS recomienda utilizar puntos de enlace regionales siempre que sea posible y configurar los suyos [Región de AWS](#).

## Asume cualquier rol IAM

Al asumir un rol, AWS STS devuelve un conjunto de credenciales de seguridad temporales. Estas credenciales provienen de otro perfil o de la instancia o contenedor en el que se ejecuta el código. Por lo general, este tipo de asunción de un rol se utiliza cuando tienes AWS credenciales para una cuenta, pero tu aplicación necesita acceder a los recursos de otra cuenta.

### Paso 1: Configurar un IAM rol

Para configurar su herramienta SDK o herramienta para que asuma un rol, primero debe crear o identificar el rol específico que desee asumir. IAM los roles se identifican de forma exclusiva mediante un rol [ARN](#). Los roles establecen relaciones de confianza con otra entidad, normalmente dentro de su cuenta o para el acceso entre cuentas. Para configurarlo, consulte [Creación de IAM roles](#) en la Guía del IAM usuario.

## Paso 2: Configure la herramienta SDK o

Configure la herramienta SDK o para obtener las credenciales de `credential_source` o `source_profile`.

Se usa `credential_source` para obtener credenciales de un ECS contenedor de Amazon, una EC2 instancia de Amazon o variables de entorno.

Se utiliza `source_profile` para obtener credenciales de otro perfil. `source_profile` también admite el encadenamiento de roles, que consiste en jerarquías de perfiles en las que se utiliza un rol asumido para asumir otro rol.

Cuando lo especificas en un perfil, la herramienta SDK o herramienta realiza automáticamente la AWS STS [AssumeRole](#) API llamada correspondiente por ti. Para recuperar y usar credenciales temporales asumiendo un rol, especifique los siguientes valores de configuración en el AWS `config` archivo compartido. Para obtener más información sobre esta configuración, consulte la sección [Asumir la configuración del proveedor de credenciales de rol](#).

- `role_arn`- Del IAM rol que creó en el paso 1
- Configure una de las siguientes opciones: `source_profile` o `credential_source`
- (Opcional) `duration_seconds`
- (Opcional) `external_id`
- (Opcional) `mfa_serial`
- (Opcional) `role_session_name`

Los siguientes ejemplos muestran la configuración de ambas opciones de asumir roles en un archivo `config` compartido:

```
role_arn = arn:aws:iam::123456789012:role/my-role-name
source_profile = profile-name-with-user-that-can-assume-role
```

```
role_arn = arn:aws:iam::123456789012:role/my-role-name
credential_source = Ec2InstanceMetadata
```

Para obtener más información sobre la configuración del proveedor de credenciales de rol, consulte [Asumir el rol de proveedor de credenciales](#) en esta guía.

## Asume un rol con identidad web o OpenID Connect

Para asumir un rol, se utiliza un conjunto de credenciales de seguridad temporales para acceder a los recursos de AWS a los que de otro modo usted no tendría acceso. Las credenciales temporales incluyen un ID de clave de acceso, una clave de acceso secreta y un token de seguridad. Para obtener más información sobre API las solicitudes AWS Security Token Service (AWS STS), consulte [Acciones](#) en la AWS Security Token Service API referencia.

Para configurar su herramienta SDK o su herramienta para que asuma un rol, primero debe crear o identificar el rol específico que desee asumir. IAM los roles se identifican de forma única mediante un rol: Amazon Resource Name ([ARN](#)). Los roles establecen relaciones de confianza con otra entidad. La entidad de confianza que usa el rol puede ser un proveedor de identidad web, OpenID Connect (OIDC) o SAML una federación. Para obtener más información sobre IAM las funciones, consulte [Métodos para asumir una función](#) en la Guía del IAM usuario.

Una vez configurada la IAM función en su empresa SDK, si esa función está configurada para confiar en su proveedor de identidad, puede configurarla aún más SDK para que asuma esa función a fin de obtener AWS credenciales temporales.

### Note

Se AWS recomienda utilizar puntos de enlace regionales siempre que sea posible y configurar los suyos [Región de AWS](#).

## Cómo federar con identidad web u OpenID Connect

Puede utilizar los JSON Web Tokens (JWTs) de proveedores de identidad públicos, como Login With Amazon, Facebook o Google, para obtener AWS credenciales temporales `AssumeRoleWithWebIdentity`. Según cómo se usen, JWTs pueden denominarse tokens de identificación o tokens de acceso. También puede utilizar proveedores de identidad JWTs emitidos por proveedores de identidad (IdPs) que sean compatibles con OIDC el protocolo de descubrimiento, como EntraId o PingFederate.

Si utiliza Amazon Elastic Kubernetes Service, esta función permite especificar IAM diferentes funciones para cada una de sus cuentas de servicio en un clúster de Amazon. EKS Esta función de Kubernetes se distribuye entre JWTs sus pods, que luego este proveedor de credenciales los utiliza para obtener credenciales temporales. AWS Para obtener más información sobre esta EKS

configuración de Amazon, consulta las [IAM funciones de las cuentas de servicio](#) en la Guía del EKS usuario de Amazon. Sin embargo, para una opción más sencilla, te recomendamos que utilices [Amazon EKS Pod Identities](#) en su lugar si [SDK lo permite](#).

## Paso 1: Configura un proveedor de identidades y un IAM rol

Para configurar la federación con un IdP externo, utilice un proveedor de IAM identidades para informar AWS sobre el IdP externo y su configuración. Esto establece la confianza entre su IdP Cuenta de AWS y el externo. Antes de SDK configurar el uso del JSON Web Token (JWT) para la autenticación, primero debe configurar el proveedor de identidad (IdP) y el IAM rol utilizado para acceder a él. Para configurar los, consulte [Creación de un rol para la identidad web o OpenID Connect Federation \(consola\)](#) en la Guía del IAM usuario.

## Paso 2: Configure la herramienta SDK or

Configure la herramienta SDK o para usar un token JSON web (JWT) AWS STS para la autenticación.

Cuando lo especificas en un perfil, la herramienta SDK o herramienta realiza automáticamente la AWS STS [AssumeRoleWithWebIdentity](#) API llamada correspondiente por ti. Para recuperar y usar credenciales temporales mediante la federación de identidades web, especifique los siguientes valores de configuración en el AWS config archivo compartido. Para obtener más información sobre esta configuración, consulte la sección [Asumir la configuración del proveedor de credenciales de rol](#).

- `role_arn`- Del IAM rol que creó en el paso 1
- `web_identity_token_file`: desde el IdP externo
- (Opcional) `duration_seconds`
- (Opcional) `role_session_name`

El siguiente es un ejemplo de una configuración de archivos compartidos config para asumir un rol con identidad web:

```
[profile web-identity]  
role_arn=arn:aws:iam::123456789012:role/my-role-name  
web_identity_token_file=/path/to/a/token
```

 Note

Para aplicaciones móviles, le recomendamos que utilice Amazon Cognito. Amazon Cognito actúa como agente de identidades y realiza gran parte del trabajo de federación por usted. Sin embargo, el proveedor de identidades de Amazon Cognito no está incluido en las bibliotecas principales de herramientas SDKs y herramientas como otros proveedores de identidades. Para acceder a Amazon CognitoAPI, incluya el cliente del servicio Amazon Cognito en la compilación o las bibliotecas de su herramienta o herramienta. SDK Para su uso con AWS SDKs, consulte los [ejemplos de código](#) en la Guía para desarrolladores de Amazon Cognito.

Para obtener más información sobre la configuración del proveedor de credenciales de rol, consulte [Asumir el rol de proveedor de credenciales](#) en esta guía.

## AWS claves de acceso

### Use credenciales a corto plazo.

Recomendamos configurar su SDK o herramienta para utilizar [IAM Autenticación de Identity Center para su SDK herramienta](#) para usar opciones de duración de sesión ampliada.

Sin embargo, para configurar directamente las credenciales temporales del SDK o de la herramienta, consulte [Autenticación mediante credenciales a corto plazo](#).

### Use credenciales a largo plazo.

 Warning

Para evitar riesgos de seguridad, no utilice a los usuarios de IAM para la autenticación cuando desarrolle software especialmente diseñado o trabaje con datos reales. En cambio, utilice la federación con un proveedor de identidades como [AWS IAM Identity Center](#).

## Gestione el acceso en todas las Cuentas de AWS

Como práctica recomendada de seguridad, te recomendamos que utilices AWS Organizations IAM Identity Center para gestionar el acceso en todas tus Cuentas de AWS. Para más información, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Puede crear usuarios en el Centro de identidades de IAM, usar Microsoft Active Directory, usar un proveedor de identidades (IdP) SAML 2.0 o federar individualmente su IdP a Cuentas de AWS. Con una de estas opciones podrá ofrecer a sus usuarios una experiencia de inicio de sesión único. También puede aplicar la autenticación multifactor (MFA) y utilizar credenciales de Cuenta de AWS temporales para el acceso. El caso de un usuario de IAM es diferente, ya que utiliza una credencial de larga duración que se puede compartir y que podría aumentar el riesgo de seguridad de sus recursos de AWS.

### Creación de usuarios de IAM únicamente para entornos aislados

Si es la primera vez que lo usa AWS, puede crear un usuario de IAM de prueba y luego usarlo para ejecutar tutoriales y explorar lo que AWS ofrece. Está bien usar este tipo de credenciales cuando se está aprendiendo, pero no recomendamos usarlas fuera de un entorno aislado.

Para los siguientes casos de uso, podría ser conveniente empezar con los usuarios de IAM en: AWS

- Cómo empezar a utilizar el AWS SDK o la herramienta y explorar los Servicios de AWS en un entorno aislado.
- Como parte de su aprendizaje, ejecute scripts, trabajos y otros procesos automatizados programados que no admitan un proceso de inicio de sesión asistido por una persona.

Si utilizas usuarios de IAM fuera de estos casos de uso, cámbiate al Centro de Identidad de IAM o federa tu proveedor de identidades de Cuentas de AWS lo antes posible. Para obtener más información, consulte [Federación de identidades en AWS](#).

### Seguridad para las claves de acceso de los usuarios de IAM

Debe rotar las claves de acceso de los usuarios de IAM regularmente. Siga las instrucciones de [Rotación de las claves de acceso](#) disponibles en la Guía del usuario de IAM. Si considera que puede haber compartido accidentalmente sus claves de acceso de usuario de IAM, cámbielas.

Las claves de acceso de los usuarios de IAM deben almacenarse en el `AWS credentials` archivo compartido de la máquina local. No guarde las claves de acceso de los usuarios de IAM en su

código. No incluya archivos de configuración que contengan sus claves de acceso de usuario de IAM en ningún software de administración de código fuente. Las herramientas externas, como el proyecto de código abierto [git-secrets](#), pueden ayudarle a no enviar información confidencial accidentalmente a un repositorio de Git. Para obtener más información acerca de los usuarios de IAM, consulte [Identidades IAM \(usuarios, grupos y funciones\)](#) en la Guía de usuario de IAM.

Para configurar un usuario de IAM para empezar, consulte [Autenticar mediante credenciales a largo plazo](#).

## Autenticación mediante credenciales a corto plazo

Le recomendamos configurar su herramienta SDK o herramienta para utilizarla [IAMAutenticación de Identity Center para su SDK herramienta](#) con opciones de duración de sesión prolongada. Sin embargo, puede copiar y usar las credenciales temporales que están disponibles en el portal de AWS acceso. Las credenciales nuevas deberán copiarse cuando caduquen. Puede utilizar las credenciales temporales en un perfil o como valores para las propiedades del sistema y las variables de entorno.

Práctica recomendada: en lugar de administrar manualmente las claves de acceso y un token del archivo de credenciales, recomendamos que la aplicación utilice credenciales temporales enviadas por:

- Un servicio de AWS cómputo, como ejecutar la aplicación en Amazon Elastic Compute Cloud o en AWS Lambda.
- Otra opción de la cadena de proveedores de credenciales, como [IAMAutenticación de Identity Center para su SDK herramienta](#).
- O utilícela [Proveedor de credenciales de proceso](#) para recuperar credenciales temporales.

Configure un archivo de credenciales con las credenciales de corta duración recuperadas del portal de AWS acceso

1. [Creación de archivos de credenciales compartidas](#).
2. En el archivo de credenciales, pegue el siguiente texto de marcador de posición hasta que pegue las credenciales temporales que funcionen.

```
[default]
aws_access_key_id=<value from AWS access portal>
aws_secret_access_key=<value from AWS access portal>
```



Si utilizas un IAM usuario para ejecutar el código, la herramienta SDK o herramienta de tu entorno de desarrollo se autentica mediante credenciales de IAM usuario de larga duración en el archivo compartido. `AWS credentials` Revisa las [prácticas recomendadas de seguridad](#) del IAM tema y pasa a IAM Identity Center o a otras credenciales temporales lo antes posible.

## Advertencias y directrices importantes para las credenciales

### Advertencias para las credenciales

- **NOT** Utilice las credenciales raíz de su cuenta para acceder a AWS los recursos. Estas credenciales proporcionan acceso ilimitado a la cuenta y son difíciles de revocar.
- **NOT** Coloca literalmente las claves de acceso o la información sobre las credenciales en los archivos de tu solicitud. Si lo hace, puede crear un riesgo de exposición accidental de sus credenciales si, por ejemplo, carga el proyecto en un repositorio público.
- **NOT** Incluya archivos que contengan credenciales en el área de su proyecto.
- Tenga en cuenta que todas las credenciales almacenadas en el `AWS credentials` archivo compartido se almacenan en texto sin formato.

### Guía adicional para administrar las credenciales de forma segura

Para obtener información general sobre cómo administrar las AWS credenciales de forma segura, consulte [Prácticas recomendadas para administrar las claves de AWS acceso](#) en el [Referencia general de AWS](#). Además de esa conversación, tenga en cuenta lo siguiente:

- Utilice [IAM roles para las tareas](#) de Amazon Elastic Container Service (Amazon ECS).
- Usa [IAM roles](#) para las aplicaciones que se ejecutan en EC2 instancias de Amazon.

## Requisitos previos: crear una cuenta AWS

Para utilizar un IAM usuario para acceder a AWS los servicios, necesita una AWS cuenta y AWS credenciales.

1. Cree una cuenta.

Para crear una AWS cuenta, consulte [Primeros pasos: ¿es la primera vez que lo usa AWS ?](#) en la Guía AWS Account Management de referencia.

2. Crear un usuario administrativo.

Evite usar la cuenta de usuario raíz (la cuenta inicial que cree) para acceder a la consola y los servicios de administración. En su lugar, cree una cuenta de usuario administrativo, tal y como se explica en la [sección Creación de un usuario administrativo](#) de la Guía del IAM usuario.

Después de crear la cuenta de usuario administrativo y registrar los detalles de inicio de sesión, asegúrese de desconectar la cuenta de usuario raíz y vuelva a iniciar sesión con la cuenta administrativa.

Ninguna de estas cuentas es adecuada para desarrollar AWS o ejecutar aplicaciones AWS. Como buena práctica, debe crear usuarios, conjuntos de permisos o roles de servicio que sean adecuados para estas tareas. Para obtener más información, consulte [Aplicar permisos de privilegio mínimo](#) en la Guía del usuario de IAM.

## Paso 1: Crea tu IAM usuario

- Cree su IAM usuario siguiendo el procedimiento de [creación de IAM usuarios \(consola\)](#) de la Guía del IAM usuario. Al crear el IAM usuario:
  - Le recomendamos que seleccione Proporcionar acceso de usuario al AWS Management Console. Esto le permite ver información Servicios de AWS relacionada con el código que está ejecutando en un entorno visual, como comprobar los registros de AWS CloudTrail diagnóstico o cargar archivos en Amazon Simple Storage Service, lo que resulta útil a la hora de depurar el código.
  - En Establecer permisos: opciones de permisos, selecciona Adjuntar políticas directamente para ver cómo quieres asignar los permisos a este usuario.
    - La mayoría de SDK los tutoriales de introducción utilizan el servicio Amazon S3 como ejemplo. Para proporcionar a su aplicación acceso completo a Amazon S3, seleccione la política AmazonS3FullAccess que desea asociar a este usuario.
  - Puede ignorar los pasos opcionales de ese procedimiento relacionados con la configuración de los límites o las etiquetas de los permisos.

## Paso 2: Obtener las claves de acceso

1. En el panel de navegación de la IAM consola, seleccione Usuarios y, a continuación, seleccione el **User name** usuario que creó anteriormente.

2. En la página del usuario, selecciona la página Credenciales de seguridad. A continuación, en Claves de acceso, seleccione Crear clave de acceso.
3. En el paso 1 de Crear la clave de acceso, elija Interfaz de línea de comandos (CLI) o Código local. Ambas opciones generan el mismo tipo de clave para usar tanto con el AWS CLI como con el SDKs.
4. En el paso 2 de Crear clave de acceso, introduzca una etiqueta opcional y seleccione Siguiente.
5. En el paso 3 de Crear la clave de acceso, selecciona Descargar el archivo.csv para guardar un .csv archivo con la clave de acceso y la clave de acceso secreta del IAM usuario. Necesitará esta información más tarde.

 Warning

Utilice las medidas de seguridad adecuadas para mantener estas credenciales seguras.

6. Seleccione Done (Listo).

### Paso 3: Actualice el archivo compartido **credentials**

1. Cree o abra el archivo AWS `credentials` compartido. Este archivo es `~/.aws/credentials` en sistemas Linux y macOS y `%USERPROFILE%\aws\credentials` en Windows. Para obtener más información, consulte la [ubicación de los archivos de credenciales](#).
2. Agregue el siguiente texto al archivo `credentials` compartido. Sustituya el valor de ID y el valor clave de ejemplo por los valores del archivo `.csv` que descargó anteriormente.

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

3. Guarde el archivo.

El archivo compartido `credentials` es la forma más común de almacenar las credenciales. También se pueden configurar como variables de entorno; consulte los nombres de las variables de entorno [AWS claves de acceso](#). Esta es una forma de empezar, pero le recomendamos que cambie a IAM Identity Center o a otras credenciales temporales lo antes posible. Cuando deje de usar credenciales de larga duración, recuerde eliminarlas del archivo compartido `credentials`.

# Uso de IAM roles para EC2 instancias de Amazon

En este ejemplo, se describe la configuración de un AWS Identity and Access Management rol con acceso a Amazon S3 para usarlo en la aplicación implementada en una EC2 instancia de Amazon.

Para ejecutar tu AWS SDK aplicación en una instancia de Amazon Elastic Compute Cloud, crea un IAM rol y luego dale a tu EC2 instancia de Amazon acceso a ese rol. Para obtener más información, consulta [IAM Roles para Amazon EC2](#) en la Guía del EC2 usuario de Amazon.

## Crear un rol de IAM

Es probable que la AWS SDK aplicación que desarrolle acceda al menos a una Servicio de AWS para realizar acciones. Crea un IAM rol que conceda los permisos necesarios para que la aplicación se ejecute.

Este procedimiento crea un rol que concede acceso de solo lectura a Amazon S3, por ejemplo. Muchas de las AWS SDK guías incluyen tutoriales de introducción que se leen en Amazon S3.

1. Inicie sesión en AWS Management Console y abra la IAM consola en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Roles y después Crear rol.
3. Para Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
4. En Caso de uso, selecciona Amazon EC2 y, a continuación, selecciona Siguiente.
5. En Añadir permisos, seleccione la casilla de verificación Acceso de solo lectura a Amazon S3 en la lista de políticas y, a continuación, seleccione Siguiente.
6. Ingrese un nombre para el rol y, a continuación, seleccione Crear rol. Recuerda este nombre porque lo necesitarás cuando crees tu EC2 instancia de Amazon.

## Lanza una EC2 instancia de Amazon y especifica tu IAM rol

Puedes crear y lanzar una EC2 instancia de Amazon con tu IAM rol de la siguiente manera:

- Siga [Lanzar rápidamente una instancia](#) en la Guía del EC2 usuario de Amazon. Sin embargo, antes del paso final de envío, haga también lo siguiente:
  - En Detalles avanzados, en Perfil de IAM instancia, elija el rol que creó en el paso anterior.

Con esta EC2 configuración IAM y con Amazon, puede implementar su aplicación en la EC2 instancia de Amazon y su aplicación tendrá acceso de lectura al servicio Amazon S3.

## Conectarse a la EC2 instancia

Conéctate a la EC2 instancia de Amazon para poder transferirle la aplicación y, a continuación, ejecutarla. Necesitará el archivo que contiene la parte privada del par de claves que utilizó en Par de claves (inicio de sesión) cuando creó la instancia; es decir, el PEM archivo.

Para ello, sigue las instrucciones correspondientes a tu tipo de instancia: [Connect to your Linux](#) or [Connect to your Windows instance](#). Cuando se conecte, hágalo de forma que pueda transferir archivos desde el equipo de desarrollo a la instancia.

### Note

En un terminal Linux o macOS, puede utilizar el comando `secure copy` para copiar la aplicación. Para usar `scp` con un key pair, puede usar el siguiente comando: `scp -i path/to/key file/to/copy ec2-user@ec2-xx-xx-xxx-xxx.compute.amazonaws.com:~`.

Para obtener más información sobre Windows, consulte [Transferir archivos a instancias de Windows](#).

Si utilizas un AWS kit de herramientas, a menudo también puedes conectarte a la instancia mediante el kit de herramientas. Para más información, consulte la guía de usuario específica del kit de herramientas que utilice.

## Ejecuta la aplicación en la instancia EC2

1. Copia los archivos de tu aplicación desde tu unidad local a tu EC2 instancia de Amazon.
2. Inicie la aplicación y compruebe que se ejecuta con los mismos resultados que en el equipo de desarrollo.
3. (Opcional) Compruebe que la aplicación utilice las credenciales proporcionadas por el IAM rol.
  - a. Inicia sesión en la EC2 consola de Amazon AWS Management Console y ábrela en <https://console.aws.amazon.com/ec2/>.
  - b. Seleccione la instancia.
  - c. Selecciona Acciones, Seguridad y, a continuación, selecciona Modificar IAM rol.

- d. Para IAM el rol, seleccione el IAM rol seleccionando Sin IAM rol.
- e. Seleccione Actualizar IAM rol.
- f. Vuelva a ejecutar la aplicación y confirme que devuelve un error de autorización.

# Referencia de configuración

SDKs proporcionar un idioma específico para APIs. Servicios de AWS Se encargan de algunas de las tareas pesadas necesarias para realizar correctamente las API llamadas, como la autenticación, el comportamiento de reintento y mucho más. Para ello, SDKs disponen de estrategias flexibles para obtener credenciales para utilizarlas en sus solicitudes, mantener la configuración que se utilizará con cada servicio y obtener valores para utilizarlos en la configuración global.

Puede encontrar información detallada sobre los ajustes de configuración en las siguientes secciones:

- [AWS SDKs y Herramientas: proveedores de credenciales estandarizadas](#)— Los proveedores de credenciales más comunes están estandarizados en varios SDKs.
- [AWS SDKs y funciones estandarizadas de Tools](#)— Características comunes estandarizadas en varios SDKs.

## Cómo crear clientes de servicio

Para acceder mediante programación Servicios de AWS, SDKs utilice una clase/objeto de cliente para cada uno. Servicio de AWS Por ejemplo, si tu aplicación necesita acceder a Amazon EC2, crea un objeto EC2 cliente de Amazon para interactuar con ese servicio. A continuación, utiliza el cliente de servicio para realizar solicitudes al mismo Servicio de AWS. En la mayoría de los casos SDKs, un objeto de cliente de servicio es inmutable, por lo que debe crear un cliente nuevo para cada servicio al que realice solicitudes y para realizar solicitudes al mismo servicio con una configuración diferente.

## Prioridad de los ajustes

La configuración global configura las funciones, los proveedores de credenciales y otras funcionalidades compatibles con la mayoría SDKs y que tienen un amplio impacto en todos los ámbitos. Servicios de AWS Todos SDKs tienen una serie de lugares (o fuentes) que comprueban para encontrar un valor para la configuración global. La siguiente es la configuración de la prioridad de búsqueda:

1. Cualquier configuración explícita establecida en el código o en el propio cliente de servicio tiene prioridad sobre cualquier otra.

- Algunos ajustes se pueden establecer por operación y se pueden cambiar según sea necesario para cada operación que se invoque. En el caso del parámetro AWS CLI o AWS Tools for PowerShell, estos parámetros adoptan la forma de parámetros por operación que se introducen en la línea de comandos. En el caso de una SDK, las asignaciones explícitas pueden adoptar la forma de un parámetro que se establece al crear una instancia de un Servicio de AWS cliente o un objeto de configuración o, a veces, al llamar a una persona. API
2. Solo en Java/Kotlin: la propiedad del JVM sistema correspondiente a la configuración está marcada. Si se ha establecido, se usa ese valor para configurar el cliente.
  3. Se comprueba la variable de entorno . Si se ha establecido, se usa ese valor para configurar el cliente.
  4. SDKComprueba la configuración en el `credentials` archivo compartido. Si está configurado, el cliente lo usa.
  5. El `config` archivo compartido de la configuración. Si la configuración está presente, la SDK usa.
    - La variable de `AWS_PROFILE` entorno o la propiedad `aws.profile` JVM del sistema se pueden utilizar para especificar qué perfil se va a SDK cargar.
  6. Los valores por defecto proporcionados por el propio código SDK fuente se utilizan en último lugar.

#### Note

Es posible que algunas SDKs herramientas se muestren en un orden diferente. Además, algunas SDKs herramientas admiten otros métodos de almacenamiento y recuperación de parámetros. Por ejemplo, AWS SDK for .NET admite una fuente adicional llamada [SDKTienda](#). Para obtener más información sobre los proveedores exclusivos de una herramienta SDK o herramienta, consulte la guía específica de la herramienta SDK o herramienta que esté utilizando.

El orden determina qué métodos tienen prioridad y sustituyen a los demás. Por ejemplo, si configuras un perfil en el `config` archivo compartido, solo se encuentra y se usa después de que la herramienta SDK o compruebe primero los demás lugares. Esto significa que si colocas una configuración en el archivo `credentials`, se utilizará en lugar de la que se encuentra en el archivo `config`. Si configura una variable de entorno con una configuración y un valor, anulará esa configuración en los archivos `credentials` y `config`. Por último, una configuración en la

operación individual (parámetro o API parámetro de la AWS CLI línea de comandos) o en el código anularía todos los demás valores de ese comando.

## Páginas de configuración

Las páginas de la sección de referencia de configuración de esta guía detallan las configuraciones disponibles que se pueden configurar mediante varios mecanismos. En las tablas siguientes se enumeran los ajustes de los archivos de configuración y credenciales, las variables de entorno y (en el caso de Java y KotlinSDKs) los JVM ajustes que se pueden utilizar fuera del código para configurar la función. Cada tema vinculado de cada lista te lleva a la página de configuración correspondiente.

- [Lista de ajustes de archivos Config](#)
- [Lista de ajustes de archivos Credentials](#)
- [Lista de variables de entorno](#)
- [JVM lista de propiedades del sistema](#)

Cada función o proveedor de credenciales tiene una página en la que se enumeran los ajustes que se utilizan para configurar esa funcionalidad. Para cada configuración, normalmente puedes establecer el valor añadiendo la configuración a un archivo de configuración, estableciendo una variable de entorno o (solo para Java y Kotlin) configurando una propiedad JVM del sistema. Cada configuración muestra todos los métodos admitidos para establecer el valor en un bloque situado encima de los detalles de la descripción. Aunque la [prioridad](#) varía, la funcionalidad resultante es la misma independientemente de cómo se establezca.

La descripción incluirá el valor predeterminado, si lo hay, que surtirá efecto si no se hace nada. También define qué valor es válido para esa configuración.

Por ejemplo, veamos una configuración de la página de [Compresión de solicitudes](#) características.

La información de la configuración de `disable_request_compression` ejemplo comunica lo siguiente:

- Hay tres formas equivalentes de controlar la compresión de las solicitudes fuera del código base. Puede:
  - Configúralo en tu archivo de configuración usando `disable_request_compression`

- Configúralo como una variable de entorno usando `AWS_DISABLE_REQUEST_COMPRESSION`
- O bien, si está utilizando Java o KotlinSDK, configúrelo como una propiedad JVM del sistema mediante `aws.disableRequestCompression`

#### Note

También puede haber una forma de configurar la misma funcionalidad directamente en el código, pero esta referencia no cubre esta cuestión, ya que es única para cada uno SDK de ellos. Si quieres establecer tu configuración en el propio código, consulta tu SDK guía o API referencia específica.

- Si no hace nada, el valor predeterminado será `false`.
- Los únicos valores válidos para esta configuración booleana son `true` y `false`

En la parte inferior de cada página de características hay una tabla de compatibilidad con AWS SDKs.

En esta tabla se muestra si SDK admite la configuración que aparece en la página. La `Supported` columna indica el nivel de soporte con los siguientes valores:

- **Yes**— La configuración es totalmente compatible con SDK lo que está escrito.
- **Partial**— Algunos de los ajustes son compatibles o el comportamiento se aparta de la descripción. `Partial`En efecto, una nota adicional indica la desviación.
- **No**— No se admite ninguno de los ajustes. Esto no indica si se podría lograr la misma funcionalidad en el código; solo indica que los ajustes de configuración externos enumerados no son compatibles.

## Lista de ajustes de archivos **Config**

Los ajustes que se muestran en la siguiente tabla se pueden asignar en el AWS `config` archivo compartido. Son globales y afectan a todos los Servicios de AWS. SDKs y las herramientas también pueden admitir configuraciones y variables de entorno únicas. Para ver los ajustes y las variables de entorno que solo admite una persona SDK o una herramienta, consulta esa guía específica SDK o de herramientas.

Nombre del conjunto	Detalles
account_id_endpoint_mode	<a href="#">Puntos finales basados en cuentas</a>
api_versions	<a href="#">Ajustes de configuración general</a>
aws_access_key_id	<a href="#">AWS claves de acceso</a>
aws_account_id	<a href="#">puntos finales basados en cuentas</a>
aws_secret_access_key	<a href="#">AWS claves de acceso</a>
aws_session_token	<a href="#">AWS claves de acceso</a>
ca_bundle	<a href="#">Ajustes de configuración general</a>
credential_process	<a href="#">Proveedor de credenciales de proceso</a>
credential_source	<a href="#">Asumir el rol de proveedor de credenciales</a>
defaults_mode	<a href="#">Valores predeterminados de configuración inteligente</a>
disable_request_compression	<a href="#">Compresión de solicitudes</a>
duration_seconds	<a href="#">Asumir el rol de proveedor de credenciales</a>

Nombre del conjunto	Detalles	
ec2_metadata_service_endpoint	<a href="#">IMDS proveedor de credenciales</a>	
ec2_metadata_service_endpoint_mode	<a href="#">IMDS proveedor de credenciales</a>	
ec2_metadata_v1_disabled	<a href="#">IMDS proveedor de credenciales</a>	
endpoint_discovery_enabled	<a href="#">Detección de puntos de conexión</a>	
endpoint_url	<a href="#">Puntos de conexión específicos del servicio</a>	
external_id	<a href="#">Asumir el rol de proveedor de credenciales</a>	
ignore_configured_endpoint_urls	<a href="#">Puntos de conexión específicos del servicio</a>	
max_attempts	<a href="#">Comportamiento de los reintentos</a>	
metadata_service_num_attempts	<a href="#">Metadatos de EC2 instancias de Amazon</a>	
metadata_service_timeout	<a href="#">Metadatos de EC2 instancias de Amazon</a>	
mfa_serial	<a href="#">Asumir el rol de proveedor de credenciales</a>	

Nombre del conjunto	Detalles
output	<a href="#">Ajustes de configuración general</a>
parameter_validation	<a href="#">Ajustes de configuración general</a>
region	<a href="#">Región de AWS</a>
request_max_in_compression_size_bytes	<a href="#">Compresión de solicitudes</a>
retry_mode	<a href="#">Comportamiento de los reintentos</a>
role_arn	<a href="#">Asumir el rol de proveedor de credenciales</a>
role_session_name	<a href="#">Asumir el rol de proveedor de credenciales</a>
s3_disable_multiregion_access_points	<a href="#">Puntos de acceso multirregión de Amazon S3</a>
s3_use_arn_region	<a href="#">Puntos de acceso de Amazon S3</a>
sdk_ua_app_id	<a href="#">Application ID</a>
source_profile	<a href="#">Asumir el rol de proveedor de credenciales</a>
sso_account_id	<a href="#">IAM Proveedor de credenciales de Identity Center</a>
sso_region	<a href="#">IAM Proveedor de credenciales de Identity Center</a>

Nombre del conjunto	Detalles
sso_regis- tration_scopes	<a href="#">IAMProveedor de credenciales de Identity Center</a>
sso_role_name	<a href="#">IAMProveedor de credenciales de Identity Center</a>
sso_start_url	<a href="#">IAMProveedor de credenciales de Identity Center</a>
sts_regio- nal_endpoints	<a href="#">AWS STS Puntos de conexión regionales</a>
use_duals- tack_endpoint	<a href="#">Pila doble y puntos finales FIPS</a>
use_fips- endpoint	<a href="#">Pila doble y puntos finales FIPS</a>
web_ident- ity_token_file	<a href="#">Asumir el rol de proveedor de credenciales</a>

## Lista de ajustes de archivos **Credentials**

Los ajustes que se muestran en la siguiente tabla se pueden asignar en el archivo compartido AWS `credentials`. Son globales y afectan a todos los Servicios de AWS. SDKsy las herramientas también pueden admitir configuraciones y variables de entorno únicas. Para ver los ajustes y las variables de entorno que solo admite una persona SDK o una herramienta, consulta esa guía específica SDK o de herramientas.

Nombre del conjunto	Detalles
aws_acces- s_key_id	<a href="#">AWS teclas de acceso</a>
aws_secre- t_access_key	<a href="#">AWS claves de acceso</a>

Nombre del conjunto	Detalles
aws_session_token	<a href="#">AWS claves de acceso</a>

## Lista de variables de entorno

Las variables de entorno compatibles con la mayoría SDKs se muestran en la siguiente tabla. Son globales y afectan a todos los Servicios de AWS. SDKsy las herramientas también pueden admitir configuraciones y variables de entorno únicas. Para ver los ajustes y las variables de entorno que solo admite una persona SDK o una herramienta, consulta esa guía específica SDK o de herramientas.

Nombre del conjunto	Detalles
AWS_ACCESS_KEY_ID	<a href="#">AWS teclas de acceso</a>
AWS_ACCOUNT_ID	<a href="#">puntos finales basados en cuentas</a>
AWS_ACCOUNT_ID_ENDPOINT_POINT_MODE	<a href="#">Puntos finales basados en cuentas</a>
AWS_CA_BUNDLE	<a href="#">Ajustes de configuración general</a>
AWS_CONFIG_FILE	<a href="#">Ubicación de los archivos compartidos config y credentials</a>
AWS_CONTAINER_AUTHORIZATION_TOKEN	<a href="#">Proveedor de credenciales de contenedor</a>
AWS_CONTAINER_AUTH	<a href="#">Proveedor de credenciales de contenedor</a>

Nombre del conjunto	Detalles
AWS_CONTAINER_CREDENTIALS_FILE	
AWS_CONTAINER_CREDENTIALS_FULL_URI	<a href="#">Proveedor de credenciales de contenedor</a>
AWS_CONTAINER_CREDENTIALS_RELATIVE_URI	<a href="#">Proveedor de credenciales de contenedor</a>
AWS_DEFAULTS_MODE	<a href="#">Valores predeterminados de configuración inteligente</a>
AWS_DISABLE_REQUEST_COMPRESSION	<a href="#">Compresión de solicitudes</a>
AWS_EC2_METADATA_DISABLED	<a href="#">IMDS proveedor de credenciales</a>
AWS_EC2_METADATA_SERVICE_ENDPOINT	<a href="#">IMDS proveedor de credenciales</a>
AWS_EC2_METADATA_SERVICE_ENDPOINT_MODE	<a href="#">IMDS proveedor de credenciales</a>
AWS_EC2_METADATA_V1_DISABLED	<a href="#">IMDS proveedor de credenciales</a>

Nombre del conjunto	Detalles
AWS_ENABLE_ENDPOINT_DISCOVERY	<a href="#">Detección de puntos de conexión</a>
AWS_ENDPOINT_URL	<a href="#">Puntos de conexión específicos del servicio</a>
AWS_ENDPOINT_URL_<SERVICE>	<a href="#">Puntos de conexión específicos del servicio</a>
AWS_IGNORE_CONFIGURED_ENDPOINT_URLS	<a href="#">Puntos de conexión específicos del servicio</a>
AWS_MAX_ATTEMPTS	<a href="#">Comportamiento de los reintentos</a>
AWS_METADATA_SERVICE_NUM_ATTEMPTS	<a href="#">Metadatos de EC2 instancias de Amazon</a>
AWS_METADATA_SERVICE_TIMEOUT	<a href="#">Metadatos de EC2 instancias de Amazon</a>
AWS_PROFILE	<a href="#">Archivos compartidos config y credenciales</a>
AWS_REGION	<a href="#">Región de AWS</a>
AWS_REQUEST_MIN_COMPRESSION_SIZE_BYTES	<a href="#">Compresión de solicitudes</a>

Nombre del conjunto	Detalles
AWS_RETRY_MODE	<a href="#">Comportamiento de los reintentos</a>
AWS_ROLE_ARN	<a href="#">Asumir el rol de proveedor de credenciales</a>
AWS_ROLE_SESSION_NAME	<a href="#">Asumir el rol de proveedor de credenciales</a>
AWS_S3_DISABLE_MULTIREGION_ACCESS_POINTS	<a href="#">Puntos de acceso multirregión de Amazon S3</a>
AWS_S3_US_E_ARN_REGION	<a href="#">Puntos de acceso de Amazon S3</a>
AWS_SDK_UA_APP_ID	<a href="#">Application ID</a>
AWS_SECRET_ACCESS_KEY	<a href="#">AWS claves de acceso</a>
AWS_SESSION_TOKEN	<a href="#">AWS claves de acceso</a>
AWS_SHARED_CREDENTIALS_FILE	<a href="#">Ubicación de los archivos compartidos <code>config</code> y <code>credentials</code></a>
AWS_STS_REGIONAL_ENDPOINTS	<a href="#">AWS STS Puntos de conexión regionales</a>
AWS_USE_DEFAULTS_ENDPOINT	<a href="#">Doble pila y puntos finales FIPS</a>

Nombre del conjunto	Detalles
AWS_USE_F IPS_ENDPOINT	<a href="#">Pila doble y puntos finales FIPS</a>
AWS_WEB_I IDENTITY_T OKEN_FILE	<a href="#">Asumir el rol de proveedor de credenciales</a>

## JVM lista de propiedades del sistema

Puede utilizar las siguientes propiedades JVM del sistema para el AWS SDK for Java y el AWS SDK para Kotlin (orientado al JVM). Consulte [the section called “¿Cómo configurar las propiedades del sistema JVM”](#) para obtener instrucciones sobre cómo configurar las propiedades JVM del sistema.

Nombre del conjunto	Detalles
aws.accessKeyId	<a href="#">AWS claves de acceso</a>
aws.accountId	<a href="#">puntos finales basados en cuentas</a>
aws.accountIdEndpointMode	<a href="#">Puntos finales basados en cuentas</a>
aws.configFile	<a href="#">Ubicación de los archivos compartidos config y credentials</a>
aws.defaultsMode	<a href="#">Valores predeterminados de configuración inteligente</a>
aws.disableEc2MetadataV1	<a href="#">IMDS proveedor de credenciales</a>
aws.disableRequestCompression	<a href="#">Compresión de solicitudes</a>

Nombre del conjunto	Detalles
<code>aws.ec2MetadataServiceEndpoint</code>	<a href="#">IMDSproveedor de credenciales</a>
<code>aws.ec2MetadataEndpointMode</code>	<a href="#">IMDSproveedor de credenciales</a>
<code>aws.endpointDiscoveryEnabled</code>	<a href="#">Detección de puntos de conexión</a>
<code>aws.endpointUrl</code>	<a href="#">Puntos de conexión específicos del servicio</a>
<code>aws.endpointUrl&lt;ServiceName&gt;</code>	<a href="#">Puntos de conexión específicos del servicio</a>
<code>aws.ignoreConfiguredEndpointUrls</code>	<a href="#">Puntos de conexión específicos del servicio</a>
<code>aws.maxAttempts</code>	<a href="#">Comportamiento de los reintentos</a>
<code>aws.profile</code>	<a href="#">Archivos compartidos config y credenciales</a>
<code>aws.region</code>	<a href="#">Región de AWS</a>
<code>aws.requestMinCompressionSizeBytes</code>	<a href="#">Compresión de solicitudes</a>
<code>aws.retryMode</code>	<a href="#">Comportamiento de los reintentos</a>

Nombre del conjunto	Detalles
<code>aws.roleArn</code>	<a href="#">Asumir el rol de proveedor de credenciales</a>
<code>aws.roleSessionName</code>	<a href="#">Asumir el rol de proveedor de credenciales</a>
<code>aws.s3DisableMultiRegionAccessPoints</code>	<a href="#">Puntos de acceso multirregión de Amazon S3</a>
<code>aws.s3UseArnRegion</code>	<a href="#">Puntos de acceso de Amazon S3</a>
<code>aws.secretAccessKey</code>	<a href="#">AWS claves de acceso</a>
<code>aws.sessionToken</code>	<a href="#">AWS claves de acceso</a>
<code>aws.sharedCredentialsFile</code>	<a href="#">Ubicación de los archivos compartidos <code>config</code> y <code>credentials</code></a>
<code>aws.useDualstackEndpoint</code>	<a href="#">Doble pila y puntos finales FIPS</a>
<code>aws.useFipsEndpoint</code>	<a href="#">Pila doble y puntos finales FIPS</a>
<code>aws.userAgentAppId</code>	<a href="#">Application ID</a>
<code>aws.webIdentityTokenFile</code>	<a href="#">Asumir el rol de proveedor de credenciales</a>

# AWS SDKs y Herramientas: proveedores de credenciales estandarizadas

Muchos proveedores de credenciales se han estandarizado para mantener valores predeterminados consistentes y para que funcionen de la misma manera en muchos de ellos. SDKs Esta coherencia aumenta la productividad y la claridad a la hora de codificar en varios. SDKs Todos los ajustes se pueden anular en el código. Para obtener más información, consulta tus especificaciones SDKAPI.

## Important

No todos SDKs apoyan a todos los proveedores, ni siquiera a todos los aspectos de un proveedor.

## Temas

- [Comprenda la cadena de proveedores de credenciales](#)
- [SDK-cadenas de proveedores de credenciales específicas y específicas de cada herramienta](#)
- [AWS claves de acceso](#)
- [Asumir el rol de proveedor de credenciales](#)
- [Proveedor de credenciales de contenedor](#)
- [IAMProveedor de credenciales de Identity Center](#)
- [IMDSproveedor de credenciales](#)
- [Proveedor de credenciales de proceso](#)

## Comprenda la cadena de proveedores de credenciales

Todos SDKs tienen una serie de lugares (o fuentes) que consultan para encontrar credenciales válidas que puedan utilizarlas para realizar una solicitud a un Servicio de AWS. Una vez que se encuentran las credenciales válidas, se detiene la búsqueda. Esta búsqueda sistemática se denomina cadena de proveedores de credenciales.

Cuando se utiliza uno de los proveedores de credenciales estandarizados, AWS SDKs siempre se intenta renovar las credenciales automáticamente cuando caducan. La cadena de proveedores de credenciales integrada permite a la aplicación actualizar las credenciales independientemente del proveedor de la cadena que utilice. Para ello, no se necesita ningún código adicional. SDK

Si bien la cadena distinta utilizada por cada uno SDK varía, la mayoría de las veces incluyen fuentes como las siguientes:

Proveedor de credenciales	Descripción
<a href="#">AWS claves de acceso</a>	AWS claves de acceso para un IAM usuario (como <code>AWS_ACCESS_KEY_ID</code> , y <code>AWS_SECRET_ACCESS_KEY</code> ).
<a href="#">Cómo federar con identidad web u OpenID Connect: asumir el rol de proveedor de credenciales</a>	Inicie sesión con un proveedor de identidad externo (IdP) conocido, como Login with Amazon, Facebook, Google o cualquier otro IdP compatible con OpenID Connect (OIDC). Asuma los permisos de un IAM rol mediante un JSON Web Token (JWT) de (). AWS Security Token Service AWS STS
<a href="#">IAM Proveedor de credenciales de Identity Center</a>	Obtenga las credenciales de AWS IAM Identity Center.
<a href="#">Asumir el rol de proveedor de credenciales</a>	Obtenga acceso a otros recursos asumiendo los permisos de un IAM rol. (Recupere las credenciales temporales para un rol y, a continuación, utilícelas).
<a href="#">Proveedor de credenciales de contenedor</a>	Credenciales de Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS). El proveedor de credenciales del contenedor obtiene las credenciales de la aplicación contenerizada del cliente.
<a href="#">Proveedor de credenciales de proceso</a>	Proveedor de credenciales personalizadas. Obtenga sus credenciales de una fuente o proceso externo, incluido IAM Roles Anywhere.
<a href="#">IMDS proveedor de credenciales</a>	Credenciales de perfil de instancia de Amazon Elastic Compute Cloud (Amazon EC2). Asocie un IAM rol a cada una de sus EC2 instancias. Las credenciales temporales de ese rol estarán disponibles para el código que se

Proveedor de credenciales	Descripción
	ejecute en la instancia. Las credenciales se entregan a través del servicio de EC2 metadatos de Amazon.

Para cada paso de la cadena, hay varias formas de asignar valores de configuración. Los valores de configuración que se especifican en el código siempre tienen prioridad. Sin embargo, también los hay [Variables de entorno](#) y los [Archivos config y credentials compartidos](#). Para obtener más información, consulte [Prioridad de los ajustes](#).

## SDK-cadenas de proveedores de credenciales específicas y específicas de cada herramienta

Para ir directamente a los detalles SDK de su cadena de proveedores de credenciales específica o de la herramienta, elija su cadena SDK o herramienta entre las siguientes opciones:

- [AWS CLI](#)
- [SDK para C++](#)
- [SDK para Go](#)
- [SDK para Java](#)
- [SDK para JavaScript](#)
- [SDK para Kotlin](#)
- [SDK para .NET](#)
- [SDK para PHP](#)
- [SDK para Python \(Boto3\)](#)
- [SDK para Ruby](#)
- [SDK para Rust](#)
- [SDK para Swift](#)
- [Herramientas para PowerShell](#)

## AWS claves de acceso

### Warning

Para evitar riesgos de seguridad, no utilices a IAM los usuarios para autenticarte cuando desarrolles software específico o trabajes con datos reales. En cambio, utilice la federación con un proveedor de identidades como [AWS IAM Identity Center](#).

AWS las claves de acceso de un IAM usuario se pueden utilizar como credenciales AWS. Utiliza AWS SDK automáticamente estas AWS credenciales para firmar las API solicitudes AWS, de modo que sus cargas de trabajo puedan acceder a sus AWS recursos y datos de forma segura y cómoda. Se recomienda utilizarlas siempre para `aws_session_token` que las credenciales sean temporales y dejen de ser válidas una vez caducadas. No se recomienda utilizar credenciales de larga duración.

### Note

Si AWS no puede actualizar estas credenciales temporales, AWS puede extender la validez de las credenciales para que sus cargas de trabajo no se vean afectadas.

El `AWS credentials` archivo compartido es la ubicación recomendada para almacenar la información sobre las credenciales, ya que se encuentra de forma segura fuera de los directorios de origen de la aplicación y separado SDK de la configuración específica del archivo `compartidoconfig`.

Para obtener más información sobre AWS las credenciales y el uso de las claves de acceso, consulte las [credenciales AWS de seguridad](#) y la [administración de las claves de acceso para IAM los usuarios](#) en la Guía del IAM usuario.

Configure esta funcionalidad mediante lo siguiente:

**aws\_access\_key\_id**- configuración de AWS **config** archivos compartidos,

**aws\_access\_key\_id**- configuración de AWS **credentials** archivos compartidos (método

recomendado), **AWS\_ACCESS\_KEY\_ID**: variable de entorno, **aws.accessKeyId**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica la clave de AWS acceso utilizada como parte de las credenciales para autenticar al usuario.

**aws\_secret\_access\_key**- configuración de AWS **config** archivos compartidos,  
**aws\_secret\_access\_key**- configuración de AWS **credentials** archivos compartidos (método recomendado), **AWS\_SECRET\_ACCESS\_KEY**: variable de entorno, **aws.secretAccessKey**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica la clave AWS secreta utilizada como parte de las credenciales para autenticar al usuario.

**aws\_session\_token**- configuración de AWS **config** archivos compartidos,  
**aws\_session\_token**- configuración de AWS **credentials** archivos compartidos (método recomendado), **AWS\_SESSION\_TOKEN**: variable de entorno, **aws.sessionToken**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica un token AWS de sesión que se utiliza como parte de las credenciales para autenticar al usuario. Este valor se recibe como parte de las credenciales temporales devueltas por las solicitudes aprobadas para asumir un rol. Un token de sesión solo es necesario si especifica manualmente credenciales de seguridad temporales. Sin embargo, le recomendamos que utilice siempre credenciales de seguridad temporales en lugar de credenciales. Para obtener recomendaciones de seguridad, consulte las [prácticas recomendadas de seguridad en IAM](#).

Para obtener instrucciones acerca de cómo obtener estos valores, consulte [Autenticación mediante credenciales a corto plazo](#).

Ejemplo de configuración de este valor en el archivo config o credentials:

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
aws_session_token = AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40Lgk
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
export
AWS_SESSION_TOKEN=AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40Lgk
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_ACCESS_KEY_ID AKIAIOSFODNN7EXAMPLE
```

```
setx AWS_SECRET_ACCESS_KEY wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
setx
AWS_SESSION_TOKEN AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40Lgk
```

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	Compatible	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	No se admite el archivo compartido config.
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Sí	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	No se admiten variables de entorno.
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	

SDK	C	Notas o más información
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	No se admiten variables de entorno.

## Asumir el rol de proveedor de credenciales

Para asumir un rol, se utiliza un conjunto de credenciales de seguridad temporales para acceder a los recursos de AWS a los que de otro modo usted no tendría acceso. Las credenciales temporales incluyen un ID de clave de acceso, una clave de acceso secreta y un token de seguridad.

Para configurar su herramienta SDK o herramienta para que asuma un rol, primero debe crear o identificar el rol específico que desee asumir. IAM los roles se identifican de forma única mediante un rol: Amazon Resource Name ([ARN](#)). Los roles establecen relaciones de confianza con otra entidad. La entidad de confianza que usa el rol puede ser un Servicio de AWS, otro Cuenta de AWS, un proveedor de identidad web o una SAML federación. OIDC

Una vez identificado el IAM rol, si ese rol confía en usted, puede configurar su SDK herramienta para que utilice los permisos que otorga el rol. Para ello, utilice los siguientes comandos.

Para comenzar a utilizar esta configuración, consulte [Asume un rol con AWS credenciales](#) en esta guía.

## Asumir la configuración del proveedor de credenciales de rol

Configure esta funcionalidad mediante lo siguiente:

**credential\_source**- configuración de AWS **config** archivos compartidos

Se usa en EC2 las instancias de Amazon o en los contenedores de Amazon Elastic Container Service para especificar dónde puede encontrar la herramienta las credenciales que tienen permiso para asumir la función que especificas con el `role_arn` parámetro. SDK

Valor predeterminado: ninguno.

Valores válidos:

- Entorno: especifica que la herramienta SDK o herramienta debe recuperar las credenciales de origen de las variables de entorno [AWS\\_ACCESS\\_KEY\\_ID](#) y [AWS\\_SECRET\\_ACCESS\\_KEY](#).
- Ec2 InstanceMetadata: especifica que la herramienta SDK o herramienta debe utilizar el [IAM rol adjunto al perfil de la EC2 instancia para](#) obtener las credenciales de origen.
- EcsContainer— Especifica que la herramienta SDK o herramienta debe utilizar la [IAM función asociada al ECS contenedor para obtener las](#) credenciales de origen.

No puede especificar `credential_source` y `source_profile` en el mismo perfil.

Ejemplo de configuración de esto en un `config` archivo para indicar que las credenciales deben proceder de AmazonEC2:

```
credential_source = Ec2InstanceMetadata
role_arn = arn:aws:iam::123456789012:role/my-role-name
```

### **duration\_seconds**- configuración de AWS **config** archivos compartidos

Especifica la duración máxima de la sesión de rol, en segundos.

Esta configuración solo se aplica cuando el perfil especifica que se asume un rol.

Valor predeterminado: 3600 segundos (una hora)

Valores válidos: Este valor puede oscilar entre 900 segundos (15 minutos) y el valor de la duración máxima de la sesión para el rol (que puede ser 43 200 segundos como máximo, o 12 horas). Para obtener más información, [consulte la configuración de duración máxima de sesión para un rol](#) en la Guía del IAM usuario.

Ejemplo de esta configuración en un archivo `config`:

```
duration_seconds = 43200
```

### **external\_id**- configuración de AWS **config** archivos compartidos

Especifica un identificador único utilizado por terceros para adoptar un rol en las cuentas de los clientes.

Esta configuración solo se aplica cuando el perfil especifica asumir un rol y la política de confianza del rol requiere un valor para `ExternalId`. El valor se asigna al parámetro `ExternalId` que se pasa a la operación `AssumeRole` cuando el perfil especifica un rol.

Valor predeterminado: ninguno.

Valores válidos: consulte [Cómo utilizar un identificador externo al conceder acceso a sus AWS recursos a un tercero](#) en la Guía del IAM usuario.

Ejemplo de esta configuración en un archivo config:

```
external_id = unique_value_assigned_by_3rd_party
```

### **mfa\_serial**- configuración de AWS **config** archivos compartidos

Especifica la identificación o el número de serie de un dispositivo de autenticación multifactorial (MFA) que el usuario debe usar al asumir una función.

Se requiere cuando se asume un rol en el que la política de confianza para ese rol incluye una condición que requiere la MFA autenticación. Para obtener más información MFA, consulte la [AWS autenticación multifactorial IAM en](#) la Guía del IAM usuario.

Valor predeterminado: ninguno.

Valores válidos: el valor puede ser un número de serie para un dispositivo de hardware (por ejemplo GAHT12345678) o un nombre de recurso de Amazon (ARN) para un MFA dispositivo virtual. El formato de ARN es: `arn:aws:iam::account-id:mfa/mfa-device-name`

Ejemplo de esta configuración en un archivo config:

En este ejemplo, se asume un MFA dispositivo virtual MyMFADevice, llamado, que se creó para la cuenta y se habilitó para un usuario.

```
mfa_serial = arn:aws:iam::123456789012:mfa/MyMFADevice
```

### **role\_arn**- configuración de AWS **config** archivos compartidos, **AWS\_ROLE\_ARN**: variable de entorno, **aws.roleArn**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica el nombre de recurso de Amazon (ARN) de un IAM rol que desea usar para realizar las operaciones solicitadas con este perfil.

Valor predeterminado: ninguno.

Valores válidos: el valor debe ser el ARN de un IAM rol y tener el siguiente formato: `arn:aws:iam::account-id:role/role-name`

Además, también debe especificar una de las siguientes configuraciones:

- `source_profile`: para identificar otro perfil y usarlo para buscar las credenciales que tengan permiso para asumir el rol en este perfil.
- `credential_source`— Utilizar las credenciales identificadas por las variables de entorno actuales o las credenciales adjuntas a un perfil de EC2 instancia de Amazon o a una instancia de ECS contenedor de Amazon.
- `web_identity_token_file`— Utilizar proveedores de identidad públicos o cualquier proveedor de identidad compatible con OpenID Connect (OIDC) para los usuarios que se hayan autenticado en una aplicación móvil o web.

**role\_session\_name**- configuración de archivos compartidos AWS **config**,

**AWS\_ROLE\_SESSION\_NAME**: variable de entorno, **aws.roleSessionName**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica el nombre que se va a asociar a la sesión de rol. Este nombre aparece en los registros de AWS CloudTrail para las entradas asociadas a esta sesión, que puede resultar útil al realizar auditorías. Para obtener más información, consulte el [CloudTrail userIdentity elemento de la Guía del usuario AWS CloudTrail](#).

Valor predeterminado: un parámetro opcional. Si no proporciona este valor, se genera automáticamente un nombre de sesión en caso de que el perfil asuma un rol.

Valores válidos: se proporcionan al `RoleSessionName` parámetro cuando el AWS CLI o AWS API llama a la `AssumeRole` operación (o a operaciones como la `AssumeRoleWithWebIdentity` operación) en su nombre. El valor pasa a formar parte del usuario de rol asumido Amazon Resource Name (ARN) que puede consultar y aparece como parte de las entradas de CloudTrail registro de las operaciones invocadas por este perfil.

`arn:aws:sts::123456789012:assumed-role/my-role-name/my-role_session_name.`

Ejemplo de esta configuración en un archivo `config`:

```
role_session_name = my-role-session-name
```

**source\_profile**- configuración de AWS **config** archivos compartidos

Especifica otro perfil cuyas credenciales se utilizan para asumir la función especificada en la configuración `role_arn` del perfil original. Para saber cómo se utilizan los perfiles en los `credentials` archivos AWS `config` y archivos compartidos, consulte [Archivos compartidos config y credentials](#).

Si especifica un perfil que también sea un perfil de asunción de roles, cada rol se asumirá en orden secuencial para resolver completamente las credenciales. Esta cadena se detiene cuando SDK encuentra un perfil con credenciales. El encadenamiento de roles limita tu sesión AWS CLI o sesión de AWS API rol a un máximo de una hora y no se puede aumentar. Para obtener más información, consulta [los términos y conceptos de los roles](#) en la Guía del IAM usuario.

Valor predeterminado: ninguno.

Valores válidos: una cadena de texto que consiste en el nombre de un perfil definido en los archivos `config` y `credentials`. También debe especificar un valor para `role_arn` en el perfil actual.

No puede especificar `credential_source` y `source_profile` en el mismo perfil.

Ejemplo de esta configuración en un archivo de configuración:

```
[profile A]
source_profile = B
role_arn = arn:aws:iam::123456789012:role/RoleA
role_session_name = ProfileARoleSession

[profile B]
credential_process = ./aws_signing_helper credential-process --certificate /
path/to/certificate --private-key /path/to/private-key --trust-anchor-
arn arn:aws:rolesanywhere:region:account:trust-anchor/TA_ID --profile-
arn arn:aws:rolesanywhere:region:account:profile/PROFILE_ID --role-arn
arn:aws:iam::account:role/ROLE_ID
```

En el ejemplo anterior, el A perfil indica a la herramienta SDK o herramienta que busque automáticamente las credenciales del B perfil vinculado. En este caso, el B perfil utiliza la herramienta auxiliar de credenciales proporcionada por [Funciones de IAM en cualquier lugar](#) para obtener las credenciales del. AWS SDK Estas credenciales temporales las utiliza el código para acceder a los recursos de AWS . El rol especificado debe tener políticas de IAM permisos adjuntas que permitan ejecutar el código solicitado, como el comando o API el Servicio de AWS método. Cada acción que realiza el perfil A incluye el nombre de la sesión del rol en CloudTrail los registros.

Para ver un segundo ejemplo de encadenamiento de funciones, puede usar la siguiente configuración si tiene una aplicación en una instancia de Amazon Elastic Compute Cloud y desea que esa aplicación asuma otra función.

```
[profile A]
source_profile = B
role_arn = arn:aws:iam::123456789012:role/RoleA
role_session_name = ProfileARoleSession
```

```
[profile B]
credential_source=Ec2InstanceMetadata
```

El perfil A utilizará las credenciales de la EC2 instancia de Amazon para asumir el rol especificado y renovará las credenciales automáticamente.

**web\_identity\_token\_file**- configuración de AWS **config** archivos compartidos, **AWS\_WEB\_IDENTITY\_TOKEN\_FILE**: variable de entorno, **aws.webIdentityTokenFile**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica la ruta a un archivo que contiene un token de acceso de un [proveedor OAuth 2.0 compatible](#) o de un [proveedor de identidad de OpenID Connect ID](#).

Esta configuración permite la autenticación mediante proveedores de federaciones de identidades web, como [Google](#), [Facebook](#) y [Amazon](#), entre muchos otros. La SDK herramienta para desarrolladores carga el contenido de este archivo y lo pasa como `WebIdentityToken` argumento cuando llama a la `AssumeRoleWithWebIdentity` operación en tu nombre.

Valor predeterminado: ninguno.

Valores válidos: este valor debe ser una ruta y un nombre de archivo. El archivo debe contener un token de acceso OAuth 2.0 o un token de OpenID Connect que le haya proporcionado un proveedor de identidad. Las rutas relativas se consideran relativas al directorio de trabajo del proceso.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con AWS SDK for Java y AWS SDK para Kotlin únicamente.

<a href="#">SDK</a>	Completamente	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Parcialmente	<code>credential_source</code> no admitido. <code>duration_seconds</code> no admitido. <code>mfa_serial</code> no admitido.
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos <code>config</code> , debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Parcialmente	<code>mfa_serial</code> no se admite. <code>duration_seconds</code> no se admite.
<a href="#">SDK para Java 1.x</a>	Parcialmente	<code>credential_source</code> no se admite. <code>mfa_serial</code> no se admite. JVM no se admiten las propiedades del sistema.
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Parcialmente	<code>credential_source</code> no admitidas.
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Proveedor de credenciales de contenedor

El proveedor de credenciales del contenedor obtiene las credenciales de la aplicación contenerizada del cliente. Este proveedor de credenciales es útil para los clientes de Amazon Elastic Container Service (AmazonECS) y Amazon Elastic Kubernetes Service (Amazon EKS). EKS SDKs intenta cargar las credenciales desde el HTTP punto de enlace especificado mediante una solicitud. GET

Si utilizas AmazonECS, te recomendamos que utilices un IAM rol de tarea para mejorar el aislamiento, la autorización y la auditabilidad de las credenciales. Cuando se configura, Amazon ECS establece la variable de entorno `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` que utilizan las herramientas SDKs y para obtener las credenciales. Para configurar Amazon ECS para esta funcionalidad, consulte [IAM Función de tarea](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Si utilizas AmazonEKS, te recomendamos que utilices Amazon EKS Pod Identity para mejorar el aislamiento de credenciales, los privilegios mínimos, la auditabilidad, el funcionamiento independiente, la reutilización y la escalabilidad. Tanto tu pod como un IAM rol están asociados a una cuenta de servicio de Kubernetes para administrar las credenciales de tus aplicaciones. Para obtener más información sobre Amazon EKS Pod Identity, consulta [Amazon EKS Pod Identities](#) en la Guía del EKS usuario de Amazon. Cuando se configura, Amazon EKS establece las variables de entorno `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` y `AWS_CONTAINER_CREDENTIALS_FULL_URI` y las variables que utilizan las herramientas SDKs y para obtener las credenciales. Para obtener información sobre la configuración, consulta [Cómo configurar el Amazon EKS Pod Identity Agent](#) en la Guía del EKS usuario de Amazon o [Amazon EKS Pod Identity simplifica IAM los permisos de las aplicaciones en los EKS clústeres de Amazon](#) en el sitio web del AWS blog.

Configure esta funcionalidad mediante lo siguiente:

**`AWS_CONTAINER_CREDENTIALS_FULL_URI`**: variable de entorno

Especifica el HTTP URL punto de enlace completo SDK que se debe utilizar al solicitar credenciales. Esto incluye tanto el esquema como el host.

Valor predeterminado: ninguno.

Valores válidos: válidosURI.

Nota: Esta configuración es una alternativa a `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` y solo se usará si `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` no está establecida.

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credentials
```

o

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost:8080/get-credentials
```

### **AWS\_CONTAINER\_CREDENTIALS\_RELATIVE\_URI:** variable de entorno

Especifica el HTTP URL punto final relativo que se debe utilizar SDK al realizar una solicitud de credenciales. El valor se añade al ECS nombre de host predeterminado de Amazon de. 169.254.170.2

Valor predeterminado: ninguno.

Valores válidos: relativo válidoURI.

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/get-credentials?a=1
```

### **AWS\_CONTAINER\_AUTHORIZATION\_TOKEN:** variable de entorno

Especifica un token de autorización en texto sin formato. Si se establece esta variable, se SDK establecerá el encabezado de autorización de la HTTP solicitud con el valor de la variable de entorno.

Valor predeterminado: ninguno.

Valores válidos: Cadena.

Nota: Esta configuración es una alternativa a `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` y solo se usará si `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` no está establecida.

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credential  
export AWS_CONTAINER_AUTHORIZATION_TOKEN=Basic abcd
```

**AWS\_CONTAINER\_AUTHORIZATION\_TOKEN\_FILE:** variable de entorno

Especifica una ruta de archivo absoluta a un archivo que contiene el token de autorización en texto sin formato.

Valor predeterminado: ninguno.

Valores válidos: Cadena.

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credential
export AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE=/path/to/token
```

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	C	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	
<a href="#">SDK para Java 2.x</a>	Sí	AWS_CONTAINER_CREDENTIALS_FULL_URI y también se utilizan para <a href="#">Lambda SnapStart para Java</a> .
<a href="#">SDK para Java 1.x</a>	Sí	AWS_CONTAINER_CREDENTIALS_FULL_URI y también se utilizan para <a href="#">Lambda SnapStart para Java</a> .

SDK	C	Notas o más información
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## IAM Proveedor de credenciales de Identity Center

Este mecanismo de autenticación se utiliza AWS IAM Identity Center para obtener acceso a su código mediante un inicio de sesión único (SSO). Servicios de AWS

### Note

En la AWS SDK API documentación, el proveedor de credenciales del Centro de IAM Identidad se denomina proveedor de SSO credenciales.

Tras activar IAM Identity Center, defina un perfil para su configuración en el archivo compartido AWS config. Este perfil se utiliza para conectarse al portal de acceso al IAM Identity Center. Cuando un usuario se autentica correctamente en IAM Identity Center, el portal devuelve las credenciales de corta duración para el IAM rol asociado a ese usuario. Para obtener información sobre cómo

SDK obtiene las credenciales temporales de la configuración y las utiliza para las Servicio de AWS solicitudes, consulte [Comprender la autenticación del Centro de identidades de IAM](#).

Hay dos formas de configurar IAM Identity Center a través del config archivo:

- Configuración (recomendada) del proveedor de SSO tokens: duraciones de sesión prolongadas. Incluye soporte para duraciones de sesión personalizadas.
- Configuración antigua que no se puede actualizar: utiliza una sesión fija de ocho horas.

En ambas configuraciones, tendrá que volver a iniciar sesión cuando caduque la sesión.

Las dos guías siguientes contienen información adicional sobre Identity Center: IAM

- [AWS IAM Identity Center Guía del usuario](#)
- [AWS IAM Identity Center API Referencia del portal](#)

Para obtener información detallada sobre cómo las herramientas SDKs y herramientas utilizan y actualizan las credenciales con esta configuración, consulte [Comprender la autenticación del Centro de identidades de IAM](#).

## Requisitos previos

Primero debe habilitar IAM Identity Center. Para obtener más información sobre cómo habilitar IAM la autenticación de Identity Center, consulte [Habilitación AWS IAM Identity Center](#) en la Guía del AWS IAM Identity Center usuario.

### Note

Como alternativa, para conocer todos los requisitos previos y la configuración necesaria de los config archivos compartidos que se detalla en esta página, consulte las instrucciones de configuración [IAM Autenticación de Identity Center para su SDK herramienta](#) detalladas.

## SSO configuración del proveedor de tokens

Cuando utilizas la configuración del proveedor de SSO tokens, tu herramienta AWS SDK o tu herramienta actualizan automáticamente la sesión hasta el período de sesión extendido. Para obtener más información sobre la duración y la duración máxima de la sesión, consulte [Configurar la](#)

[duración de la sesión del portal de AWS acceso y las aplicaciones integradas de IAM Identity Center](#) en la Guía del AWS IAM Identity Center usuario.

La `sso-session` sección del config archivo se usa para agrupar las variables de configuración para adquirir los tokens de SSO acceso, que luego se pueden usar para adquirir AWS credenciales. Para obtener más información sobre esta sección dentro de un config archivo, consulte [Formato del archivo de configuración](#).

El siguiente ejemplo de config archivo compartido configura la herramienta SDK o mediante un dev perfil para solicitar las credenciales de IAM Identity Center.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

En los ejemplos anteriores se muestra cómo definir una `sso-session` sección y asociarla a un perfil. Normalmente, `sso_account_id` y `sso_role_name` debe configurarse en la `profile` sección para SDK poder solicitar AWS las credenciales. `sso_region`, `sso_start_url`, y `sso_registration_scopes` debe configurarse dentro de la `sso-session` sección.

`sso_account_id` y `sso_role_name` no son necesarios para todos los escenarios de configuración de los SSO tokens. Si su aplicación solo utiliza Servicios de AWS ese soporte de autenticación de portador, no necesitará AWS las credenciales tradicionales. La autenticación de portador es un esquema de HTTP autenticación que utiliza fichas de seguridad denominadas fichas de portador. En este escenario, no se necesitan `sso_account_id` ni `sso_role_name`. Consulte la Servicio de AWS guía individual para determinar si el servicio admite la autorización de tokens de portador.

Los ámbitos de registro se configuran como parte de un `sso-session`. El alcance es un mecanismo en OAuth 2.0 para limitar el acceso de una aplicación a la cuenta de un usuario. El ejemplo anterior proporciona el `sso_registration_scopes` acceso necesario para enumerar las cuentas y los roles.

El siguiente ejemplo muestra cómo puede reutilizar la misma `sso-session` configuración en varios perfiles.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[profile prod]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole2

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

El token de autenticación se almacena en caché en el disco en el directorio `~/ .aws/sso/cache` con un nombre de archivo basado en el nombre de la sesión.

## Configuración heredada no actualizable

La actualización automática de tokens no se admite con la configuración no actualizable heredada. Se recomienda utilizar el [SSO configuración del proveedor de tokens](#) en su lugar.

Para utilizar la configuración heredada no renovable, debe especificar los siguientes parámetros en su perfil:

- `sso_start_url`
- `sso_region`
- `sso_account_id`
- `sso_role_name`

Debe especificar el portal de usuario para un perfil con la configuración de `sso_start_url` y `sso_region`. Los permisos se especifican con la configuración de `sso_account_id` y `sso_role_name`.

En el siguiente ejemplo se definen los cuatro valores obligatorios del archivo `config`.

```
[profile my-sso-profile]
sso_start_url = https://my-sso-portal.awsapps.com/start
```

```
sso_region = us-west-2
sso_account_id = 111122223333
sso_role_name = SSOReadOnlyRole
```

El token de autenticación se almacena en caché en el disco en el directorio `~/ .aws/sso/cache` con un nombre de archivo basado en el `sso_start_url`.

## IAM Configuración del proveedor de credenciales de Identity Center

Configure esta funcionalidad mediante lo siguiente:

### **sso\_start\_url**- configuración de AWS **config** archivos compartidos

La URL que apunta al centro de IAM identidad, al emisor URL o al portal URL de acceso de su organización. Para obtener más información, consulte [Uso del portal de AWS acceso](#) en la Guía del AWS IAM Identity Center usuario.

Para encontrar este valor, abra la [consola de IAM Identity Center](#), consulte el panel de control y busque el portal de AWS acceso URL.

- Como alternativa, a partir de la versión 2.22.0 de AWS CLI, puede utilizar el valor de `Issuer.AWS URL`

### **sso\_region**- configuración de archivos compartidos AWS **config**

El Región de AWS que contiene el host del portal de IAM Identity Center, es decir, la región que seleccionó antes de activar IAM Identity Center. Es independiente de AWS la región predeterminada y puede ser diferente.

Para obtener una lista completa de ellos Regiones de AWS y sus códigos, consulte los [puntos finales regionales](#) en. Referencia general de Amazon Web Services Para encontrar este valor, abra la [consola de IAM Identity Center](#), consulte el panel de control y busque la región.

### **sso\_account\_id**- configuración de AWS **config** archivos compartidos

El identificador numérico del Cuenta de AWS que se agregó a través del AWS Organizations servicio para usarlo en la autenticación.

Para ver la lista de cuentas disponibles, vaya a la [consola de IAM Identity Center](#) y abra la Cuentas de AWS página. También puede ver la lista de cuentas disponibles mediante el [ListAccounts](#) API método de la API Referencia del AWS IAM Identity Center portal. Por ejemplo, puede llamar al AWS CLI método [list-accounts](#).

## **sso\_role\_name**- configuración de archivos compartidos AWS **config**

El nombre de un conjunto de permisos proporcionado como un IAM rol que define los permisos resultantes del usuario. El rol debe existir en el lugar Cuenta de AWS especificado por `sso_account_id`. Utilice el nombre del rol, no el nombre de Amazon Resource Name (ARN) del rol.

Los conjuntos de permisos tienen adjuntas IAM políticas y políticas de permisos personalizadas y definen el nivel de acceso que los usuarios tienen asignado a sus permisos Cuentas de AWS.

Para ver la lista de conjuntos de permisos disponibles por cada Cuenta de AWS uno, vaya a la [consola de IAM Identity Center](#) y abra la Cuentas de AWS página. Elija el nombre correcto del conjunto de permisos que aparece en la Cuentas de AWS tabla. También puede ver la lista de conjuntos de permisos disponibles mediante el [ListAccountRoles](#) API método en la API Referencia del AWS IAM Identity Center portal. Por ejemplo, puede llamar al AWS CLI método [list-account-roles](#).

## **sso\_registration\_scopes**- configuración de AWS **config** archivos compartidos

Una lista delimitada por comas de los ámbitos válidos que deben autorizarse para la `sso-session`. Una solicitud puede pedir uno o varios ámbitos y el token de acceso emitido a la solicitud se limita a los ámbitos concedidos. Se `sso:account:access` debe conceder un alcance mínimo de `iam:iam:iam` para recuperar un token de actualización del servicio IAM Identity Center. Para ver la lista de opciones de alcance de acceso disponibles, consulte los [ámbitos de acceso](#) en la Guía del AWS IAM Identity Center usuario.

Estos ámbitos definen los permisos que se solicitan para autorizar el OIDC cliente registrado y los tokens de acceso recuperados por el cliente. Los ámbitos autorizan el acceso a los puntos finales autorizados por el portador del IAM Identity Center.

Esta configuración no aplica a la configuración heredada no actualizable. Los tokens emitidos con la configuración heredada tienen un alcance limitado de `sso:account:access` de forma implícita.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	Categoría	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDKpara C++</a>	Sí	
<a href="#">SDKpara Go V2 (1.x)</a>	Sí	
<a href="#">SDKpara Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDKpara Java 2.x</a>	Sí	Los valores de configuración también se admiten en el archivo <code>credentials</code> .
<a href="#">SDKpara Java 1.x</a>	No	
<a href="#">SDKpara JavaScript 3.x</a>	Sí	
<a href="#">SDKpara JavaScript 2.x</a>	Sí	
<a href="#">SDKpara Kotlin</a>	Sí	
<a href="#">SDKpara .NET3.x</a>	Sí	
<a href="#">SDKpara PHP 3.x</a>	Sí	
<a href="#">SDKpara Python (Boto3)</a>	Sí	
<a href="#">SDKpara Ruby 3.x</a>	Sí	
<a href="#">SDKpara Rust</a>	Parcial	Solo configuración heredada no actualizable.
<a href="#">SDKpara Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## IMDS proveedor de credenciales

Instance Metadata Service (IMDS) proporciona datos sobre la instancia que puede usar para configurar o administrar la instancia en ejecución. Para obtener más información sobre los datos disponibles, consulta [Cómo trabajar con metadatos de instancias](#) en la Guía del EC2 usuario de Amazon. Amazon EC2 proporciona un punto de enlace local disponible para las instancias que puede proporcionar varios bits de información a la instancia. Si la instancia tiene una función asociada, puede proporcionar un conjunto de credenciales válidas para esa función. SDKs Pueden usar ese punto final para resolver las credenciales como parte de su [cadena de proveedores de credenciales predeterminada](#). De forma predeterminada, se usa la versión 2 (IMDSv2) del Servicio de Metadatos de Instancia, una versión más segura IMDS que usa un token de sesión. Si se produce un error debido a una condición que no se puede volver a intentar (códigos de HTTP error 403, 404, 405), IMDSv1 se utiliza como alternativa.

Configure esta funcionalidad mediante lo siguiente:

**AWS\_EC2\_METADATA\_DISABLED**: variable de entorno

Si debe o no intentar utilizar Amazon EC2 Instance Metadata Service (IMDS) para obtener credenciales.

Valor predeterminado: `false`.

Valores válidos:

- **true**— No lo utilice IMDS para obtener credenciales.
- **false**— Se utiliza IMDS para obtener credenciales.

**ec2\_metadata\_v1\_disabled**- configuración de AWS **config** archivos compartidos, **AWS\_EC2\_METADATA\_V1\_DISABLED**: variable de entorno, **aws.disableEc2MetadataV1**- propiedad JVM del sistema: solo en Java/Kotlin

Si se debe utilizar o no la versión 1 (IMDSv1) del Servicio de Metadatos de Instancia como alternativa en caso de que se produzca un error. IMDSv2

### Note

Los nuevos SDKs no admiten esta configuración IMDSv1 y, por lo tanto, no la admiten. Para obtener más información, consulte la tabla [Compatibilidad con AWS SDKs](#).

Valor predeterminado: `false`.

Valores válidos:

- **true**— No lo utilices IMDSv1 como alternativa.
- **false**— Úselo IMDSv1 como alternativa.

**ec2\_metadata\_service\_endpoint**- configuración de AWS **config** archivos compartidos, **AWS\_EC2\_METADATA\_SERVICE\_ENDPOINT**: variable de entorno, **aws.ec2MetadataServiceEndpoint**- propiedad JVM del sistema: solo en Java/Kotlin

El punto final de IMDS. Este valor anula la ubicación predeterminada en la que AWS SDKs las herramientas buscarán los metadatos de las EC2 instancias de Amazon.

Valor predeterminado: si el `ec2_metadata_service_endpoint_mode` es igual a IPv4, el punto de conexión predeterminado es `http://169.254.169.254`. Valor predeterminado: si el `ec2_metadata_service_endpoint_mode` es igual a IPv6, el punto de conexión predeterminado es `http://[fd00:ec2::254]`.

Valores válidos: válidosURI.

**ec2\_metadata\_service\_endpoint\_mode**- configuración de AWS **config** archivos compartidos, **AWS\_EC2\_METADATA\_SERVICE\_ENDPOINT\_MODE**: variable de entorno, **aws.ec2MetadataServiceEndpointMode**- propiedad JVM del sistema: solo en Java/Kotlin

El modo de punto final de IMDS

Valor predeterminado: IPv4.

Valores válidos: IPv4, IPv6.

#### Note

El proveedor de IMDS credenciales forma parte de [Comprenda la cadena de proveedores de credenciales](#). Sin embargo, el proveedor de IMDS credenciales solo se comprueba después de varios otros proveedores de esta serie. Por lo tanto, si desea que su programa utilice las credenciales de este proveedor, debe eliminar otros proveedores de credenciales válidos de la configuración o utilizar un perfil diferente. Como alternativa, en lugar de confiar en la cadena de proveedores de credenciales para descubrir automáticamente qué proveedor devuelve credenciales válidas, especifique el uso del proveedor de IMDS credenciales en

el código. Puede especificar las fuentes de credenciales directamente al crear clientes de servicio.

## Seguridad de las credenciales IMDS

De forma predeterminada, cuando no AWS SDK está configurado con credenciales válidas, SDK intentará utilizar el Amazon EC2 Instance Metadata Service (IMDS) para recuperar las credenciales de un AWS rol. Este comportamiento se puede deshabilitar configurando la variable del entorno de `AWS_EC2_METADATA_DISABLED` en `true`. Esto evita actividades de red innecesarias y mejora la seguridad en redes que no son de confianza en las que se puede suplantar el Amazon EC2 Instance Metadata Service.

### Note

AWS SDK los clientes configurados con credenciales válidas nunca las utilizarán IMDS para recuperar las credenciales, independientemente de cualquiera de estas configuraciones.

## Inhabilitar el uso de las credenciales de Amazon EC2 IMDS

La forma de configurar esta variable de entorno depende del sistema operativo que se utilice y de si desea o no que el cambio sea persistente.

### Linux y macOS

Los clientes que utilizan Linux o macOS pueden configurar esta variable de entorno con el siguiente comando:

```
$ export AWS_EC2_METADATA_DISABLED=true
```

Si desea que esta configuración se mantenga durante varias sesiones del intérprete de comandos y se reinicie el sistema, puede añadir el comando anterior al archivo de perfil de intérprete de comandos, como `.bash_profile`, `.zsh_profile` o `.profile`.

### Windows

Los clientes que utilizan Windows pueden configurar esta variable de entorno con el siguiente comando:

```
$ set AWS_EC2_METADATA_DISABLED=true
```

Si desea que esta configuración sea persistente en varias sesiones de intérprete de comandos y se reinicie el sistema, utilice el siguiente comando en su lugar:

```
$ setx AWS_EC2_METADATA_DISABLED=true
```

### Note

El comando `setx` no aplica el valor a la sesión de shell actual, por lo que tendrá que volver a cargar o volver a abrir el intérprete de comandos para que el cambio surta efecto.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Todas las configuraciones de propiedades del JVM sistema son compatibles con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	C	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos <code>config</code> , debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Parcial	JVM propiedades del sistema: se usa <code>com.amazonaws.sdk.disableEc2MetadataV1</code> en lugar de <code>aws.sdk.disableEc2MetadataV1</code> ; <code>aws.ec2Me</code>

SDK	C	Notas o más información
	e	<code>tadataServiceEndpoint</code> y <code>aws.ec2MetadataServiceEndpointMode</code> no se admite.
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	No utiliza la opción IMDSv1 alternativa.
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	No utiliza la opción IMDSv1 alternativa.
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	Puede deshabilitar la opción IMDSv1 alternativa de forma explícita en el código mediante <code>[Amazon.Util.EC2InstanceMetadata]::EC2MetadataV1Disabled = \$true</code> .

## Proveedor de credenciales de proceso

SDKs proporcionan una forma de ampliar la cadena de proveedores de credenciales para casos de uso personalizados. Este proveedor se puede utilizar para proporcionar implementaciones personalizadas, como recuperar credenciales de un almacén de credenciales local o integrarlas con su proveedor de identificación local.

Por ejemplo, IAM Roles Anywhere utiliza `credential_process` para obtener credenciales temporales en nombre de su aplicación. Para configurar `credential_process` para este uso, consulte [Funciones de IAM en cualquier lugar](#).

**Note**

A continuación se describe un método para obtener credenciales de un proceso externo y se puede utilizar si se ejecuta software fuera de AWS. Si está construyendo sobre una AWS recurso informático, utilice otros proveedores de credenciales. Si usa esta opción, debe asegurarse de que el archivo de configuración esté lo más bloqueado posible siguiendo las mejores prácticas de seguridad para su sistema operativo. Confirme que su herramienta de credenciales personalizada no escriba ninguna información secreta en ellaStdErr, ya que y SDKs AWS CLI puede capturar y registrar dicha información, lo que podría exponerla a usuarios no autorizados.

Configure esta funcionalidad mediante lo siguiente:

**credential\_process**- compartido AWS **config** configuración de archivos

Especifica un comando externo que la herramienta SDK o herramienta ejecuta en su nombre para generar o recuperar las credenciales de autenticación que se van a utilizar. La configuración especifica el nombre del programa o comando que se SDK invocará. Cuando SDK invoca el proceso, espera a que el proceso escriba datos en él. JSON stdout El proveedor personalizado debe devolver la información en un formato específico. Esa información contiene las credenciales que la herramienta SDK o herramienta puede usar para autenticarte.

**Note**

El proveedor de credenciales del proceso forma parte del [Comprenda la cadena de proveedores de credenciales](#). Sin embargo, el proveedor de credenciales del proceso solo se comprueba después de varios otros proveedores de esta serie. Por lo tanto, si desea que su programa utilice las credenciales de este proveedor, debe eliminar otros proveedores de credenciales válidos de la configuración o utilizar un perfil diferente. Como alternativa, en lugar de confiar en la cadena de proveedores de credenciales para descubrir automáticamente qué proveedor devuelve credenciales válidas, especifique el uso del proveedor de credenciales de proceso en el código. Puede especificar las fuentes de credenciales directamente al crear clientes de servicio.

## Especificar la ruta al programa de credenciales

El valor de la configuración es una cadena que contiene la ruta a un programa que la herramienta de desarrollo SDK o la herramienta de desarrollo ejecutan en tu nombre:

- La ruta y el nombre del archivo solo pueden constar de los siguientes caracteres: A-Z, a-z, 0-9, guion ( - ), guion bajo ( \_ ), punto ( . ), barra oblicua ( / ), barra diagonal inversa ( \ ) y espacio.
- Si la ruta de acceso o el nombre del archivo contienen un espacio, rodee la ruta completa y el nombre del archivo con comillas dobles ( " " ).
- Si un nombre de parámetro o un valor de parámetro contienen un espacio, rodee ese elemento con comillas dobles ( " " ). Incluya solo el nombre o el valor, no el par.
- No incluya ninguna variable de entorno en las cadenas. Por ejemplo, no puede incluir \$HOME ni %USERPROFILE%.
- No especifique la carpeta de inicio como ~. \* En la solicitud debe especificar la ruta completa o el nombre del archivo base. Si hay un nombre de archivo base, el sistema intentará encontrar el programa en las carpetas especificadas por la variable del entorno PATH. La ruta varía en función del sistema operativo:

El siguiente ejemplo muestra la configuración de `credential_process` en el archivo `config` compartido en Linux/macOS.

```
credential_process = "/path/to/credentials.sh" parameterWithoutSpaces "parameter with spaces"
```

El siguiente ejemplo muestra la configuración de `credential_process` en el archivo `config` compartido en Windows.

```
credential_process = "C:\Path\To\credentials.cmd" parameterWithoutSpaces "parameter with spaces"
```

- Se puede especificar dentro de un perfil específico:

```
[profile cred_process]  
credential_process = /Users/username/process.sh  
region = us-east-1
```

## Salida válida del programa de credenciales

SDKEjecuta el comando tal como se especifica en el perfil y, a continuación, lee los datos del flujo de salida estándar. El comando que especifique, ya sea un script o un programa binario, debe generar un JSON resultado STDOUT que coincida con la siguiente sintaxis.

```
{
  "Version": 1,
  "AccessKeyId": "an AWS access key",
  "SecretAccessKey": "your AWS secret access key",
  "SessionToken": "the AWS session token for temporary credentials",
  "Expiration": "RFC3339 timestamp for when the credentials expire"
}
```

### Note

En la fecha de publicación del presente documento, la clave `Version` debe establecerse en 1. Puede aumentar con el paso del tiempo a medida que la estructura evolucione.

La `Expiration` clave es una marca de tiempo RFC3339 formateada. Si la `Expiration` clave no aparece en el resultado de la herramienta, se SDK supone que las credenciales son credenciales de larga duración que no se actualizan. De otro modo, las credenciales se consideran credenciales temporales y se actualizan automáticamente volviendo a ejecutar el comando `credential_process` antes de que caduquen las credenciales.

### Note

SDKNo almacena en caché las credenciales de los procesos externos de la misma forma en que lo hace con las credenciales de rol. Si se requiere el almacenamiento en caché, debe implementarlo en el proceso externo.

El proceso externo puede devolver un código de devolución distinto de cero para indicar que se ha producido un error al intentar recuperar las credenciales.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Compatible	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Sí	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	

SDK	C	Notas o más información
<a href="#">Herramientas para PowerShell</a>	Sí	

## AWS SDKs y funciones estandarizadas de Tools

Muchas funciones se han estandarizado con valores predeterminados consistentes y funcionan de la misma manera en muchas SDKs de ellas. Esta coherencia aumenta la productividad y la claridad a la hora de codificar en varios SDKs. Todos los ajustes se pueden anular en el código, consulta tus especificaciones SDK API para obtener más información.

### Important

No todas son SDKs compatibles con todas las funciones, ni siquiera con todos los aspectos de una función.

### Temas

- [Puntos finales basados en cuentas](#)
- [Application ID](#)
- [Metadatos de EC2 instancias de Amazon](#)
- [Puntos de acceso de Amazon S3](#)
- [Puntos de acceso multirregión de Amazon S3](#)
- [Región de AWS](#)
- [AWS STS Puntos finales regionales](#)
- [Pila doble y puntos finales FIPS](#)
- [Detección de puntos de conexión](#)
- [Ajustes de configuración general](#)
- [IMDScliente](#)
- [Comportamiento de los reintentos](#)
- [Compresión de solicitudes](#)

- [Puntos de conexión específicos del servicio](#)
- [Valores predeterminados de configuración inteligente](#)

## Puntos finales basados en cuentas

Los puntos de enlace basados en cuentas ayudan a garantizar un alto rendimiento y escalabilidad al utilizar su Cuenta de AWS ID para agilizar el enrutamiento de las Servicio de AWS solicitudes de servicios compatibles con esta función. Cuando utilice un proveedor de credenciales y un AWS SDK servicio que admita puntos de enlace basados en cuentas, se creará y SDK utilizará automáticamente un punto de enlace basado en cuentas en lugar de un punto de enlace regional. Los puntos de enlace basados en cuentas adoptan la forma de: se sustituyen por su ID `https://<account-id>.ddb.<region>.amazonaws.com` y `<account-id>` se sustituyen por su Cuenta de AWS `<region>` Región de AWS

De forma predeterminada, el ID de la cuenta se recopila cuando se procesa la solicitud y se utiliza para crear un punto final. La resolución de credenciales también se produce cuando se procesa la solicitud y puede cambiar el método de resolución del punto final. Según el proveedor de credenciales que utilice, es posible que el ID de la cuenta tenga un origen diferente.

Configure esta funcionalidad mediante lo siguiente:

**aws\_account\_id**- configuración de AWS **config** archivos compartidos, **AWS\_ACCOUNT\_ID**: variable de entorno, **aws.accountId**- propiedad JVM del sistema: solo en Java/Kotlin

El ID. Cuenta de AWS Se utiliza para el enrutamiento de puntos finales basado en cuentas. Un Cuenta de AWS ID tiene un formato similar al 111122223333.

El enrutamiento de puntos finales basado en cuentas proporciona un mejor rendimiento de las solicitudes para algunos servicios.

**account\_id\_endpoint\_mode**- configuración de archivos compartidos AWS **config**, **AWS\_ACCOUNT\_ID\_ENDPOINT\_MODE**: variable de entorno, **aws.accountIdEndpointMode**- propiedad JVM del sistema: solo en Java/Kotlin

Esta configuración se usa para desactivar el enrutamiento de puntos finales basado en cuentas si es necesario y omitir las reglas basadas en cuentas.

Valor predeterminado: `preferred`

Valores válidos:

- **preferred**— El punto final debe incluir el ID de cuenta, si está disponible.
- **disabled**— Un punto final resuelto no incluye el ID de cuenta.
- **required**— El punto final debe incluir el ID de la cuenta. Si el ID de la cuenta no está disponible, se SDK produce un error.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	Com e	Publicado en la SDK versión	Notas o más información
<a href="#">AWS CLI v2</a>	No		
<a href="#">SDK para C++</a>	No		
<a href="#">SDK para Go V2 (1.x)</a>	Sí	v1.35.0	
<a href="#">SDK para Go 1.x (V1)</a>	No		
<a href="#">SDK para Java 2.x</a>	Sí	v2.28.4	
<a href="#">SDK para Java 1.x</a>	Sí	v1.12.771	
<a href="#">SDK para 3.x JavaScript</a>	Sí	v3.656.0	
<a href="#">SDK para 2.x JavaScript</a>	No		
<a href="#">SDK para Kotlin</a>	Sí	v1.3.37	
<a href="#">SDK para .NET 3.x</a>	No		

SDK	Com e	Publicado en la SDK versión	Notas o más información
<a href="#">SDKpara PHP 3.x</a>	Sí	v3.318.0	
<a href="#">SDKpara Python (Boto3)</a>	No		
<a href="#">SDKpara Ruby 3.x</a>	Sí	v1.123.0	
<a href="#">SDKpara Rust</a>	No		
<a href="#">SDKpara Swift</a>	No		
<a href="#">Herramientas para PowerShell</a>	No		

## Application ID

Una sola Cuenta de AWS puede ser utilizado por múltiples aplicaciones de clientes para realizar llamadas a Servicios de AWS. El identificador de aplicación permite a los clientes identificar qué aplicación de origen realizó una serie de llamadas mediante un Cuenta de AWS. AWS SDKsy los servicios no utilizan ni interpretan este valor más que para mostrarlo en las comunicaciones con los clientes. Por ejemplo, este valor se puede incluir en los correos electrónicos operativos o en el AWS Health Dashboard para identificar de forma exclusiva cuáles de sus aplicaciones están asociadas a la notificación.

Configure esta funcionalidad mediante lo siguiente:

**sdk\_ua\_app\_id**- compartido AWS **config** configuración de archivos, **AWS\_SDK\_UA\_APP\_ID**: variable de entorno, **aws.userAgentAppId**- propiedad JVM del sistema: solo en Java/Kotlin

Esta configuración es una cadena única que se asigna a la aplicación para identificar cuáles de las aplicaciones están dentro de una determinada Cuenta de AWS hace llamadas a AWS.

Valor predeterminado: None

Valores válidos: cadena con una longitud máxima de 50. Se permiten letras, números y los siguientes caracteres especiales: !, ,, \$, %, &, \*, +, -, ., /, ^, \_ , ` , |, ~.

Ejemplo de configuración de este valor en el archivo config:

```
[default]
sdk_ua_app_id=ABCDEF
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_SDK_UA_APP_ID=ABCDEF
export AWS_SDK_UA_APP_ID="ABC DEF"
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_SDK_UA_APP_ID ABCDEF
setx AWS_SDK_UA_APP_ID="ABC DEF"
```

Si incluye símbolos que tienen un significado especial para la concha que se utiliza, evite el valor según corresponda.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Ci e	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	No se admite el archivo compartido config.
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	No	

SDK	C	Notas o más información
<a href="#">SDK para Java 2.x</a>	Parci	No se admite la configuración de config archivos compartidos; no se admite la variable de entorno.
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	No se admiten variables de entorno.
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	No	

## Metadatos de EC2 instancias de Amazon

Amazon EC2 proporciona un servicio para las instancias denominado Instance Metadata Service (IMDS). Para obtener más información sobre este servicio, consulta [Trabajar con metadatos de instancias](#) en la Guía del EC2 usuario de Amazon. Al intentar recuperar las credenciales de una EC2 instancia de Amazon que se ha configurado con un IAM rol, la conexión al servicio de metadatos de la instancia se puede ajustar.

Configure esta funcionalidad mediante lo siguiente:

**metadata\_service\_num\_attempts**- compartido AWS **config** configuración de archivos,  
**AWS\_METADATA\_SERVICE\_NUM\_ATTEMPTS**: variable de entorno

Esta configuración especifica la cantidad total de intentos que hay que realizar antes de intentar recuperar datos desde el servicio de metadatos de instancias.

Valor predeterminado: 1

Valores válidos: número mayor o igual a 1.

**metadata\_service\_timeout**- compartido AWS **config** configuración de archivos,  
**AWS\_METADATA\_SERVICE\_TIMEOUT**: variable de entorno

Especifica el número de segundos antes de que se agote el tiempo de espera cuando se intentan recuperar datos desde el servicio de metadatos de instancias.

Valor predeterminado: 1

Valores válidos: número mayor o igual a 1.

Ejemplo de configuración de este valor en el archivo config:

```
[default]
metadata_service_num_attempts=10
metadata_service_timeout=10
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_METADATA_SERVICE_NUM_ATTEMPTS=10
export AWS_METADATA_SERVICE_TIMEOUT=10
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_METADATA_SERVICE_NUM_ATTEMPTS 10
setx AWS_METADATA_SERVICE_TIMEOUT 10
```

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Comparte	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	No	
<a href="#">SDK para Go V2 (1.x)</a>	No	
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	No	
<a href="#">SDK para Java 1.x</a>	Parcial	Solo se admite <code>AWS_METADATA_SERVICE_TIMEOUT</code> .
<a href="#">SDK para JavaScript 3.x</a>	No	
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	No	
<a href="#">SDK para .NET 3.x</a>	No	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	No	
<a href="#">SDK para Rust</a>	No	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	No	

## Puntos de acceso de Amazon S3

El servicio Amazon S3 proporciona puntos de acceso como una forma alternativa de interactuar con los buckets de Amazon S3. Los puntos de acceso pueden tener políticas y configuraciones únicas

que se pueden aplicar a ellos en lugar de directamente al bucket. Con AWS SDKs, puede utilizar el punto de acceso Amazon Resource Names (ARNs) en el campo bucket para API las operaciones en lugar de especificar el nombre del bucket de forma explícita. Se utilizan para operaciones específicas, como utilizar un punto ARN de acceso [GetObject](#) para recuperar un objeto de un depósito o utilizar un punto ARN de acceso [PutObject](#) para añadir un objeto a un depósito.

Para obtener más información sobre los puntos de acceso de Amazon S3 ARNs, consulte [Uso de puntos de acceso](#) en la Guía del usuario de Amazon S3.

Configure esta funcionalidad mediante lo siguiente:

**s3\_use\_arn\_region**- compartido AWS **config** configuración de archivos,  
**AWS\_S3\_USE\_ARN\_REGION**: variable de entorno, **aws.s3UseArnRegion**- propiedad JVM del sistema: solo Java/Kotlin, Para configurar el valor directamente en el código, consulte su especificación directamente. SDK

Esta configuración controla si SDK utiliza el punto de acceso ARN Región de AWS para construir el punto final regional de la solicitud. Esto SDK valida que el ARN Región de AWS es servido por el mismo AWS partición según la configuración del cliente Región de AWS para evitar las llamadas entre particiones que muy probablemente fallarán. Si se ha definido de forma múltiple, prevalece la configuración por código, seguida de la configuración de la variable de entorno.

Valor predeterminado: `false`

Valores válidos:

- **true**— Los SDK usos, los ARN Región de AWS al construir el punto final en lugar del configurado por el cliente Región de AWS. Excepción: si el cliente está configurado Región de AWS es un FIPS Región de AWS, entonces debe coincidir con ARN la Región de AWS. De lo contrario, se producirá un error.
- **false**— Los SDK usos configurados por el cliente Región de AWS al construir el punto final.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Configuración	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos <code>config</code> , debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Sí	JVM propiedad del sistema no compatible.
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	No sigue la prioridad estándar; el valor del archivo compartido <code>config</code> tiene prioridad sobre la variable de entorno.
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	No	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	No sigue la prioridad estándar; el valor del archivo compartido <code>config</code> tiene prioridad sobre la variable de entorno.

## Puntos de acceso multirregión de Amazon S3

Los puntos de acceso multirregionales de Amazon S3 proporcionan un punto de enlace global que las aplicaciones pueden utilizar para gestionar las solicitudes de los buckets de Amazon S3 ubicados en varios Regiones de AWS. Puede utilizar puntos de acceso multirregionales para crear aplicaciones multirregionales con la misma arquitectura utilizada en una sola región y, a continuación, ejecutar esas aplicaciones en cualquier parte del mundo.

Para obtener más información acerca de los puntos de acceso multirregión, consulte [Puntos de acceso multirregión de Amazon S3](#) en la Guía del usuario de Amazon S3.

Para obtener más información sobre los nombres de recursos de Amazon (ARNs) de puntos de acceso multirregionales, consulte [Realizar solicitudes mediante un punto de acceso multirregional](#) en la Guía del usuario de Amazon S3.

Para obtener más información acerca de los puntos de acceso multirregión, consulte [Puntos de acceso multirregión de Amazon S3](#) en la Guía del usuario de Amazon S3.

El algoritmo SigV4a es la implementación de firma que se utiliza para firmar las solicitudes regionales globales. Este algoritmo se obtiene SDK mediante una dependencia de [AWS Bibliotecas Common Runtime \(CRT\)](#)

Configure esta funcionalidad mediante lo siguiente:

**s3\_disable\_multiregion\_access\_points**- compartido AWS **config** configuración de archivos, **AWS\_S3\_DISABLE\_MULTIREGION\_ACCESS\_POINTS**: variable de entorno, **aws.s3DisableMultiRegionAccessPoints**- propiedad JVM del sistema: solo en Java/Kotlin, Para configurar el valor directamente en el código, consulte su especificación directamente. SDK

Esta configuración controla si es SDK posible que intente realizar solicitudes entre regiones. Si se ha definido de forma múltiple, prevalece la configuración por código, seguida de la configuración de la variable de entorno.

Valor predeterminado: `false`

Valores válidos:

- **true**: detiene el uso de solicitudes entre regiones.
- **false**: permite las solicitudes entre regiones mediante puntos de acceso multirregionales.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Compatible	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Región de AWS

Regiones de AWS son un concepto importante que hay que entender cuando se trabaja con ellos Servicios de AWS.

Con Regiones de AWS, puede acceder a Servicios de AWS esa residencia física en un área geográfica específica. Esto puede ser útil para evitar redundancias y para que sus datos y aplicaciones se ejecuten cerca del lugar desde donde usted y sus usuarios accederán a ellos. Las regiones proporcionar tolerancia a errores, estabilidad y resistencia, y también pueden reducir la latencia. Con las regiones, puede crear recursos redundantes que sigan estando disponibles y no resulten afectados por una interrupción regional.

La mayoría de Servicio de AWS las solicitudes están asociadas a una región geográfica en particular. Los recursos que crea en una región no existen en ninguna otra región salvo que utilice explícitamente una característica de replicación ofrecida por un Servicio de AWS. Por ejemplo, Amazon S3 y Amazon EC2 admiten la replicación entre regiones. Algunos servicios, por ejemplo IAM, no tienen recursos regionales.

El informe Referencia general de AWS contiene la siguiente información:

- Para entender la relación entre las regiones y los puntos de conexión, y para ver una lista de los puntos de conexión regionales existentes, consulte los [Puntos de conexión del servicio de AWS](#).
- Para ver la lista actual de todas las regiones y puntos de conexión para cada servicio de Servicio de AWS, consulte [Puntos de conexión de servicio y cuotas](#).

### Cómo crear clientes de servicio

Para acceder mediante programación Servicios de AWS, SDKs utilice una clase/objeto de cliente para cada uno. Servicio de AWS Si tu aplicación necesita acceder a AmazonEC2, por ejemplo, crearía un objeto EC2 cliente de Amazon para interactuar con ese servicio.

Si no se especifica explícitamente ninguna región para el cliente en el propio código, el cliente utilizará de forma predeterminada la región que se establece mediante la siguiente `region` configuración. Sin embargo, la región activa de un cliente se puede establecer explícitamente para cualquier objeto de cliente individual. La configuración de la región de esta manera prevalece sobre cualquier configuración global para ese cliente de servicio concreto. La región alternativa se especifica durante la creación de instancias de ese cliente y es específica para usted SDK (consulte su SDK guía específica o su base SDK de código).

Configure esta funcionalidad mediante lo siguiente:

**region**- configuración de archivos compartidos AWS **config**, **AWS\_REGION**: variable de entorno, **aws.region**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica el valor predeterminado que se debe Región de AWS usar en las solicitudes. AWS Esta región se usa para las solicitudes de SDK servicio que no se proporcionan con una región específica para su uso.

Valor predeterminado: ninguno. Debe especificar este valor de forma explícita.

Valores válidos:

- Cualquiera de los códigos de región disponibles para el servicio elegido, como se muestran en [Puntos de conexión de AWS](#) en la referencia general de AWS . Por ejemplo, el valor `us-east-1` establece el punto de conexión en la región Región de AWS Este de EE. UU. (Norte de Virginia).
- `aws-global` especifica el punto de enlace global para los servicios que admiten un punto de enlace global independiente además de los puntos de enlace regionales, como AWS Security Token Service (AWS STS) y Amazon Simple Storage Service (Amazon S3).

Ejemplo de configuración de este valor en el archivo `config`:

```
[default]
region = us-west-2
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_REGION=us-west-2
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_REGION us-west-2
```

La mayoría SDKs tienen un objeto de «configuración» que está disponible para establecer la región predeterminada desde el código de la aplicación. Para obtener más información, consulta tu guía específica para AWS SDK desarrolladores.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Todas las configuraciones de propiedades del JVM sistema son compatibles con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	Comentarios
<a href="#">AWS CLI v2</a>	Sí AWS CLI v2 utiliza cualquier valor introducido <code>AWS_REGION</code> antes que cualquier valor introducido <code>AWS_DEFAULT_REGION</code> (ambas variables están marcadas).
<a href="#">AWS CLI v1</a>	Sí AWS CLI v1 usa una variable de entorno nombrada <code>AWS_DEFAULT_REGION</code> para este propósito.
<a href="#">SDK para C++</a>	Sí
<a href="#">SDK para Go V2 (1.x)</a>	Sí
<a href="#">SDK para Go 1.x (V1)</a>	Sí Para usar la configuración de archivos compartidos <code>config</code> , debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí
<a href="#">SDK para Java 1.x</a>	Sí
<a href="#">SDK para JavaScript 3.x</a>	Sí
<a href="#">SDK para JavaScript 2.x</a>	Sí
<a href="#">SDK para Kotlin</a>	Sí
<a href="#">SDK para .NET 3.x</a>	Sí
<a href="#">SDK para PHP 3.x</a>	Sí
<a href="#">SDK para Python (Boto3)</a>	Sí SDK utiliza una variable de entorno nombrada <code>AWS_DEFAULT_REGION</code> para este propósito.

SDK	C	Notas o más información
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## AWS STS Puntos finales regionales

AWS Security Token Service (AWS STS) está disponible como servicio global y regional. Algunos CLIs utilizan el punto final del servicio global (<https://sts.amazonaws.com>) de forma predeterminada, mientras que otros utilizan los puntos finales del servicio regional ([https://sts.{region\\_identifier}.{partition\\_domain}](https://sts.{region_identifier}.{partition_domain})). AWS SDKs Las solicitudes globales se asignan a la región EE. UU. Este (Virginia del Norte). Para obtener más información sobre los AWS STS puntos finales, consulte los [puntos finales](#) en la AWS Security Token Service API referencia. O bien, aprenda a [administrar AWS STS Región de AWS en una](#) de las guías del AWS Identity and Access Management usuario.

Se AWS recomienda utilizar puntos finales regionales siempre que sea posible y configurar los suyos [Región de AWS](#). Los clientes de [particiones](#) que no sean comerciales deben usar puntos de conexión regionales. No todas SDKs las herramientas de Internet admiten esta configuración, pero todas tienen un comportamiento definido en cuanto a los puntos finales globales y regionales. Consulte la siguiente sección para obtener más información.

En el SDKs caso de las herramientas compatibles con esta configuración, los clientes pueden configurar la funcionalidad mediante lo siguiente:

**sts\_regional\_endpoints**- configuración de AWS **config** archivos compartidos,  
**AWS\_STS\_REGIONAL\_ENDPOINTS**: variable de entorno

Esta configuración especifica cómo la herramienta SDK o determina el Servicio de AWS punto final que utiliza para comunicarse con el AWS Security Token Service (AWS STS).

Valor predeterminado: legacy

**Note**

Todas las nuevas versiones SDK principales que se publiquen después de julio de 2022 se establecerán de forma predeterminada `regional`. Es posible que las nuevas versiones SDK principales eliminen esta configuración y este `regional` comportamiento de uso. Para reducir el impacto futuro de este cambio, le recomendamos que comience a usar `regional` en su aplicación siempre que sea posible.

Valores válidos: (Valor recomendado: `regional`)

- **legacy**— Utiliza el AWS STS punto final global, `sts.amazonaws.com`.
- **regional**— La herramienta SDK o siempre usa el AWS STS punto final de la región configurada actualmente. Por ejemplo, si el cliente está configurado para usar `us-west-2`, todas las llamadas AWS STS se realizan al punto final `sts.us-west-2.amazonaws.com`, en lugar de al `sts.amazonaws.com` punto final global. Para enviar una solicitud al punto de enlace global mientras esta configuración está habilitada, puede establecer la región en `aws-global`.

Ejemplo de configuración de este valor en el archivo `config`:

```
[default]
sts_regional_endpoints = regional
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_STS_REGIONAL_ENDPOINTS=regional
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_STS_REGIONAL_ENDPOINTS regional
```

## Compatibilidad con AWS SDKs

### Note

Se AWS recomienda utilizar puntos de conexión regionales siempre que sea posible y configurar sus [Región de AWS](#).

En la siguiente tabla se resume lo siguiente, para su herramienta SDK:

- Admite la configuración: si se admiten la variable de `config` archivo compartido y la variable de entorno para los puntos finales STS regionales.
- Valor de configuración predeterminado: el valor predeterminado de la configuración si es compatible.
- STS Punto final de destino del cliente de servicio predeterminado: qué punto final predeterminado utiliza el cliente, incluso si la configuración para cambiarlo no está disponible.
- Comportamiento alternativo del cliente de servicio: qué SDK hace cuando se supone que debe utilizar un punto final regional pero no se ha configurado ninguna región. Este es el comportamiento independientemente de si utiliza un punto final regional debido a un valor predeterminado o porque lo `regional` ha seleccionado la configuración.

La tabla también utiliza los siguientes valores:

- Punto final global: `https://sts.amazonaws.com`.
- Punto final regional: según la configuración [Región de AWS](#) utilizada por su aplicación.
- **us-east-1**(Regional): utiliza el punto final de la `us-east-1` región, pero con identificadores de sesión más largos que las solicitudes globales habituales.

SDK	Valor de configuración predeterminado	STSEndpoint de destino del cliente de servicio predeterminado	Comportamiento alternativo del cliente de servicio	Notas o más información
<a href="#">AWS CLI v2</a>	N N/A	Punto de conexión regional	Punto final global	
<a href="#">AWS CLI v1</a>	S legacy	Punto final global	Punto final global	
<a href="#">SDK para C++</a>	N N/A	Punto de conexión regional	us-east-1 (Regional)	
<a href="#">SDK para Go V2 (1.x)</a>	N N/A	Punto de conexión regional	Error en la solicitud	
<a href="#">SDK para Go 1.x (V1)</a>	S legacy	Punto final global	Punto final global	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	N N/A	Punto de conexión regional	Error en la solicitud	Si no hay ninguna región configurada, AssumeRole y AssumeRoleWithWebIdentity utilizará el STS punto final global
<a href="#">SDK para Java 1.x</a>	S legacy	Punto final global	Punto final global	

SDK	Valor de configuración predeterminado	STSEndpoint de destino del cliente de servicio predeterminado	Comportamiento alternativo del cliente de servicio	Notas o más información
<a href="#">SDK para JavaScript 3.x</a>	N	N/A	Punto de conexión regional	Error en la solicitud
<a href="#">SDK para JavaScript 2.x</a>	S	legacy	Punto final global	Punto final global
<a href="#">SDK para Kotlin</a>	N	N/A	Punto de conexión regional	Punto final global
<a href="#">SDK para .NET 3.x</a>	S	legacy	Punto final global	Punto final global
<a href="#">SDK para PHP 3.x</a>	S	legacy	Punto final global	Error en la solicitud
<a href="#">SDK para Python (Boto3)</a>	S	legacy	Punto final global	Punto final global
<a href="#">SDK para Ruby 3.x</a>	S	regional	Punto de conexión regional	Error en la solicitud
<a href="#">SDK para Rust</a>	N	N/A	Punto de conexión regional	Error en la solicitud

SDK	Valor de configuración predeterminado	STSEndpoint de destino del cliente de servicio predeterminado	Comportamiento alternativo del cliente de servicio	Notas o más información
<a href="#">SDK para Swift</a>	N/A	Punto de conexión regional	Error en la solicitud	
<a href="#">Herramientas para PowerShell</a>	Legacy	Punto final global	Punto final global	

## Pila doble y puntos finales FIPS

Configure esta funcionalidad mediante lo siguiente:

**use\_dualstack\_endpoint**- compartido AWS **config** configuración de archivos, **AWS\_USE\_DUALSTACK\_ENDPOINT**: variable de entorno, **aws.useDualstackEndpoint**- propiedad JVM del sistema: solo Java/Kotlin

Activa o desactiva si SDK enviará las solicitudes a puntos finales de doble pila. Para obtener más información sobre los puntos de enlace de doble pila, que admiten tanto como IPv4 el IPv6 tráfico, consulte [Uso de los puntos de enlace de doble pila de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service](#). Los puntos de conexión de doble pila están disponibles para algunos servicios en algunas regiones.

Valor predeterminado: `false`

Valores válidos:

- **true**— La herramienta SDK o herramienta intentará utilizar puntos de enlace de doble pila para realizar solicitudes de red. Si no existe un punto final de doble pila para el servicio y/o Región de AWS, la solicitud fallará.
- **false**— La herramienta SDK or no utilizará puntos de conexión de doble pila para realizar solicitudes de red.

**use\_fips\_endpoint**- compartido AWS **config** configuración de archivos,

**AWS\_USE\_FIPS\_ENDPOINT**: variable de entorno, **aws.useFipsEndpoint**- propiedad JVM del sistema: solo Java/Kotlin

Activa o desactiva si la herramienta SDK o herramienta enviará solicitudes a FIPS puntos finales compatibles. Los estándares federales de procesamiento de información (FIPS) son un conjunto de requisitos de seguridad del Gobierno de EE. UU. para los datos y su cifrado. Las agencias gubernamentales, los socios y quienes deseen hacer negocios con el gobierno federal deben cumplir con FIPS las pautas. A diferencia del estándar AWS Los puntos finales utilizan una biblioteca de TLS software que cumple con FIPS la norma 140-2. FIPS Si esta configuración está habilitada y no existe un FIPS punto final para el servicio en su Región de AWS, el AWS la llamada puede fallar. [Puntos de conexión específicos del servicio](#) y la `--endpoint-url` opción para el AWS Command Line Interface anular esta configuración.

Para obtener más información sobre otras formas de especificar puntos FIPS finales, consulte Región de AWS, consulte [FIPS Puntos finales por servicio](#). Para obtener más información sobre los puntos de enlace del servicio Amazon Elastic Compute Cloud, consulte los puntos de enlace de [doble pila \(IPv4|IPv6\)](#) en Amazon Reference. EC2 API

Valor predeterminado: `false`

Valores válidos:

- **true**— La herramienta SDK o herramienta enviará las solicitudes a los puntos de enlace que cumplan con los requisitos FIPS.
- **false**— La herramienta SDK o herramienta no enviará solicitudes a puntos finales que cumplan con los requisitos FIPS.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Comparte o más información
<a href="#">AWS CLI v2</a>	Sí

SDK	C	Notas o más información
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Detección de puntos de conexión

SDKs utilice la detección de puntos finales para acceder a los puntos finales del servicio (URLs para acceder a varios recursos) y, al mismo tiempo, mantener la flexibilidad para AWS para modificarlos

URLs según sea necesario. De esta forma, el código puede detectar automáticamente nuevos puntos de conexión. No hay puntos de conexión fijos para algunos servicios. En su lugar, para obtener los puntos de conexión disponibles durante el tiempo de ejecución, debe realizar una solicitud para obtener primero los puntos de conexión. Tras recuperar los puntos de conexión disponibles, el código utiliza los puntos de conexión para acceder a otras operaciones. Por ejemplo, en Amazon Timestream, realiza `DescribeEndpoints` una solicitud para recuperar SDK los puntos de enlace disponibles y, a continuación, los utiliza para completar operaciones específicas, como `o. CreateDatabase CreateTable`

Configure esta funcionalidad mediante lo siguiente:

**endpoint\_discovery\_enabled**- compartido AWS **config** configuración de archivos, **AWS\_ENABLE\_ENDPOINT\_DISCOVERY**: variable de entorno, **aws.endpointDiscoveryEnabled**- propiedad JVM del sistema: solo Java/Kotlin, Para configurar el valor directamente en el código, consulte su especificación directamente. SDK

Activa o desactiva la detección de puntos finales para DynamoDB.

La detección de puntos de conexión es obligatoria en Timestream y opcional en Amazon DynamoDB. Esta configuración se establece de forma predeterminada en uno `true` o en `false` función de si el servicio requiere la detección de puntos finales. Las solicitudes Timestream se establecen de forma predeterminada y las solicitudes de Amazon DynamoDB se establecen de forma predeterminada en. `true false`

Valores válidos:

- **true**— SDK Debería intentar descubrir automáticamente un punto final para los servicios en los que la detección de puntos finales sea opcional.
- **false**— No SDK deberían intentar detectar automáticamente un punto final en el caso de servicios en los que la detección de puntos finales sea opcional.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Completamente	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	Sí	Para usar la configuración de archivos compartidos config, debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	Sí	SDK para Java 2.x utiliza el nombre de <code>AWS_ENDPOINT_DISCOVERY_ENABLED</code> la variable de entorno.
<a href="#">SDK para Java 1.x</a>	Parcialmente	JVM propiedad del sistema no compatible.
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Parcialmente	Compatible solo con Timestream.
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Ajustes de configuración general

SDKs admiten algunos ajustes generales que configuran SDK los comportamientos generales.

Configure esta funcionalidad mediante lo siguiente:

**api\_versions**- compartido AWS **config** configuración de archivos

Alguno AWS los servicios mantienen varias API versiones para admitir la compatibilidad con versiones anteriores. De forma predeterminada, SDK y AWS CLI las operaciones utilizan la última API versión disponible. Si desea solicitar una API versión específica para utilizarla en sus solicitudes, incluya la `api_versions` configuración en su perfil.

Valor predeterminado: ninguno. (La última API versión la utiliza el SDK.)

Valores válidos: se trata de una configuración anidada seguida de una o más líneas sangradas, cada una de las cuales identifica una AWS el servicio y la API versión que se va a utilizar. Consulte la documentación del AWS servicio para saber qué API versiones están disponibles.

El ejemplo establece una API versión específica para dos AWS servicios del `config` archivo. Estas API versiones se utilizan únicamente para los comandos que se ejecutan en el perfil que contiene esta configuración. Los comandos de cualquier otro servicio utilizan la versión más reciente de ese servicio API.

```
api_versions =  
  ec2 = 2015-03-01  
  cloudfront = 2015-09-017
```

**ca\_bundle**- compartido AWS **config** configuración de archivos, **AWS\_CA\_BUNDLE**: variable de entorno

Especifica la ruta a un paquete de certificados personalizado (un archivo con una `.pem` extensión) que se utilizará al establecer TLS las conexiones SSL/.

Valor predeterminado: ninguno

Valores válidos: especifique la ruta completa o el nombre del archivo base. Si hay un nombre de archivo base, el sistema intentará encontrar el programa en las carpetas especificadas por la variable del entorno `PATH`.

Ejemplo de configuración de este valor en el archivo `config`:

```
[default]
ca_bundle = dev/apps/ca-certs/cabundle-2019mar05.pem
```

Debido a las diferencias en la forma en que los sistemas operativos gestionan las rutas y el escape de los caracteres de las rutas, a continuación se muestra un ejemplo de cómo configurar este valor en el config archivo en Windows:

```
[default]
ca_bundle = C:\\Users\\username\\.aws\\aws-custom-bundle.pem
```

Ejemplo de configuración de variables de entorno en Linux/macOS mediante la línea de comandos:

```
export AWS_CA_BUNDLE=/dev/apps/ca-certs/cabundle-2019mar05.pem
```

Ejemplo de configuración de variables de entorno en Windows mediante la línea de comandos:

```
setx AWS_CA_BUNDLE C:\dev\apps\ca-certs\cabundle-2019mar05.pem
```

## **output-** compartido AWS **config** configuración de archivos

Especifica el formato de los resultados en el AWS CLI y otros AWS SDKs y herramientas.

Valor predeterminado: json

Valores válidos:

- **json**— La salida tiene el formato de una [JSON](#) cadena.
- **yaml**— La salida tiene el formato de una [YAML](#) cadena.
- **yaml-stream**— La salida se transmite y se formatea como una cadena. [YAML](#) El streaming permite un manejo más rápido de tipos de datos de gran tamaño.
- **text**: la salida tiene el formato de varias líneas de valores de cadena separados por tabuladores. Esto puede ser útil para pasar la salida a un procesador de texto, como `grep`, `sed` o `awk`.
- **table**: el resultado tiene el formato de una tabla en la que se usan los caracteres `+|-` para los bordes de celda. Normalmente, la información se presenta en un formato que es más fácil de leer que los demás formatos, pero que no es útil para programar.

**parameter\_validation**- compartido AWS **config** configuración de archivos

Especifica si la herramienta SDK o la herramienta intentarán validar los parámetros de la línea de comandos antes de enviarlos al AWS punto final del servicio.

Valor predeterminado: `true`

Valores válidos:

- **true**: el valor predeterminado. La herramienta SDK o realiza la validación de los parámetros de la línea de comandos por parte del cliente. Esto ayuda a la herramienta SDK o a confirmar que los parámetros son válidos y detecta algunos errores. La herramienta SDK o puede rechazar las solicitudes que no sean válidas antes de enviarlas al AWS punto final del servicio.
- **false**— La herramienta SDK o no valida los parámetros de la línea de comandos antes de enviarlos al AWS punto final del servicio. La AWS el punto final del servicio es responsable de validar todas las solicitudes y rechazar las que no sean válidas.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Compatibilidad	Notas o más información
<a href="#">AWS CLI v2</a>	Parcial	<code>api_versions</code> no admitidas.
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Parcial	Las <code>api_versions</code> y la <code>parameter_validation</code> no son compatibles.
<a href="#">SDK para Go 1.x (V1)</a>	Parcial	Las <code>api_versions</code> y la <code>parameter_validation</code> no son compatibles. Para usar la configuración de archivos compartidos <code>config</code> , debe activar la carga desde el archivo de configuración; consulte <a href="#">Sesiones</a> .
<a href="#">SDK para Java 2.x</a>	No	

SDK	Categoría	Notas o más información
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	No	
<a href="#">SDK para .NET 3.x</a>	No	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	No	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	No	

## IMDS cliente

El SDK simplemente es un cliente de Instance Metadata Service versión 2 (IMDSv2) mediante solicitudes orientadas a la sesión. Para obtener más información sobre IMDSv2, consulte [Uso de IMDSv2](#) en la Guía del usuario de Amazon EC2. El cliente de IMDS se puede configurar mediante un objeto de configuración de cliente disponible en la base de código de SDK.

Configure esta funcionalidad mediante lo siguiente:

**retries**: miembro del objeto de configuración del cliente

El número de reintentos adicionales de cualquier solicitud fallida.

Valor predeterminado: 3

Valores válidos: un número mayor que 0.

**port**: miembro del objeto de configuración del cliente

El puerto del punto de conexión.

Valor predeterminado: 80

Valores válidos: un número.

**token\_ttl**: miembro del objeto de configuración del cliente

El TTL del token.

Valor predeterminado: 21.600 segundos (6 horas, el tiempo máximo asignado).

Valores válidos: un número.

**endpoint**: miembro del objeto de configuración del cliente

El punto final de IMDS.

Valor predeterminado: si el `endpoint_mode` es igual a IPv4, el punto de conexión predeterminado es `http://169.254.169.254`. Valor predeterminado: si el `endpoint_mode` es igual a IPv6, el punto de conexión predeterminado es `http://[fd00:ec2::254]`.

Valores válidos: válidos URI.

La mayoría admite las siguientes opciones SDKs. Consulte su base de SDK código específica para obtener más información.

**endpoint\_mode**: miembro del objeto de configuración del cliente

El modo de punto final de IMDS.

Valor predeterminado: IPv4

Valores válidos: IPv4, IPv6

**http\_open\_timeout**: miembro del objeto de configuración del cliente (puede variar el nombre)

La cantidad de segundos que se va a esperar para que se abra la conexión.

Valor predeterminado: 1 segundo.

Valores válidos: un número mayor que 0.

**http\_read\_timeout**: miembro del objeto de configuración del cliente (puede variar el nombre)

El número de segundos que tarda en leerse un fragmento de datos.

Valor predeterminado: 1 segundo.

Valores válidos: un número mayor que 0.

**http\_debug\_output**: miembro del objeto de configuración del cliente (puede variar el nombre)

Establece un flujo de salida para la depuración.

Valor predeterminado: ninguno.

Valores válidos: un flujo de E/S válido, por ejemplo. STDOUT

**backoff**: miembro del objeto de configuración del cliente (puede variar el nombre)

El número de segundos que permanecen inactivos entre los reintentos o la función de espera proporcionada por el cliente para llamar. Esto reemplaza la estrategia de retroceso exponencial predeterminada.

Valor predeterminado: varía según SDK.

Valores válidos: varían según SDK. Puede ser un valor numérico o una llamada a una función personalizada.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Todas las configuraciones de propiedades del JVM sistema son compatibles con AWS SDK for Java y AWS SDK para Kotlin únicamente.

SDK	Ci e	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	No	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	

SDK	Comportamiento	Notas o más información
<a href="#">SDK para Go 1.x (V1)</a>	Sí	
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Sí	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	Sí	
<a href="#">SDK para Kotlin</a>	No	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Comportamiento de los reintentos

El comportamiento de SDKs reintento incluye la configuración relativa a la forma en que se intenta recuperarse de los errores resultantes de las solicitudes realizadas a Servicios de AWS.

Configure esta funcionalidad mediante lo siguiente:

**retry\_mode**- compartido AWS **config** configuración de archivos, **AWS\_RETRY\_MODE**: variable de entorno, **aws.retryMode**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica el modo en que la herramienta para desarrolladores SDK intenta volver a intentarlo.

Valor predeterminado: este valor es específico de su SDK. Consulte su SDK guía específica o su base SDK de código para ver si está predeterminado `retry_mode`.

Valores válidos:

- `standard`— (Recomendado) El conjunto recomendado de reglas de reintento para todos AWS SDKs. Este modo incluye un conjunto estándar de errores que se repiten y ajusta automáticamente el número de reintentos para maximizar la disponibilidad y la estabilidad. Este modo es seguro para su uso en aplicaciones multiusuario. El número máximo predeterminado de intentos con este modo es tres, a menos que los `max_attempts` se configuren de forma explícita.
- `adaptive`— Un modo de reintento, adecuado solo para casos de uso especializados, que incluye la funcionalidad del modo estándar, así como una limitación automática de la velocidad por parte del cliente. Este modo de reintento no se recomienda para aplicaciones con varios usuarios, a menos que se procure aislar a los inquilinos de las aplicaciones. Para obtener más información, consulte [Elegir entre los modos `standard` y `adaptive` volver a intentarlo](#). Este modo es experimental y podría cambiar su comportamiento en el futuro.
- `legacy`— (No recomendado) Específico para SDK ti (consulte su SDK guía específica o su SDK código base).

**max\_attempts**- compartido AWS **config** configuración de archivos, **AWS\_MAX\_ATTEMPTS**: variable de entorno, **aws.maxAttempts**- propiedad JVM del sistema: solo en Java/Kotlin

Especifica el número máximo de intentos que se pueden realizar en una solicitud.

Valor predeterminado: si no se especifica este valor, su valor predeterminado depende del valor de la configuración `retry_mode`:

- Si `retry_mode` lo está `legacy`: usa un valor predeterminado específico para usted SDK (consulte su SDK guía específica o su base SDK de código para `max_attempts` ver el valor predeterminado).
- Si el `retry_mode` es `standard`: realiza tres intentos.
- Si el `retry_mode` es `adaptive`: realiza tres intentos.

Valores válidos: un número mayor que 0.

## Elegir entre los modos **standard** y **adaptive** volver a intentarlo

Le recomendamos que utilice el modo de `standard` reintento a menos que esté seguro de que su uso es el más adecuado. `adaptive`

**Note**

El `adaptive` modo presupone que se agrupan los clientes en función del ámbito en el que el servicio de backend puede limitar las solicitudes. Si no lo haces, la limitación de un recurso podría retrasar las solicitudes de un recurso no relacionado si utilizas el mismo cliente para ambos recursos.

Estándar	Adaptativo
Casos de uso de aplicaciones: todos.	Casos de uso de aplicaciones: <ol style="list-style-type: none"> <li>1. No es sensible a la latencia.</li> <li>2. El cliente solo accede a un único recurso, o bien, usted proporciona una lógica para agrupar a sus clientes por separado según el recurso de servicio al que se accede.</li> </ol>
Admite la interrupción de circuitos para evitar que se vuelvan a intentar durante SDK las interrupciones.	Admite la interrupción del circuito para evitar que se vuelva a intentar durante las interrupciones. SDK
Utiliza un retroceso exponencial fluctuante en caso de averías.	Utiliza tiempos de espera dinámicos para intentar minimizar el número de solicitudes fallidas, a cambio de la posibilidad de aumentar la latencia.
Nunca retrasa el primer intento de solicitud, solo los reintentos.	Puede acelerar o retrasar el intento de solicitud inicial.

Si opta por utilizar `adaptive` el modo, la aplicación debe crear clientes diseñados en función de cada recurso que pueda estar limitado. Un recurso, en este caso, está más ajustado que solo pensar en cada uno Servicio de AWS. Servicios de AWS pueden tener dimensiones adicionales que utilizan para limitar las solicitudes. Usemos el servicio Amazon DynamoDB como ejemplo. DynamoDB utiliza Región de AWS además de la tabla a la que se accede para acelerar las solicitudes. Esto significa que una tabla a la que está accediendo tu código podría estar más restringida que otras. Si el código utilizaba el mismo cliente para acceder a todas las tablas y las solicitudes a una de esas tablas están

restringidas, el modo de reintento adaptativo reducirá la tasa de solicitudes de todas las tablas. Su código debe diseñarse para tener un cliente por región y tabla. Si experimentas una latencia inesperada al usar el modo adaptivo, consulta la sección específica de la guía de documentación del servicio que está utilizando.

## Detalles de implementación del modo de reintento

La AWS SDKs utilice [cubos de fichas](#) para decidir si se debe volver a intentar una solicitud y (en el caso del modo de reintento adaptativo) con qué rapidez se deben enviar las solicitudes. El grupo utiliza dos grupos de fichas SDK: un grupo de fichas de reintentos y un grupo de fichas de tasa de solicitudes.

- El depósito de reintentos se utiliza para determinar si se SDK deben deshabilitar temporalmente los reintentos a fin de proteger los servicios ascendentes y descendentes durante las interrupciones. Los tokens se obtienen del depósito antes de que se intenten reintentarlo y, cuando las solicitudes se realizan correctamente, se devuelven al depósito. Si el depósito está vacío cuando se intenta reintentar, no SDK volverá a intentar la solicitud.
- El depósito de fichas de tasa de solicitudes solo se usa en el modo de reintento adaptativo para determinar la velocidad a la que se envían las solicitudes. Los tokens se adquieren del depósito antes de que se envíe la solicitud y se devuelven al depósito a un ritmo determinado dinámicamente en función de la limitación de las respuestas devueltas por el servicio.

A continuación se muestra el pseudocódigo de alto nivel para ambos modos de reintento `standard` y `adaptive`:

```
MakeSDKRequest() {
  attempts = 0
  loop {
    GetSendToken()
    response = SendHTTPRequest()
    RequestBookkeeping(response)
    if not Retryable(response)
      return response
    attempts += 1
    if attempts >= MAX_ATTEMPTS:
      return response
    if not HasRetryQuota(response)
      return response
    delay = ExponentialBackoff(attempts)
    sleep(delay)
  }
}
```

```
}  
}
```

A continuación se muestran más detalles sobre los componentes utilizados en el pseudocódigo:

### **GetSendToken:**

Este paso solo se utiliza en el modo de reintento. `adaptive` Este paso adquiere un token del grupo de tokens de tasa de solicitud. Si un token no está disponible, esperará a que esté disponible.

SDKEs posible que tengas opciones de configuración disponibles para rechazar la solicitud en lugar de esperar. Los tokens del depósito se rellenan a un ritmo que se determina de forma dinámica, en función del número de respuestas restrictivas que reciba el cliente.

### **SendHttpRequest:**

En este paso, se envía la solicitud a AWS. La mayoría AWS SDKs utilizan una HTTP biblioteca que utilice grupos de conexiones para reutilizar una conexión existente al realizar una HTTP solicitud. Por lo general, las conexiones se reutilizan si una solicitud falla debido a errores de limitación, pero no si la solicitud falla debido a un error transitorio.

### **RequestBookkeeping:**

Los tokens se añaden al depósito de fichas si la solicitud se realiza correctamente. Solo en el modo de `adaptive` reintento, la tasa de llenado del depósito de fichas de tasa de solicitudes se actualiza en función del tipo de respuesta recibida.

### **Retryable:**

Este paso determina si se puede volver a intentar una respuesta en función de lo siguiente:

- El código HTTP de estado.
- El código de error devuelto por el servicio.
- Los errores de conexión, definidos como cualquier error recibido por SDK el que no se recibe una HTTP respuesta del servicio.

Los errores transitorios (códigos de HTTP estado 400, 408, 500, 502, 503 y 504) y los errores de regulación (códigos de HTTP estado 400, 403, 429, 502, 503 y 509) pueden volver a intentarse. SDKEl comportamiento de los reintentos se determina en combinación con los códigos de error u otros datos del servicio.

**MAX\_ATTEMPTS:**

El número máximo de intentos predeterminado lo establece la `retry_mode` configuración, a menos que la configuración lo anule. `max_attempts`

**HasRetryQuota**

En este paso, se obtiene un token del grupo de reintentos. Si el depósito de fichas de reintento está vacío, no se volverá a intentar la solicitud.

**ExponentialBackoff**

En el caso de un error que se pueda volver a intentar, el retraso del reintento se calcula mediante un retroceso exponencial truncado. El SDKs uso de un retardo exponencial binario truncado con fluctuación de fase. El siguiente algoritmo muestra cómo se define la cantidad de tiempo de reposo, en segundos, para una respuesta a una solicitud *i*:

```
seconds_to_sleep_i = min(b*r^i, MAX_BACKOFF)
```

En el algoritmo anterior, se aplican los siguientes valores:

`b` = random number within the range of:  $0 \leq b \leq 1$

`r` = 2

`MAX_BACKOFF` = 20 seconds SDKs para la mayoría. Consulta tu SDK guía específica o tu código fuente para confirmarlo.

**Compatibilidad con AWS SDKs**

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Ci e	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	

SDK	Comportamiento de los reintentos	Notas o más información
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	Sí	JVM propiedades del sistema: usar <code>com.amazonaws.sdk.maxAttempts</code> en lugar de <code>deaws.maxAttempts</code> ; usar <code>com.amazonaws.sdk.retryMode</code> en lugar de <code>deaws.retryMode</code> .
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	No	Admite un número máximo de reintentos, el retroceso exponencial con fluctuación de fase y la opción de un método personalizado para el retraso de los reintentos.
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	Sí	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Compresión de solicitudes

### Note

Para obtener ayuda para comprender el diseño de las páginas de configuración o para interpretar la compatibilidad con AWS SDKs en la siguiente tabla, consulte [Páginas de configuración](#).

AWS SDKs y las herramientas pueden comprimir automáticamente las cargas útiles al enviar solicitudes a Servicios de AWS que admiten la recepción de cargas útiles comprimidas. Comprimir la carga útil en el cliente antes de enviarla a un servicio puede reducir el número total de solicitudes y el ancho de banda necesario para enviar datos al servicio, así como reducir las solicitudes que se realizan incorrectamente debido a las limitaciones del servicio en cuanto al tamaño de la carga útil. Para la compresión, la herramienta SDK o selecciona un algoritmo de codificación compatible tanto con el servicio como con el SDK. Sin embargo, la lista actual de codificaciones posibles solo incluye gzip, pero es posible que se amplíe en el futuro.

La compresión de solicitudes puede resultar especialmente útil si tu aplicación utiliza [Amazon CloudWatch](#). CloudWatch es un servicio de monitoreo y observabilidad que recopila datos operativos y de monitoreo en forma de registros, métricas y eventos. Un ejemplo de una operación de servicio que admite la compresión CloudWatch es el [PutMetricDataAPI](#) método.

Configure esta funcionalidad mediante lo siguiente:

**disable\_request\_compression**- compartido AWS **config** configuración de archivos, **AWS\_DISABLE\_REQUEST\_COMPRESSION**: variable de entorno, **aws.disableRequestCompression**- propiedad JVM del sistema: solo Java/Kotlin

Activa o desactiva si la herramienta SDK o comprimirá una carga útil antes de enviar una solicitud.

Valor predeterminado: `false`

Valores válidos:

- **true**: desactive la compresión de solicitudes.
- **false**: utilice la compresión de solicitudes siempre que sea posible.

**request\_min\_compression\_size\_bytes**- compartido AWS **config** configuración de archivos, **AWS\_REQUEST\_MIN\_COMPRESSION\_SIZE\_BYTES**: variable de entorno, **aws.requestMinCompressionSizeBytes**- propiedad JVM del sistema: solo Java/Kotlin

Establece el tamaño mínimo en bytes del cuerpo de la solicitud que la herramienta SDK o debe comprimir. Las cargas útiles pequeñas pueden aumentar de longitud al comprimirse, por lo que existe un límite inferior para realizar la compresión. Este valor está incluido, un tamaño de solicitud mayor o igual al valor se comprimirá.

Valor predeterminado: 10 240 bytes

Valores válidos: valor entero comprendido entre 0 y 10 485 760 bytes, ambos incluidos.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Compatible	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	Sí	
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	Sí	

SDK	Comparte	Notas o más información
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	Sí	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Puntos de conexión específicos del servicio

La configuración del punto final específico del servicio ofrece la opción de utilizar el punto final que elija para API las solicitudes y mantener esa opción. Esta configuración proporciona la flexibilidad necesaria para admitir puntos de conexión locales, puntos de conexión y puntos de conexión VPC locales de terceros AWS entornos de desarrollo. Se pueden usar diferentes puntos de conexión para los entornos de prueba y producción. Puede especificar un punto final URL para cada usuario Servicios de AWS.

Configure esta funcionalidad mediante lo siguiente:

**endpoint\_url**- compartido AWS **config** configuración de archivos, **AWS\_ENDPOINT\_URL**: variable de entorno, **aws.endpointUrl**- propiedad JVM del sistema: solo en Java/Kotlin

Cuando se especifica directamente en un perfil o como variable de entorno, esta configuración especifica el punto de conexión que se utiliza para todas las solicitudes de servicio. Este punto final es anulado por cualquier punto de conexión específico del servicio configurado.

También puedes usar esta configuración dentro de una `services` sección de un espacio compartido AWS `config` archivo para configurar un punto final personalizado para un servicio específico. Para obtener una lista de todas las claves de identificación de servicio que se van

a utilizar para las subsecciones en la sección `services`, consulte [Identificadores de punto de conexión específicos del servicio](#).

Valor predeterminado: `none`

Valores válidos: AURL, incluidos el esquema y el host del punto final. Opcionalmente, URL puede contener un componente de ruta que contenga uno o más segmentos de ruta.

**AWS\_ENDPOINT\_URL\_<SERVICE>**: variable de entorno, **`aws.endpointUrl<ServiceName>`**- propiedad JVM del sistema: solo en Java/Kotlin

**AWS\_ENDPOINT\_URL\_<SERVICE>**, ¿dónde está el <SERVICE> Servicio de AWS identificador, establece un punto final personalizado para un servicio específico. Para obtener una lista de todas las variables de entorno específicas del servicio, consulte [Identificadores de punto de conexión específicos del servicio](#).

Este punto de conexión específico del servicio anula cualquier punto de conexión global establecido en **AWS\_ENDPOINT\_URL**.

Valor predeterminado: `none`

Valores válidos: AURL, incluidos el esquema y el host del punto final. Opcionalmente, URL puede contener un componente de ruta que contenga uno o más segmentos de ruta.

**ignore\_configured\_endpoint\_urls**- compartido AWS **config** configuración de archivos, **AWS\_IGNORE\_CONFIGURED\_ENDPOINT\_URLS**: variable de entorno, **`aws.ignoreConfiguredEndpointUrls`**- propiedad JVM del sistema: solo en Java/Kotlin

Esta configuración se utiliza para ignorar todas las configuraciones de puntos de conexión personalizadas.

Tenga en cuenta que cualquier punto de conexión explícito establecido en el código o en el propio cliente de servicio se utiliza independientemente de esta configuración. Por ejemplo, incluir el parámetro de línea de `--endpoint-url` comandos con un AWS CLI El comando o el paso de un punto final URL a un constructor de clientes siempre surtirán efecto.

Valor predeterminado: `false`

Valores válidos:

- **true**— La herramienta SDK o no lee ninguna opción de configuración personalizada del `config` archivo compartido ni de las variables de entorno para configurar un punto final URL.

- **false**— La herramienta SDK o utiliza todos los puntos finales disponibles proporcionados por el usuario del `config` archivo compartido o de las variables de entorno.

## Configuración de puntos de conexión mediante variables de entorno

Para dirigir las solicitudes de todos los servicios a un punto final personalizado URL, defina la variable de entorno `AWS_ENDPOINT_URL` global.

```
export AWS_ENDPOINT_URL=http://localhost:4567
```

Para enrutar las solicitudes de un determinado Servicio de AWS a un punto final personalizado URL, utilice la variable de `AWS_ENDPOINT_URL_<SERVICE>` entorno. Amazon DynamoDB tiene un `serviceId` de [DynamoDB](#). Para este servicio, la variable de URL entorno del punto final es `AWS_ENDPOINT_URL_DYNAMODB`. Este punto de conexión tiene prioridad sobre el punto de conexión global establecido en `AWS_ENDPOINT_URL` para este servicio.

```
export AWS_ENDPOINT_URL_DYNAMODB=http://localhost:5678
```

Como otro ejemplo, AWS Elastic Beanstalk tiene un `serviceId` de [Elastic Beanstalk](#). La Servicio de AWS el identificador se basa en el API modelo sustituyendo todos los espacios `serviceId` por guiones bajos y mayúsculas en todas las letras. Para este servicio, la variable de entorno de la URL del punto de conexión es `AWS_ENDPOINT_URL_ELASTIC_BEANSTALK`. Para obtener una lista de todas las variables de entorno específicas del servicio, consulte [Identificadores de punto de conexión específicos del servicio](#).

```
export AWS_ENDPOINT_URL_ELASTIC_BEANSTALK=http://localhost:5567
```

## Configure los puntos de conexión mediante el archivo compartido **config**

En el archivo compartido `config`, `endpoint_url` se usa en diferentes lugares para diferentes funciones.

- Si se especifica `endpoint_url` directamente en un `profile`, ese punto de conexión se convierte en el punto de conexión global.
- El `endpoint_url` anidado bajo una clave identificadora de servicio en una sección `services`, hace que ese punto de conexión se aplique únicamente a las solicitudes realizadas a ese servicio.

Para obtener más información sobre cómo definir una sección de `services` en el archivo compartido `config`, consulte [Formato del archivo de configuración](#).

En el siguiente ejemplo, se utiliza una `services` definición para configurar un punto de enlace específico del servicio URL que se utilizará para Amazon S3 y un punto de enlace global personalizado que se utilizará para todos los demás servicios:

```
[profile dev-s3-specific-and-global]
endpoint_url = http://localhost:1234
services = s3-specific

[services s3-specific]
s3 =
  endpoint_url = https://play.min.io:9000
```

Un único perfil puede configurar puntos de conexión para varios servicios. En este ejemplo se muestra cómo configurar el punto final específico del servicio URLs para Amazon S3 y AWS Elastic Beanstalk en el mismo perfil. AWS Elastic Beanstalk tiene un `serviceId` de [Elastic Beanstalk](#). La Servicio de AWS el identificador se basa en el API modelo sustituyendo todos los espacios `serviceId` por guiones bajos y minúsculas todas las letras. Por lo tanto, la clave identificadora del servicio pasa a ser `elastic_beanstalk` y la configuración de este servicio comienza en la línea `elastic_beanstalk =` . Para obtener una lista de todas las claves de identificación de servicio que se van a utilizar en la sección de `services`, consulte [Identificadores de punto de conexión específicos del servicio](#).

```
[services testing-s3-and-eb]
s3 =
  endpoint_url = http://localhost:4567
elastic_beanstalk =
  endpoint_url = http://localhost:8000

[profile dev]
services = testing-s3-and-eb
```

La sección de configuración de servicios se puede utilizar en varios perfiles. Por ejemplo, dos perfiles pueden usar la misma definición de `services` y, al mismo tiempo, modificar otras propiedades del perfil:

```
[services testing-s3]
```

```
s3 =
    endpoint_url = https://localhost:4567

[profile testing-json]
output = json
services = testing-s3

[profile testing-text]
output = text
services = testing-s3
```

## Configure los puntos de conexión de los perfiles mediante credenciales basadas en roles

Si su perfil tiene credenciales basadas en funciones configuradas mediante un `source_profile` parámetro para la funcionalidad de IAM asumir funciones, SDK solo utilizará configuraciones de servicio para el perfil especificado. No utiliza perfiles que estén vinculados a él por roles. Por ejemplo, mediante el siguiente archivo `config` compartido:

```
[profile A]
credential_source = Ec2InstanceMetadata
endpoint_url = https://profile-a-endpoint.aws/

[profile B]
source_profile = A
role_arn = arn:aws:iam::123456789012:role/roleB
services = profileB

[services profileB]
ec2 =
    endpoint_url = https://profile-b-ec2-endpoint.aws
```

Si utilizas el perfil B y haces una llamada en tu código a AmazonEC2, el punto final se resuelve como `https://profile-b-ec2-endpoint.aws`. Si el código realiza una solicitud a cualquier otro servicio, la resolución del punto de conexión no seguirá ninguna lógica personalizada. El punto de conexión no se convierte en el punto de conexión global definido en el perfil A. Para que un punto de conexión global surta efecto en el perfil B, tendrá que configurar `endpoint_url` directamente dentro del perfil B. Para obtener más información sobre la configuración de `source_profile`, consulte [Asumir el rol de proveedor de credenciales](#).

## Precedencia de configuración

La configuración de esta característica se puede usar al mismo tiempo, pero solo tendrá prioridad un valor por servicio. Para API llamadas realizadas a una persona determinada Servicio de AWS, se utiliza el siguiente orden para seleccionar un valor:

1. Cualquier ajuste explícito establecido en el código o en el propio cliente de un servicio tiene prioridad sobre cualquier otra cosa.
  - Para el registro AWS CLI, es el valor que proporciona el parámetro de la línea de `--endpoint-url` comandos. En el caso de una SDK, las asignaciones explícitas pueden adoptar la forma de un parámetro que se establece al crear una instancia Servicio de AWS cliente u objeto de configuración.
2. El valor proporcionado por una variable de entorno específica del servicio, como `AWS_ENDPOINT_URL_DYNAMODB`.
3. El valor proporcionado por la variable de entorno de punto de conexión `AWS_ENDPOINT_URL` global.
4. El valor que proporciona la configuración anidada `endpoint_url` bajo una clave de identificación de servicio dentro de una sección `services` del archivo compartido `config`.
5. El valor proporcionado por la configuración de `endpoint_url` en un `profile` de un archivo compartido `config`.
6. Cualquier punto final predeterminado URL para el respectivo Servicio de AWS se usa por última vez.

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	C	Notas o más información
<a href="#">AWS CLI v2</a>	Sí	
<a href="#">SDK para C++</a>	No	

SDK	Comparte	Notas o más información
<a href="#">SDK para Go V2 (1.x)</a>	Sí	
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	Sí	
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	Sí	
<a href="#">SDK para .NET 3.x</a>	Sí	
<a href="#">SDK para PHP 3.x</a>	Sí	
<a href="#">SDK para Python (Boto3)</a>	Sí	
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	No	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	

## Identificadores de punto de conexión específicos del servicio

Para obtener información sobre cómo y dónde usar los identificadores de la siguiente tabla, consulte [Puntos de conexión específicos del servicio](#).

<b>serviceId</b>	<b>Cl</b>	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b>	<b>variable de entorno</b>
	id		
	ac		
	de		
	se		
	pá		
	us		
	cc		
	o		
	A		
	c		
	fil		
AccessAnalyzer	ac	AWS_ENDPOINT_URL_ACCESSANALYZER	
Account	ac	AWS_ENDPOINT_URL_ACCOUNT	
ACM	ac	AWS_ENDPOINT_URL_ACM	
ACM PCA	ac	AWS_ENDPOINT_URL_ACM_PCA	
Alexa For Business	a	AWS_ENDPOINT_URL_ALEXA_FOR_BUSINESS	
	_l		
amp	ar	AWS_ENDPOINT_URL_AMP	
Amplify	ar	AWS_ENDPOINT_URL_AMPLIFY	
AmplifyBackend	ar	AWS_ENDPOINT_URL_AMPLIFYBACKEND	
	cl		
AmplifyUIBuilder	ar	AWS_ENDPOINT_URL_AMPLIFYUIBUILDER	
	bt		
API Gateway	ap	AWS_ENDPOINT_URL_API_GATEWAY	
	a)		

<b>serviceId</b>	Clave de configuración	Variable de entorno
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
ApiGatewayManagementApi	<code>AWS_ENDPOINT_URL_APIGATEWAYMANAGEMENTAPI</code>	
ApiGatewayV2	<code>AWS_ENDPOINT_URL_APIGATEWAYV2</code>	
AppConfig	<code>AWS_ENDPOINT_URL_APPCONFIG</code>	
AppConfigData	<code>AWS_ENDPOINT_URL_APPCONFIGDATA</code>	
AppFabric	<code>AWS_ENDPOINT_URL_APPFABRIC</code>	
Appflow	<code>AWS_ENDPOINT_URL_APPFLOW</code>	
AppIntegrations	<code>AWS_ENDPOINT_URL_APPINTEGRATIONS</code>	
Application Auto Scaling	<code>AWS_ENDPOINT_URL_APPLICATION_AUTO_SCALING</code>	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Application Insights	<code>AWS_ENDPOINT_URL_APPLICATION_INSIGHTS</code>	
ApplicationCostProfiler	<code>AWS_ENDPOINT_URL_APPLICATIONCOSTPROFILER</code>	
App Mesh	<code>AWS_ENDPOINT_URL_APP_MESH</code>	
AppRunner	<code>AWS_ENDPOINT_URL_APPRUNNER</code>	
AppStream	<code>AWS_ENDPOINT_URL_APPSTREAM</code>	
AppSync	<code>AWS_ENDPOINT_URL_APPS_SYNC</code>	
ARC Zonal Shift	<code>AWS_ENDPOINT_URL_ARC_ZONAL_SHIFT</code>	
Artifact	<code>AWS_ENDPOINT_URL_ARTIFACT</code>	
Athena	<code>AWS_ENDPOINT_URL_ATHENA</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
AuditManager	<code>AWS_ENDPOINT_URL_AUDITMANAGER</code>	
Auto Scaling	<code>AWS_ENDPOINT_URL_AUTO_SCALING</code>	
Auto Scaling Plans	<code>AWS_ENDPOINT_URL_AUTO_SCALING_PLANS</code>	
b2bi	<code>AWS_ENDPOINT_URL_B2BI</code>	
Backup	<code>AWS_ENDPOINT_URL_BACKUP</code>	
Backup Gateway	<code>AWS_ENDPOINT_URL_BACKUP_GATEWAY</code>	
BackupStorage	<code>AWS_ENDPOINT_URL_BACKUPSTORAGE</code>	
Batch	<code>AWS_ENDPOINT_URL_BATCH</code>	
BCM Data Exports	<code>AWS_ENDPOINT_URL_BCM_DATA_EXPORTS</code>	
Bedrock	<code>AWS_ENDPOINT_URL_BEDROCK</code>	



<b>serviceId</b>	<b>Cl</b>	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b>	<b>variable de entorno</b>
Chime SDK Identity	cl	AWS_ENDPOINT_URL_CHIME_SDK_IDENTITY	
Chime SDK Media Pipelines	cl	AWS_ENDPOINT_URL_CHIME_SDK_MEDIA_PIPELINES	
Chime SDK Meetings	cl	AWS_ENDPOINT_URL_CHIME_SDK_MEETINGS	
Chime SDK Messaging	cl	AWS_ENDPOINT_URL_CHIME_SDK_MESSAGING	
Chime SDK Voice	cl	AWS_ENDPOINT_URL_CHIME_SDK_VOICE	
CleanRooms	c:	AWS_ENDPOINT_URL_CLEANROOMS	
CleanRoomsML	c:	AWS_ENDPOINT_URL_CLEANROOMSML	

<b>serviceId</b>	<b>Cl</b> <b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
Cloud9	c: AWS_ENDPOINT_URL_CLOUD9
CloudControl	c: AWS_ENDPOINT_URL_CLOUDCONTROL r:
CloudDirectory	c: AWS_ENDPOINT_URL_CLOUDDIRECTORY c:
CloudFormation	c: AWS_ENDPOINT_URL_CLOUDFORMATION a:
CloudFront	c: AWS_ENDPOINT_URL_CLOUDFRONT t:
CloudFront Key Value Store	c: AWS_ENDPOINT_URL_CLOUDFRONT_KEYVALUESTORE t: e:
CloudHSM	c: AWS_ENDPOINT_URL_CLOUDHSM
CloudHSM V2	c: AWS_ENDPOINT_URL_CLOUDHSM_V2 v:
CloudSearch	c: AWS_ENDPOINT_URL_CLOUDSEARCH c:

<b>serviceId</b>	<b>Cl</b>	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b>	<b>variable de entorno</b>
CloudSearch Domain	cl	AWS_ENDPOINT_URL_CLOUDSEARCH_DOMAIN	
CloudTrail	cl	AWS_ENDPOINT_URL_CLOUDTRAIL	
CloudTrail Data	cl	AWS_ENDPOINT_URL_CLOUDTRAIL_DATA	
CloudWatch	cl	AWS_ENDPOINT_URL_CLOUDWATCH	
codeartifact	cl	AWS_ENDPOINT_URL_CODEARTIFACT	
CodeBuild	cl	AWS_ENDPOINT_URL_CODEBUILD	
CodeCatalyst	cl	AWS_ENDPOINT_URL_CODECATALYST	
CodeCommit	cl	AWS_ENDPOINT_URL_CODECOMMIT	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
CodeDeploy	<code>AWS_ENDPOINT_URL_CODEDEPLOY</code>	
CodeGuru Reviewer	<code>AWS_ENDPOINT_URL_CODEGURU_REVIEWER</code>	
CodeGuru Security	<code>AWS_ENDPOINT_URL_CODEGURU_SECURITY</code>	
CodeGuruProfiler	<code>AWS_ENDPOINT_URL_CODEGURUPROFILER</code>	
CodePipeline	<code>AWS_ENDPOINT_URL_CODEPIPELINE</code>	
CodeStar	<code>AWS_ENDPOINT_URL_CODESTAR</code>	
CodeStar connections	<code>AWS_ENDPOINT_URL_CODESTAR_CONNECTIONS</code>	
codestar notificaciones	<code>AWS_ENDPOINT_URL_CODESTAR_NOTIFICATIONS</code>	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Cognito Identity	<code>AWS_ENDPOINT_URL_COGNITO_IDENTITY</code>	
Cognito Identity Provider	<code>AWS_ENDPOINT_URL_COGNITO_IDENTITY_PROVIDER</code>	
Cognito Sync	<code>AWS_ENDPOINT_URL_COGNITO_SYNC</code>	
Comprehend	<code>AWS_ENDPOINT_URL_COMPREHEND</code>	
ComprehendMedical	<code>AWS_ENDPOINT_URL_COMPREHENDMEDICAL</code>	
Compute Optimizer	<code>AWS_ENDPOINT_URL_COMPUTE_OPTIMIZER</code>	
Config Service	<code>AWS_ENDPOINT_URL_CONFIG_SERVICE</code>	
Connect	<code>AWS_ENDPOINT_URL_CONNECT</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Connect Contact Lens	<code>AWS_ENDPOINT_URL_CONNECT_CONTACT_LENS</code>	
ConnectCampaigns	<code>AWS_ENDPOINT_URL_CONNECTCAMPAIGNS</code>	
ConnectCases	<code>AWS_ENDPOINT_URL_CONNECTCASES</code>	
ConnectParticipant	<code>AWS_ENDPOINT_URL_CONNECTPARTICIPANT</code>	
ControlTower	<code>AWS_ENDPOINT_URL_CONTROLTOWER</code>	
Cost Optimization Hub	<code>AWS_ENDPOINT_URL_COST_OPTIMIZATION_HUB</code>	
Cost and Usage Report Service	<code>AWS_ENDPOINT_URL_COST_AND_USAGE_REPO</code> <code>RT_SERVICE</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Customer Profiles	<code>AWS_ENDPOINT_URL_CUSTOMER_PROFILES</code>	
DataBrew	<code>AWS_ENDPOINT_URL_DATABREW</code>	
DataExchange	<code>AWS_ENDPOINT_URL_DATAEXCHANGE</code>	
Data Pipeline	<code>AWS_ENDPOINT_URL_DATA_PIPELINE</code>	
DataSync	<code>AWS_ENDPOINT_URL_DATASYNC</code>	
DataZone	<code>AWS_ENDPOINT_URL_DATAZONE</code>	
DAX	<code>AWS_ENDPOINT_URL_DAX</code>	
Detective	<code>AWS_ENDPOINT_URL_DETECTIVE</code>	
Device Farm	<code>AWS_ENDPOINT_URL_DEVICE_FARM</code>	
DevOps Guru	<code>AWS_ENDPOINT_URL_DEVOPS_GURU</code>	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Direct Connect	<code>AWS_ENDPOINT_URL_DIRECT_CONNECT</code>	
Application Discovery Service	<code>AWS_ENDPOINT_URL_APPLICATION_DISCOVERY_SERVICE</code>	
DLM	<code>AWS_ENDPOINT_URL_DLM</code>	
Database Migration Service	<code>AWS_ENDPOINT_URL_DATABASE_MIGRATION_SERVICE</code>	
DocDB	<code>AWS_ENDPOINT_URL_DOCDB</code>	
DocDB Elastic	<code>AWS_ENDPOINT_URL_DOCDB_ELASTIC</code>	
drs	<code>AWS_ENDPOINT_URL_DRS</code>	
Directory Service	<code>AWS_ENDPOINT_URL_DIRECTORY_SERVICE</code>	
DynamoDB	<code>AWS_ENDPOINT_URL_DYNAMODB</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
DynamoDB Streams	<code>AWS_ENDPOINT_URL_DYNAMODB_STREAMS</code>	
EBS	<code>AWS_ENDPOINT_URL_EBS</code>	
EC2	<code>AWS_ENDPOINT_URL_EC2</code>	
EC2 Instance Connect	<code>AWS_ENDPOINT_URL_EC2_INSTANCE_CONNECT</code>	
ECR	<code>AWS_ENDPOINT_URL_ECR</code>	
ECR PUBLIC	<code>AWS_ENDPOINT_URL_ECR_PUBLIC</code>	
ECS	<code>AWS_ENDPOINT_URL_ECS</code>	
EFS	<code>AWS_ENDPOINT_URL_EFS</code>	
EKS	<code>AWS_ENDPOINT_URL_EKS</code>	
EKS Auth	<code>AWS_ENDPOINT_URL_EKS_AUTH</code>	
Elastic Inference	<code>AWS_ENDPOINT_URL_ELASTIC_INFERENCE</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
ElastiCache	<code>AWS_ENDPOINT_URL_ELASTICACHE</code>	
Elastic Beanstalk	<code>AWS_ENDPOINT_URL_ELASTIC_BEANSTALK</code>	
Elastic Transcoder	<code>AWS_ENDPOINT_URL_ELASTIC_TRANSCODER</code>	
Elastic Load Balancing	<code>AWS_ENDPOINT_URL_ELASTIC_LOAD_BALANCING</code>	
Elastic Load Balancing v2	<code>AWS_ENDPOINT_URL_ELASTIC_LOAD_BALANCING_V2</code>	
EMR	<code>AWS_ENDPOINT_URL_EMR</code>	
EMR containers	<code>AWS_ENDPOINT_URL_EMR_CONTAINERS</code>	
EMR Serverless	<code>AWS_ENDPOINT_URL_EMR_SERVERLESS</code>	

<b>serviceId</b>	C: id ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
EntityResolution	en o:	<b>AWS_ENDPOINT_URL_ENTITYRESOLUTION</b>
Elasticsearch Service	e: a: i:	<b>AWS_ENDPOINT_URL_ELASTICSEARCH_SERVICE</b>
EventBridge	en g:	<b>AWS_ENDPOINT_URL_EVENTBRIDGE</b>
Evidently	en	<b>AWS_ENDPOINT_URL_EVIDENTLY</b>
finspace	f:	<b>AWS_ENDPOINT_URL_FINSPEACE</b>
finspace data	f: d:	<b>AWS_ENDPOINT_URL_FINSPEACE_DATA</b>
Firehose	f:	<b>AWS_ENDPOINT_URL_FIREHOSE</b>
fis	f:	<b>AWS_ENDPOINT_URL_FIS</b>
FMS	fr	<b>AWS_ENDPOINT_URL_FMS</b>
forecast	fr	<b>AWS_ENDPOINT_URL_FORECAST</b>

<b>serviceId</b>	C: <b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno id ac de se pa us cc o A c fil
forecastquery	f: AWS_ENDPOINT_URL_FORECASTQUERY u
FraudDetector	f: AWS_ENDPOINT_URL_FRAUDETECTOR c
FreeTier	f: AWS_ENDPOINT_URL_FREETIER
FSx	f: AWS_ENDPOINT_URL_FSX
GameLift	g: AWS_ENDPOINT_URL_GAMELIFT
Glacier	g: AWS_ENDPOINT_URL_GLACIER
Global Accelerator	g: AWS_ENDPOINT_URL_GLOBAL_ACCELERATOR c
Glue	g: AWS_ENDPOINT_URL_GLUE
grafana	g: AWS_ENDPOINT_URL_GRAFANA
Greengrass	g: AWS_ENDPOINT_URL_GREENGRASS s

<b>serviceId</b>	Cl id ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
GreengrassV2	g: s\	AWS_ENDPOINT_URL_GREENGRASSV2
GroundStation	g: t:	AWS_ENDPOINT_URL_GROUNDSTATION
GuardDuty	g:	AWS_ENDPOINT_URL_GUARDDUTY
Health	h:	AWS_ENDPOINT_URL_HEALTH
HealthLake	h: e	AWS_ENDPOINT_URL_HEALTHLAKE
Honeycode	h:	AWS_ENDPOINT_URL_HONEYCODE
IAM	i:	AWS_ENDPOINT_URL_IAM
identitystore	i: t:	AWS_ENDPOINT_URL_IDENTITYSTORE
imagebuilder	i: d:	AWS_ENDPOINT_URL_IMAGEBUILDER

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
ImportExport	<code>AWS_ENDPOINT_URL_IMPORTEXPORT</code>	
Inspector	<code>AWS_ENDPOINT_URL_INSPECTOR</code>	
Inspector Scan	<code>AWS_ENDPOINT_URL_INSPECTOR_SCAN</code>	
Inspector2	<code>AWS_ENDPOINT_URL_INSPECTOR2</code>	
InternetMonitor	<code>AWS_ENDPOINT_URL_INTERNETMONITOR</code>	
IoT	<code>AWS_ENDPOINT_URL_IOT</code>	
IoT Data Plane	<code>AWS_ENDPOINT_URL_IOT_DATA_PLANE</code>	
IoT Jobs Data Plane	<code>AWS_ENDPOINT_URL_IOT_JOBS_DATA_PLANE</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
IoT 1Click Devices Service	<code>AWS_ENDPOINT_URL_IOT_1CLICK_DEVICES_&lt;REGION&gt;</code>	
IoT 1Click Projects	<code>AWS_ENDPOINT_URL_IOT_1CLICK_PROJECTS_&lt;REGION&gt;</code>	
IoTAnalytics	<code>AWS_ENDPOINT_URL_IOTANALYTICS_&lt;REGION&gt;</code>	
IotDeviceAdvisor	<code>AWS_ENDPOINT_URL_IOTDEVICEADVISOR_&lt;REGION&gt;</code>	
IoT Events	<code>AWS_ENDPOINT_URL_IOT_EVENTS_&lt;REGION&gt;</code>	
IoT Events Data	<code>AWS_ENDPOINT_URL_IOT_EVENTS_DATA_&lt;REGION&gt;</code>	
IoTFleetHub	<code>AWS_ENDPOINT_URL_IOTFLEETHUB_&lt;REGION&gt;</code>	
IoTFleetWise	<code>AWS_ENDPOINT_URL_IOTFLEETWISE_&lt;REGION&gt;</code>	

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
<code>IoTSecureTunneling</code>	<code>AWS_ENDPOINT_URL_IOTSECURETUNNELING</code>	
<code>IoTSiteWise</code>	<code>AWS_ENDPOINT_URL_IOTSITWISE</code>	
<code>IoTThingsGraph</code>	<code>AWS_ENDPOINT_URL_IOTTHINGSGRAPH</code>	
<code>IoTTwinMaker</code>	<code>AWS_ENDPOINT_URL_IOTTWINMAKER</code>	
<code>IoT Wireless</code>	<code>AWS_ENDPOINT_URL_IOT_WIRELESS</code>	
<code>ivs</code>	<code>AWS_ENDPOINT_URL_IVS</code>	
<code>IVS RealTime</code>	<code>AWS_ENDPOINT_URL_IVS_REALTIME</code>	
<code>ivschat</code>	<code>AWS_ENDPOINT_URL_IVSCHAT</code>	
<code>Kafka</code>	<code>AWS_ENDPOINT_URL_KAFKA</code>	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
KafkaConnect	<code>AWS_ENDPOINT_URL_KAFKACONNECT</code>	
kendra	<code>AWS_ENDPOINT_URL_KENDRA</code>	
Kendra Ranking	<code>AWS_ENDPOINT_URL_KENDRA_RANKING</code>	
Keyspaces	<code>AWS_ENDPOINT_URL_KEYSPACES</code>	
Kinesis	<code>AWS_ENDPOINT_URL_KINESIS</code>	
Kinesis Video Archived Media	<code>AWS_ENDPOINT_URL_KINESIS_VIDEO_ARCHIVED_MEDIA</code>	
Kinesis Video Media	<code>AWS_ENDPOINT_URL_KINESIS_VIDEO_MEDIA</code>	
Kinesis Video Signaling	<code>AWS_ENDPOINT_URL_KINESIS_VIDEO_SIGNALING</code>	

<b>serviceId</b>	<b>Código de acceso de servicio para usuarios con acceso a la configuración</b>	<b>variable de entorno</b>
Kinesis Video WebRTC Storage	k: AWS_ENDPOINT_URL_KINESIS_VIDEO_WEBRTC i: C_STORAGE	
Kinesis Analytics	k: AWS_ENDPOINT_URL_KINESIS_ANALYTICS n:	
Kinesis Analytics V2	k: AWS_ENDPOINT_URL_KINESIS_ANALYTICS_V2 n: v:	
Kinesis Video	k: AWS_ENDPOINT_URL_KINESIS_VIDEO i:	
KMS	k: AWS_ENDPOINT_URL_KMS	
LakeFormation	l: AWS_ENDPOINT_URL_LAKEFORMATION t:	
Lambda	l: AWS_ENDPOINT_URL_LAMBDA	
Launch Wizard	l: AWS_ENDPOINT_URL_LAUNCH_WIZARD z:	

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Lex Model Building Service	<code>AWS_ENDPOINT_URL_LEX_MODEL_BUILDING_SERVICE</code>	
Lex Runtime Service	<code>AWS_ENDPOINT_URL_LEX_RUNTIME_SERVICE</code>	
Lex Models V2	<code>AWS_ENDPOINT_URL_LEX_MODELS_V2</code>	
Lex Runtime V2	<code>AWS_ENDPOINT_URL_LEX_RUNTIME_V2</code>	
License Manager	<code>AWS_ENDPOINT_URL_LICENSE_MANAGER</code>	
License Manager Linux Subscriptions	<code>AWS_ENDPOINT_URL_LICENSE_MANAGER_LINUX_SUBSCRIPTIONS</code>	

<b>serviceId</b>	<p>Clave de acceso de servicio para usar con el cliente de AWS SDKs</p> <p><b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno</p>
License Manager User Subscriptions	<p>1: AWS_ENDPOINT_URL_LICENSE_MANAGER_USER_SUBSCRIPTIONS</p>
Lightsail	<p>1: AWS_ENDPOINT_URL_LIGHTSAIL</p>
Location	<p>1: AWS_ENDPOINT_URL_LOCATION</p>
CloudWatch Logs	<p>1: AWS_ENDPOINT_URL_CLOUDWATCH_LOGS</p>
CloudWatch Logs	<p>1: AWS_ENDPOINT_URL_CLOUDWATCH_LOGS</p>
LookoutEquipment	<p>1: AWS_ENDPOINT_URL_LOOKOUTEQUIPMENT</p>
LookoutMetrics	<p>1: AWS_ENDPOINT_URL_LOOKOUTMETRICS</p>
LookoutVision	<p>1: AWS_ENDPOINT_URL_LOOKOUTVISION</p>

<b>serviceId</b>	<p>Clid ac de se pa us cc o Al co fil</p>	AWS_ENDPOINT_URL_<SERVICE> variable de entorno
m2	m:	AWS_ENDPOINT_URL_M2
Machine Learning	m:	AWS_ENDPOINT_URL_MACHINE_LEARNING
Macie2	m:	AWS_ENDPOINT_URL_MACIE2
ManagedBlockchain	m:	AWS_ENDPOINT_URL_MANAGEDBLOCKCHAIN
ManagedBlockchain Query	m:	AWS_ENDPOINT_URL_MANAGEDBLOCKCHAIN_QUERY
Marketplace Agreement	m:	AWS_ENDPOINT_URL_MARKETPLACE_AGREEMENT
Marketplace Catalog	m:	AWS_ENDPOINT_URL_MARKETPLACE_CATALOG
Marketplace Deployment	m:	AWS_ENDPOINT_URL_MARKETPLACE_DEPLOYMENT

<b>serviceId</b>	<p>Clave de acceso de sesión para usuarios con acceso a la configuración de archivo</p> <p><b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno</p>
Marketplace Entitlement Service	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MARKETPLACE_ENTITLEMENT_SERVICE</b></p>
Marketplace Commerce Analytics	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MARKETPLACE_COMMERCIAL_ANALYTICS</b></p>
MediaConnect	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MEDIACONNECT</b></p>
MediaConvert	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MEDIACONVERT</b></p>
MediaLive	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MEDIALIVE</b></p>
MediaPackage	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MEDIAPACKAGE</b></p>
MediaPackage Vod	<p>muestra el endpoint de configuración de servicio</p> <p><b>AWS_ENDPOINT_URL_MEDIAPACKAGE_VOD</b></p>

<b>serviceId</b>	Clave de configuración	Descripción
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
MediaPackageV2	<code>AWS_ENDPOINT_URL_MEDIAPACKAGEV2</code>	
MediaStore	<code>AWS_ENDPOINT_URL_MEDIASTORE</code>	
MediaStore Data	<code>AWS_ENDPOINT_URL_MEDIASTORE_DATA</code>	
MediaTailor	<code>AWS_ENDPOINT_URL_MEDIATAILOR</code>	
Medical Imaging	<code>AWS_ENDPOINT_URL_MEDICAL_IMAGING</code>	
MemoryDB	<code>AWS_ENDPOINT_URL_MEMORYDB</code>	
Marketplace Metering	<code>AWS_ENDPOINT_URL_MARKETPLACE_METERING</code>	
Migration Hub	<code>AWS_ENDPOINT_URL_MIGRATION_HUB</code>	
mgn	<code>AWS_ENDPOINT_URL_MGN</code>	

<b>serviceId</b>	Cl id ac de se pa us cc o A c fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
Migration Hub Refactor Spaces	m: _I TOR_SPACES c e:	AWS_ENDPOINT_URL_MIGRATION_HUB_REFAC TOR_SPACES
MigrationHub Config	m: h g	AWS_ENDPOINT_URL_MIGRATIONHUB_CONFIG
MigrationHubOrches trator	m: h t:	AWS_ENDPOINT_URL_MIGRATIONHUBORCHESTRATOR
MigrationHubStrategy	m: h g)	AWS_ENDPOINT_URL_MIGRATIONHUBSTRATEGY
Mobile	m:	AWS_ENDPOINT_URL_MOBILE
mq	m:	AWS_ENDPOINT_URL_MQ
MTurk	m:	AWS_ENDPOINT_URL_MTURK
MWAA	m:	AWS_ENDPOINT_URL_MWAA

<b>serviceId</b>	Clase de configuración de servicio	Variable de entorno
	Clase de configuración de servicio de SDK de AWS	variable de entorno
Neptune	neptune	AWS_ENDPOINT_URL_NEPTUNE
Neptune Graph	neptune-graph	AWS_ENDPOINT_URL_NEPTUNE_GRAPH
neptunedata	neptune-data	AWS_ENDPOINT_URL_NEPTUNEDATA
Network Firewall	network-firewall	AWS_ENDPOINT_URL_NETWORK_FIREWALL
NetworkManager	networkmanager	AWS_ENDPOINT_URL_NETWORKMANAGER
NetworkMonitor	networkmonitor	AWS_ENDPOINT_URL_NETWORKMONITOR
nimble	nimble	AWS_ENDPOINT_URL_NIMBLE
OAM	oam	AWS_ENDPOINT_URL_OAM
Omics	omics	AWS_ENDPOINT_URL_OMICS
OpenSearch	opensearch	AWS_ENDPOINT_URL_OPENSEARCH

<b>serviceId</b>	Ci id ac de se pa us cc o A c fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
OpenSearchServerless	o h: s:	<b>AWS_ENDPOINT_URL_OPENSEARCHSERVERLESS</b>
OpsWorks	o	<b>AWS_ENDPOINT_URL_OPSWORKS</b>
OpsWorksCM	o m	<b>AWS_ENDPOINT_URL_OPSWORKSCM</b>
Organizations	o: ic	<b>AWS_ENDPOINT_URL_ORGANIZATIONS</b>
OSIS	o:	<b>AWS_ENDPOINT_URL_OSIS</b>
Outposts	o:	<b>AWS_ENDPOINT_URL_OUTPOSTS</b>
p8data	p:	<b>AWS_ENDPOINT_URL_P8DATA</b>
p8data	p:	<b>AWS_ENDPOINT_URL_P8DATA</b>
Panorama	p:	<b>AWS_ENDPOINT_URL_PANORAMA</b>
Payment Cryptography	p: r: h:	<b>AWS_ENDPOINT_URL_PAYMENT_CRYPTOGRAPHY</b>

<b>serviceId</b>	Cl id ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
Payment Cryptography Data	pa ry hy	<b>AWS_ENDPOINT_URL_PAYMENT_CRYPTOGRAPHY_DATA</b>
Pca Connector Ad	pa ct	<b>AWS_ENDPOINT_URL_PCA_CONNECTOR_AD</b>
Personalize	pa ze	<b>AWS_ENDPOINT_URL_PERSONALIZE</b>
Personalize Events	pa ze	<b>AWS_ENDPOINT_URL_PERSONALIZE_EVENTS</b>
Personalize Runtime	pa ze e	<b>AWS_ENDPOINT_URL_PERSONALIZE_RUNTIME</b>
PI	pa	<b>AWS_ENDPOINT_URL_PI</b>
Pinpoint	pa	<b>AWS_ENDPOINT_URL_PINPOINT</b>
Pinpoint Email	pa er	<b>AWS_ENDPOINT_URL_PINPOINT_EMAIL</b>

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Pinpoint SMS Voice	<code>p: AWS_ENDPOINT_URL_PINPOINT_SMS_VOICE</code>	
Pinpoint SMS Voice V2	<code>p: AWS_ENDPOINT_URL_PINPOINT_SMS_VOICE_V2</code>	
Pipes	<code>p: AWS_ENDPOINT_URL_PIPES</code>	
Polly	<code>p: AWS_ENDPOINT_URL_POLLY</code>	
Pricing	<code>p: AWS_ENDPOINT_URL_PRICING</code>	
PrivateNetworks	<code>p: AWS_ENDPOINT_URL_PRIVATENETWORKS</code>	
Proton	<code>p: AWS_ENDPOINT_URL_PROTON</code>	
QBusiness	<code>q: AWS_ENDPOINT_URL_QBUSINESS</code>	
QConnect	<code>q: AWS_ENDPOINT_URL_QCONNECT</code>	
QLDB	<code>q: AWS_ENDPOINT_URL_QLDB</code>	

<b>serviceId</b>	Cl id ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
QLDB Session	q ic	<b>AWS_ENDPOINT_URL_QLDB_SESSION</b>
QuickSight	q t	<b>AWS_ENDPOINT_URL_QUICKSIGHT</b>
RAM	r	<b>AWS_ENDPOINT_URL_RAM</b>
rbin	r	<b>AWS_ENDPOINT_URL_RBIN</b>
RDS	r	<b>AWS_ENDPOINT_URL_RDS</b>
RDS Data	r	<b>AWS_ENDPOINT_URL_RDS_DATA</b>
Redshift	r	<b>AWS_ENDPOINT_URL_REDSHIFT</b>
Redshift Data	r d	<b>AWS_ENDPOINT_URL_REDSHIFT_DATA</b>
Redshift Serverless	r S S	<b>AWS_ENDPOINT_URL_REDSHIFT_SERVERLESS</b>
Rekognition	r O	<b>AWS_ENDPOINT_URL_REKOGNITION</b>

<b>serviceId</b>	Clid ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
repostspace	re co	<b>AWS_ENDPOINT_URL_REPOSTSPACE</b>
resiliencehub	re el	<b>AWS_ENDPOINT_URL_RESILIENCEHUB</b>
Resource Explorer 2	re e) 2	<b>AWS_ENDPOINT_URL_RESOURCE_EXPLORER_2</b>
Resource Groups	re g:	<b>AWS_ENDPOINT_URL_RESOURCE_GROUPS</b>
Resource Groups Tagging API	re g: g:	<b>AWS_ENDPOINT_URL_RESOURCE_GROUPS_TAGGING_API</b>
RoboMaker	re	<b>AWS_ENDPOINT_URL_ROBOMAKER</b>
RolesAnywhere	re he	<b>AWS_ENDPOINT_URL_ROLESEANYWHERE</b>
Route 53	re	<b>AWS_ENDPOINT_URL_ROUTE_53</b>

<b>serviceId</b>	Cl id ac de se pa us cc o Al co fil	AWS_ENDPOINT_URL_<SERVICE> variable de entorno
Route53 Recovery Cluster	re en li	AWS_ENDPOINT_URL_ROUTE53_RECOVERY_CLUSTER
Route53 Recovery Control Config	re en or n	AWS_ENDPOINT_URL_ROUTE53_RECOVERY_CONTROL_CONFIG
Route53 Recovery Readiness	re en e:	AWS_ENDPOINT_URL_ROUTE53_RECOVERY_READINESS
Route 53 Domains	re de	AWS_ENDPOINT_URL_ROUTE_53_DOMAINS
Route53Resolver	re so	AWS_ENDPOINT_URL_ROUTE53RESOLVER
RUM	re	AWS_ENDPOINT_URL_RUM
S3	s:	AWS_ENDPOINT_URL_S3
S3 Control	s: 1	AWS_ENDPOINT_URL_S3_CONTROL

<b>serviceId</b>	Clave de acceso de servicio para usuarios con acceso a la configuración	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
S3Outposts	s3	AWS_ENDPOINT_URL_S3OUTPOSTS
SageMaker	sagemaker	AWS_ENDPOINT_URL_SAGEMAKER
SageMaker A2I Runtime	sagemaker_a2i_runtime	AWS_ENDPOINT_URL_SAGEMAKER_A2I_RUNTIME
Sagemaker Edge	sagemaker_edge	AWS_ENDPOINT_URL_SAGEMAKER_EDGE
SageMaker FeatureStore Runtime	sagemaker_featurestore_runtime	AWS_ENDPOINT_URL_SAGEMAKER_FEATURESTORE_RUNTIME
SageMaker Geospatial	sagemaker_geospatial	AWS_ENDPOINT_URL_SAGEMAKER_GEOSPATIAL
SageMaker Metrics	sagemaker_metrics	AWS_ENDPOINT_URL_SAGEMAKER_METRICS

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
SageMaker Runtime	<code>AWS_ENDPOINT_URL_SAGEMAKER_RUNTIME</code>	
savingsplans	<code>AWS_ENDPOINT_URL_SAVINGSPLANS</code>	
Scheduler	<code>AWS_ENDPOINT_URL_SCHEDULER</code>	
schemas	<code>AWS_ENDPOINT_URL_SCHEMAS</code>	
SimpleDB	<code>AWS_ENDPOINT_URL_SIMPLEDB</code>	
Secrets Manager	<code>AWS_ENDPOINT_URL_SECRETS_MANAGER</code>	
SecurityHub	<code>AWS_ENDPOINT_URL_SECURITYHUB</code>	
SecurityLake	<code>AWS_ENDPOINT_URL_SECURITYLAKE</code>	

<b>serviceId</b>	Clave de acceso de servicio para usar con el cliente de AWS	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
ServerlessApplicationRepository	servicio de repositorio de aplicaciones sin servidor	<b>AWS_ENDPOINT_URL_SERVERLESSAPPLICATIONREPOSITORY</b>
Service Quotas	servicio de cuotas de servicio	<b>AWS_ENDPOINT_URL_SERVICE_QUOTAS</b>
Service Catalog	servicio de catálogo de servicios	<b>AWS_ENDPOINT_URL_SERVICE_CATALOG</b>
Service Catalog AppRegistry	servicio de registro de aplicaciones de catálogo de servicios	<b>AWS_ENDPOINT_URL_SERVICE_CATALOG_APPREGISTRY</b>
ServiceDiscovery	servicio de descubrimiento de servicios	<b>AWS_ENDPOINT_URL_SERVICEDISCOVERY</b>
SES	servicio de correo electrónico simple	<b>AWS_ENDPOINT_URL_SES</b>
SESV2	servicio de correo electrónico simple (versión 2)	<b>AWS_ENDPOINT_URL_SESV2</b>
Shield	servicio de protección de aplicaciones web	<b>AWS_ENDPOINT_URL_SHIELD</b>

<b>serviceId</b>	Cl id ac de se pa us cc o Al co fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
signer	s:	AWS_ENDPOINT_URL_SIGNER
SimSpaceWeaver	s: e:	AWS_ENDPOINT_URL_SIMSPACEWEAVER
SMS	sr	AWS_ENDPOINT_URL_SMS
Snow Device Management	sr C m	AWS_ENDPOINT_URL_SNOW_DEVICE_MANAGEMENT
Snowball	sr	AWS_ENDPOINT_URL_SNOWBALL
SNS	sr	AWS_ENDPOINT_URL_SNS
SQS	sr	AWS_ENDPOINT_URL_SQS
SSM	s:	AWS_ENDPOINT_URL_SSM
SSM Contacts	s: c:	AWS_ENDPOINT_URL_SSM_CONTACTS
SSM Incidents	s: e:	AWS_ENDPOINT_URL_SSM_INCIDENTS
Ssm Sap	s:	AWS_ENDPOINT_URL_SSM_SAP

<b>serviceId</b>	<b>Clave de configuración</b>	<b>Descripción</b>
	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
SSO	<code>AWS_ENDPOINT_URL_SSO</code>	
SSO Admin	<code>AWS_ENDPOINT_URL_SSO_ADMIN</code>	
SSO OIDC	<code>AWS_ENDPOINT_URL_SSO_OIDC</code>	
SFN	<code>AWS_ENDPOINT_URL_SFN</code>	
Storage Gateway	<code>AWS_ENDPOINT_URL_STORAGE_GATEWAY</code>	
STS	<code>AWS_ENDPOINT_URL_STS</code>	
SupplyChain	<code>AWS_ENDPOINT_URL_SUPPLYCHAIN</code>	
Support	<code>AWS_ENDPOINT_URL_SUPPORT</code>	
Support App	<code>AWS_ENDPOINT_URL_SUPPORT_APP</code>	
SWF	<code>AWS_ENDPOINT_URL_SWF</code>	
synthetics	<code>AWS_ENDPOINT_URL_SYNTHETICS</code>	

<b>serviceId</b>	Clave de acceso de sesión para usuarios con acceso a la configuración	<code>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</code>	variable de entorno
Textract		<code>textract</code>	<code>AWS_ENDPOINT_URL_TEXTRACT</code>
Timestream InfluxDB		<code>timestream-influxdb</code>	<code>AWS_ENDPOINT_URL_TIMESTREAM_INFLUXDB</code>
Timestream Query		<code>timestream-query</code>	<code>AWS_ENDPOINT_URL_TIMESTREAM_QUERY</code>
Timestream Write		<code>timestream-write</code>	<code>AWS_ENDPOINT_URL_TIMESTREAM_WRITE</code>
tnb		<code>tnb</code>	<code>AWS_ENDPOINT_URL_TNB</code>
Transcribe		<code>transcribe</code>	<code>AWS_ENDPOINT_URL_TRANSCRIBE</code>
Transfer		<code>transfer</code>	<code>AWS_ENDPOINT_URL_TRANSFER</code>
Translate		<code>translate</code>	<code>AWS_ENDPOINT_URL_TRANSLATE</code>
TrustedAdvisor		<code>trustedadvisor</code>	<code>AWS_ENDPOINT_URL_TRUSTEDADVISOR</code>

<b>serviceId</b>	Ci id ac de se pa us cc o A c fil	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b> variable de entorno
VerifiedPermissions	ve e: s	<b>AWS_ENDPOINT_URL_VERIFIEDPERMISSIONS</b>
Voice ID	vo	<b>AWS_ENDPOINT_URL_VOICE_ID</b>
VPC Lattice	vp C	<b>AWS_ENDPOINT_URL_VPC_LATTICE</b>
WAF	wi	<b>AWS_ENDPOINT_URL_WAF</b>
WAF Regional	wi n:	<b>AWS_ENDPOINT_URL_WAF_REGIONAL</b>
WAFV2	wi	<b>AWS_ENDPOINT_URL_WAFV2</b>
WellArchitected	wi te	<b>AWS_ENDPOINT_URL_WELLARCHITECTED</b>
Wisdom	wi	<b>AWS_ENDPOINT_URL_WISDOM</b>
WorkDocs	wi	<b>AWS_ENDPOINT_URL_WORKDOCS</b>
WorkLink	wi	<b>AWS_ENDPOINT_URL_WORKLINK</b>
WorkMail	wi	<b>AWS_ENDPOINT_URL_WORKMAIL</b>

<b>serviceId</b>	Clase de configuración	Variable de entorno
	ClientConfiguration	AWS_ENDPOINT_URL_<SERVICE>
WorkMailMessageFlow	WorkMailMessageFlowClientConfiguration	AWS_ENDPOINT_URL_WORKMAILMESSAGEFLOW
WorkSpaces	WorkSpacesClientConfiguration	AWS_ENDPOINT_URL_WORKSPACES
WorkSpaces Thin Client	WorkSpacesThinClientConfiguration	AWS_ENDPOINT_URL_WORKSPACES_THIN_CLIENT
WorkSpaces Web	WorkSpacesWebClientConfiguration	AWS_ENDPOINT_URL_WORKSPACES_WEB
XRay	XRayClientConfiguration	AWS_ENDPOINT_URL_XRAY

## Valores predeterminados de configuración inteligente

Con la función de configuración inteligente por defecto, AWS SDK puede proporcionar valores predeterminados optimizados y predefinidos para otros ajustes de configuración.

Configure esta funcionalidad mediante lo siguiente:

**defaults\_mode**- compartido AWS **config** configuración de archivos, **AWS\_DEFAULTS\_MODE**: variable de entorno, **aws.defaultsMode**- propiedad JVM del sistema: solo en Java/Kotlin

Con esta configuración, puede elegir un modo que se alinee con la arquitectura de la aplicación y, a continuación, proporcionar valores predeterminados optimizados para la aplicación. Si un AWS SDK la configuración tiene un valor establecido explícitamente, entonces ese valor siempre tiene prioridad. Si un AWS SDK la configuración no tiene un valor establecido de forma explícita y `defaults_mode` es igual al heredado, esta función puede proporcionar diferentes valores predeterminados para diversas configuraciones optimizadas para su aplicación. La configuración puede incluir lo siguiente: configuración de HTTP comunicación, comportamiento de reintento, configuración de punto final regional del servicio y, posiblemente, cualquier configuración SDK relacionada. Los clientes que utilizan esta característica pueden obtener nuevos valores predeterminados de configuración adaptados a los escenarios de uso habituales. Si el tuyo no `defaults_mode` es igual a `legacy`, te recomendamos que realices pruebas en la aplicación cuando la actualices SDK, ya que los valores predeterminados proporcionados podrían cambiar a medida que evolucionen las prácticas recomendadas.

Valor predeterminado: `legacy`

Nota: Las nuevas versiones principales de SDKs se establecerán de forma predeterminada en `standard`.

Valores válidos:

- `legacy`— Proporciona la configuración predeterminada que varía según el establecimiento de SDK y que existía antes de su establecimiento `defaults_mode`.
- `standard`: proporciona los últimos valores predeterminados recomendados que deberían poder ejecutarse de forma segura en la mayoría de los escenarios.
- `in-region`— Se basa en el modo estándar e incluye una optimización adaptada a las aplicaciones que requieren Servicios de AWS desde dentro del mismo Región de AWS.
- `cross-region`— Se basa en el modo estándar e incluye una optimización adaptada a las aplicaciones que requieren Servicios de AWS en una región diferente.
- `mobile`: se basa en el modo estándar e incluye una optimización adaptada a las aplicaciones móviles.
- `auto`: se basa en el modo estándar e incluye funciones experimentales. SDK Intenta descubrir el entorno de ejecución para determinar automáticamente la configuración adecuada. La detección automática se basa en la heurística y no proporciona una precisión del 100 %. Si no

se puede determinar el tiempo de ejecución, se utiliza el modo `standard`. La autodetección podría consultar [los metadatos de la instancia](#), lo que podría introducir latencia. Si la startup es fundamental para tu aplicación, te recomendamos que elijas un `defaults_mode` explícito en su lugar.

Ejemplo de configuración de este valor en el archivo `config`:

```
[default]
defaults_mode = standard
```

Los siguientes parámetros pueden optimizarse en función de la selección de `defaults_mode`:

- `retryMode`— Especifica cómo se SDK reintentan los intentos. Consulte [Comportamiento de los reintentos](#).
- `stsRegionalEndpoints`— Especifica cómo SDK determina el Servicio de AWS punto final que utiliza para comunicarse con el AWS Security Token Service (AWS STS). Mira [AWS STS Puntos finales regionales](#).
- `s3UsEast1RegionalEndpoints`— Especifica cómo SDK determina la AWS punto final de servicio que utiliza para comunicarse con Amazon S3 de la `us-east-1` región.
- `connectTimeoutInMillis`: tras realizar un intento de conexión inicial en un socket, el tiempo transcurrido hasta que se agote el tiempo de espera. Si el cliente no recibe la finalización del apretón de manos de conexión, se da por vencido y no se realiza la operación.
- `tlsNegotiationTimeoutInMillis`— El tiempo máximo que puede tardar un TLS apretón de manos desde el momento en que se envía el CLIENT HELLO mensaje hasta el momento en que el cliente y el servidor negocian completamente los cifrados e intercambian claves.

El valor predeterminado de cada configuración cambia en función del valor `defaults_mode` seleccionado para la aplicación. Estos valores se configuran actualmente de la siguiente manera (sujetos a cambios):

Parámetro	modo <b>standard</b>	modo <b>in-region</b>	modo <b>cross-region</b>	modo <b>mobile</b>
<code>retryMode</code>	<code>standard</code>	<code>standard</code>	<code>standard</code>	<code>standard</code>

Parámetro	modo <b>standard</b>	modo <b>in-region</b>	modo <b>cross-region</b>	modo <b>mobile</b>
<code>stsRegionalEndpoints</code>	regional	regional	regional	regional
<code>s3UsEast1RegionalEndpoints</code>	regional	regional	regional	regional
<code>connectTimeoutInMillis</code>	3100	1 100	3100	30000
<code>tlsNegotiationTimeoutInMillis</code>	3100	1 100	3100	30000

Por ejemplo, si el `defaults_mode` que ha seleccionado es `standard`, entonces el valor `standard` se asignará para `retry_mode` (de las opciones `retry_mode` válidas) y el valor `regional` se asignará para `stsRegionalEndpoints` (de las opciones `stsRegionalEndpoints` válidas).

## Compatibilidad con AWS SDKs

Las siguientes opciones SDKs son compatibles con las funciones y configuraciones descritas en este tema. Se anotan todas las excepciones parciales. Cualquier configuración de propiedades del JVM sistema es compatible con la AWS SDK for Java y el AWS SDK para Kotlin únicamente.

SDK	Compatible	Notas o más información
<a href="#">AWS CLI v2</a>	No	
<a href="#">SDK para C++</a>	Sí	Parámetros no optimizados: <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalE</code>

SDK	Compatible	Notas o más información
		<code>ndpoints</code> , <code>tlsNegotiationTimeoutInMilliseconds</code> .
<a href="#">SDK para Go V2 (1.x)</a>	Sí	Parámetros no optimizados: <code>retryMode</code> , <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalEndpoints</code> .
<a href="#">SDK para Go 1.x (V1)</a>	No	
<a href="#">SDK para Java 2.x</a>	Sí	Parámetros no optimizados: <code>stsRegionalEndpoints</code> .
<a href="#">SDK para Java 1.x</a>	No	
<a href="#">SDK para JavaScript 3.x</a>	Sí	Parámetros no optimizados: <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalEndpoints</code> , <code>tlsNegotiationTimeoutInMilliseconds</code> . <code>connectTimeoutInMilliseconds</code> se llama <code>connectionTimeout</code> .
<a href="#">SDK para JavaScript 2.x</a>	No	
<a href="#">SDK para Kotlin</a>	No	
<a href="#">SDK para .NET 3.x</a>	Sí	Parámetros no optimizados: <code>connectTimeoutInMilliseconds</code> , <code>tlsNegotiationTimeoutInMilliseconds</code> .

SDK	Compatible	Notas o más información
<a href="#">SDK para PHP 3.x</a>	Sí	Parámetros no optimizados: tlsNegotiationTime outInMillis .
<a href="#">SDK para Python (Boto3)</a>	Sí	Parámetros no optimizados: tlsNegotiationTime outInMillis .
<a href="#">SDK para Ruby 3.x</a>	Sí	
<a href="#">SDK para Rust</a>	No	
<a href="#">SDK para Swift</a>	No	
<a href="#">Herramientas para PowerShell</a>	Sí	Parámetros no optimizados: connectTimeoutInMi llis ,tlsNegoti ationTimeoutInMill is .

# AWS Bibliotecas Common Runtime (CRT)

Las bibliotecas AWS Common Runtime (CRT) son una biblioteca base de SDKs. CRT se trata de una familia modular de paquetes independientes, escrita en C. Cada paquete proporciona un buen rendimiento y un espacio mínimo para las diferentes funcionalidades requeridas. Estas funcionalidades son comunes y se comparten entre todas, lo SDKs que proporciona una mejor reutilización, optimización y precisión del código. Los paquetes son:

- [aws-labs/aws-c-auth](#): autenticación AWS del lado del cliente (proveedores de credenciales estándar y firma (sigv4))
- [aws-labs/aws-c-cal](#): tipos primitivos criptográficos, hashes (MD5, SHA256), firmantes, HMAC AES
- [aws-labs/aws-c-common](#): estructuras de datos básicas, tipos primitivos de subproceso/sincronización, administración de búferes, funciones relacionadas con stdlib
- [aws-labs/aws-c-compression](#): algoritmos de compresión (codificación/decodificación de Huffman)
- [aws-labs/aws-c-event-stream](#): procesamiento de mensajes de flujo de eventos (encabezados, preludio, carga útil, crc/trailer), implementación de llamadas a procedimientos remotos () sobre flujos de eventos RPC
- [aws-labs/aws-c-http](#): Implementación C99 de las especificaciones /1.1 y /2 HTTP
- [aws-labs/aws-c-io](#): Enchufes (TCP,UDP), tuberías DNS, bucles de eventos, canales, SSL/TLS
- [aws-labs/aws-c-iot](#): Implementación C99 de la integración de servicios de AWS IoT en la nube con dispositivos
- [aws-labs/aws-c-mqtt](#): protocolo de mensajería ligero y estándar para Internet de las cosas (IoT)
- [aws-labs/aws-c-s3](#): implementación de la biblioteca C99 para comunicarse con el servicio Amazon S3, diseñada para maximizar el rendimiento en las instancias de Amazon de gran ancho de banda EC2
- [aws-labs/aws-c-sdkutils](#): una biblioteca de utilidades para analizar y administrar perfiles AWS
- [aws-labs/aws-checksums](#): Multiplataforma, acelerada por hardware CRC32c y CRC32 con la posibilidad de recurrir a implementaciones de software eficientes
- [aws-labs/aws-lc](#): Biblioteca criptográfica de uso general mantenida por el equipo de AWS criptografía para sus clientes AWS y para ellos, basada en el código de los proyectos Google Boring y Open SSL

- [aws1abs/s2n](#): Implementación C99 de los SSL protocolos TLS/, diseñada para ser pequeña y rápida, con la seguridad como prioridad

CRT está disponible en todos SDKs excepto en Go y Rust.

## CRT dependencias

Las CRT bibliotecas forman una red compleja de relaciones y dependencias. Conocer estas relaciones es útil si necesita crearlas CRT directamente desde la fuente. Sin embargo, la mayoría de los usuarios acceden a la CRT funcionalidad a través de su idioma SDK (como AWS SDK C++ o AWS SDK Java) o de su dispositivo IoT idiomático SDK (como AWS IoT SDK para C++ o AWS IoT SDK para Java). En el siguiente diagrama, el cuadro de CRT enlaces de idioma hace referencia al paquete que contiene las CRT bibliotecas de un idioma SDK específico. Se trata de una colección de paquetes del formulario `aws-crt-*`, donde «\*» es un SDK idioma (por ejemplo, [aws-crt-cpp](#) o [aws-crt-java](#)).

La siguiente es una ilustración de las dependencias jerárquicas de las CRT bibliotecas.

# AWS Política de mantenimiento de SDK y herramientas

## Información general

Este documento describe la política de mantenimiento de los kits y herramientas de desarrollo de AWS software (SDK), incluidos los SDK móviles y de IoT, y sus dependencias subyacentes. AWS proporciona periódicamente a los AWS SDK y las herramientas actualizaciones que pueden incluir compatibilidad con AWS API nuevas o actualizadas, nuevas funciones, mejoras, correcciones de errores, parches de seguridad o actualizaciones de la documentación. Las actualizaciones también pueden abordar los cambios en las dependencias, los idiomas, los tiempos de ejecución y los sistemas operativos. Las versiones del SDK se publican en los administradores de paquetes (por ejemplo NuGet, Maven o PyPI) y están disponibles como código fuente en GitHub.

Recomendamos a los usuarios que utilicen up-to-date las versiones del SDK para mantenerse al día con las últimas funciones, actualizaciones de seguridad y dependencias subyacentes. No se recomienda el uso continuo de una versión del SDK no admitida, y debe hacerse según el criterio del usuario.

## Control de versiones

Las versiones de lanzamiento del AWS SDK tienen el formato X.Y.Z, donde X representa la versión principal. El aumento de la versión principal de un SDK indica que este ha tenido cambios considerables y sustanciales para admitir nuevos modismos y patrones en el idioma. Las versiones principales se introducen cuando las interfaces públicas (como las clases, métodos, tipos, etc.), los comportamientos o la semántica cambian. Las aplicaciones deben actualizarse para que funcionen con la versión más reciente del SDK. Es importante actualizar las versiones principales con cuidado y de acuerdo con las pautas de actualización proporcionadas por AWS.

## Ciclo de vida de las versiones principales del

El ciclo de vida de las principales versiones de SDK y herramientas consta de 5 fases, que se describen a continuación.

- Vista previa para desarrolladores (fase 0): durante esta fase, los SDK no son compatibles, no deben usarse en entornos de producción y están pensados únicamente para facilitar el acceso anticipado y para enviar comentarios. Es posible que en futuras versiones se introduzcan cambios

importantes. Una vez que AWS identifique una versión como un producto estable, puede marcarla como versión candidata. Las versiones candidatas a ser lanzadas están listas para su publicación en GA, a menos que surjan errores importantes, y recibirán soporte técnico completo de AWS .

- Disponibilidad general (GA) (fase 1): durante esta fase, los SDK son totalmente compatibles. AWS proporcionará versiones periódicas del SDK que incluyen soporte para nuevos servicios, actualizaciones de API para los servicios existentes y correcciones de errores y de seguridad. En el caso de Tools, AWS se publicarán versiones periódicas que incluyen nuevas actualizaciones de funciones y correcciones de errores. AWS será compatible con la versión GA de un SDK durante al menos 24 meses.
- Anuncio de mantenimiento (fase 2): AWS se publicará un anuncio público al menos 6 meses antes de que el SDK entre en modo de mantenimiento. Durante este período, el SDK seguirá siendo totalmente compatible. Por lo general, el modo de mantenimiento se anuncia al mismo tiempo que la siguiente versión principal pasa a GA.
- Mantenimiento (fase 3): durante el modo de mantenimiento, AWS limita las versiones del SDK para abordar únicamente las correcciones de errores críticos y los problemas de seguridad. Un SDK no recibirá actualizaciones de API para servicios nuevos o existentes, ni se actualizará para que sea compatible con nuevas regiones. El modo de mantenimiento tiene una duración predeterminada de 12 meses, a menos que se especifique lo contrario.
- Fin del soporte (fase 4): cuando un SDK llega al final del soporte, ya no recibirá actualizaciones ni versiones. Las versiones publicadas anteriormente seguirán estando disponibles a través de los administradores de paquetes públicos y el código permanecerá activo GitHub. El GitHub repositorio puede estar archivado. El uso de un SDK disponible end-of-support queda a discreción del usuario. Recomendamos a los usuarios que actualicen a la nueva versión principal.

La siguiente es una ilustración visual del ciclo de vida de la versión principal del SDK. Tenga en cuenta que los plazos que se muestran a continuación son ilustrativos y no vinculantes.

## Ciclo de vida de

La mayoría de AWS los SDK tienen dependencias subyacentes, como los tiempos de ejecución de los idiomas, los sistemas operativos o las bibliotecas y marcos de terceros. Estas dependencias suelen estar vinculadas a la comunidad lingüística o al proveedor propietario de ese componente en particular. Cada comunidad o proveedor publica su propio end-of-support cronograma para su producto.

Los siguientes términos se utilizan para clasificar las dependencias subyacentes de terceros:

- Sistema operativo (SO): algunos ejemplos incluyen Amazon Linux AMI, Amazon Linux 2, Windows 2008, Windows 2012, Windows 2016, etc.
- Lenguaje del tiempo de ejecución: algunos ejemplos son Java 7, Java 8, Java 11, .NET Core, .NET Standard, .NET PCL, etc.
- Biblioteca/Marco de trabajo de terceros: algunos ejemplos incluyen OpenSSL, .NET Framework 4.5, Java EE, etc.

Nuestra política consiste en seguir dando soporte a las dependencias del SDK durante al menos 6 meses después de que la comunidad o el proveedor hayan dejado de dar soporte a la dependencia. Sin embargo, esta política puede variar en función de la dependencia específica.

#### Note

AWS se reserva el derecho de interrumpir el soporte para una dependencia subyacente sin aumentar la versión principal del SDK

## Métodos de comunicación

Los anuncios de mantenimiento se comunican de varias maneras:

- Se envía un anuncio por correo electrónico a las cuentas afectadas en el que anunciamos nuestros planes de dejar de ofrecer soporte para la versión específica del SDK. El correo electrónico describirá la ruta de acceso end-of-support, especificará los plazos de la campaña y proporcionará una guía de actualización.
- AWS La documentación del SDK, como la documentación de referencia de la API, las guías de usuario, las páginas de marketing de los productos del SDK y los GitHub archivos readme (s), se actualiza para indicar el calendario de la campaña y proporcionar orientación sobre la actualización de las aplicaciones afectadas.
- Se publica una entrada de AWS blog en la que se describe el camino a seguir end-of-support y se reiteran los plazos de la campaña.
- Se añaden advertencias de obsolescencia a los SDK, en las que se describe la ruta de acceso a la documentación del SDK end-of-support y se enlaza con ella.

Para ver la lista de las principales versiones disponibles de los AWS SDK y las herramientas y en qué punto del ciclo de vida de mantenimiento se encuentran, consulte. [Compatibilidad de versiones](#)

## AWS SDKsy compatibilidad con las versiones de Tools

En la siguiente tabla se muestra la lista de las disponibles AWS Versiones principales del kit de desarrollo de software (SDK) y en qué parte del ciclo de vida del mantenimiento se encuentran, con los plazos correspondientes. Para obtener información detallada sobre el ciclo de vida de las versiones principales de AWS SDKsy Tools y sus dependencias subyacentes, consulte [Política de mantenimiento](#).

SDK	Versión principal	Fase actual	Fecha de disponibilidad general	Notas
<a href="#">AWS CLI</a>	1.x	Disponibilidad general	2 de septiembre de 2013	
<a href="#">AWS CLI</a>	2.x	Disponibilidad general	2/10/2020	
<a href="#">SDKpara C++</a>	1.x	Disponibilidad general	2 de septiembre de 2015	
<a href="#">SDKpara Go V2</a>	V2 1.x	Disponibilidad general	19/1/2021	
<a href="#">SDKpara Go</a>	1.x	Mantenimiento	19/11/2015	Consulte el <a href="#">anuncio</a> para conocer los detalles y las fechas
<a href="#">SDKpara Java</a>	1.x	Mantenimiento	25/03/2010	Consulte el <a href="#">anuncio</a> para conocer los detalles y las fechas

SDK	Versión principal	Fase actual	Fecha de disponibilidad general	Notas
<a href="#">SDK para Java</a>	2.x	Disponibilidad general	20/11/2018	
<a href="#">SDK para JavaScript</a>	1.x	Fin-del-soporte	6/5/2013	
<a href="#">SDK para JavaScript</a>	2.x	Mantenimiento	19/06/2014	Consulte el <a href="#">anuncio</a> para conocer los detalles y las fechas
<a href="#">SDK para JavaScript</a>	3.x	Disponibilidad general	15/12/2020	
<a href="#">SDK para Kotlin</a>	1.x	Disponibilidad general	27 de noviembre de 2023	
<a href="#">SDK para .NET</a>	1.x	Fin-del-soporte	11/2009	
<a href="#">SDK para .NET</a>	2.x	Fin-del-soporte	8/11/2013	
<a href="#">SDK para .NET</a>	3.x	Disponibilidad general	28/7/2015	
<a href="#">SDK para PHP</a>	2.x	Fin-del-soporte	2/11/2012	
<a href="#">SDK para PHP</a>	3.x	Disponibilidad general	27/05/2015	
<a href="#">SDK para Python (Boto2)</a>	1.x	Fin-del-soporte	13 de julio de 2011	
<a href="#">SDK para Python (Boto3)</a>	1.x	Disponibilidad general	22/06/2015	

SDK	Versión principal	Fase actual	Fecha de disponibilidad general	Notas
<a href="#">SDK para Python (Botocore)</a>	1.x	Disponibilidad general	22/06/2015	
<a href="#">SDK para Ruby</a>	1.x	Fin-del-soporte	14/7/2011	
<a href="#">SDK para Ruby</a>	2.x	Fin-del-soporte	15/02/2015	
<a href="#">SDK para Ruby</a>	3.x	Disponibilidad general	29 de agosto de 2017	
<a href="#">SDK para Rust</a>	1.x	Disponibilidad general	27/11/2023	
<a href="#">SDK para Swift</a>	1.x	Disponibilidad general	17/09/2024	
<a href="#">Herramientas para PowerShell</a>	2.x	Fin-del-soporte	8/11/2013	
<a href="#">Herramientas para PowerShell</a>	3.x	Fin-del-soporte	29/7/2015	
<a href="#">Herramientas para PowerShell</a>	4.x	Disponibilidad general	21/11/2019	

¿Busca una herramienta SDK o herramienta que no se menciona? El cifrado SDKs, los dispositivos SDKs IoT y los dispositivos móviles SDKs, por ejemplo, no se incluyen en esta guía. Para encontrar documentación sobre estas otras herramientas, consulte [Herramientas útiles AWS](#).

# Historial de documentos para AWS SDKsy Guía de referencia de herramientas

En la siguiente tabla se describen las adiciones y actualizaciones importantes del AWS SDKsy la Guía de referencia de herramientas. Para recibir notificaciones sobre las actualizaciones de esta documentación, puede suscribirse al RSS feed.

Cambio	Descripción	Fecha
<a href="#">Añadir Swift SDK a la referencia de ajustes</a>	Añadir la SDK compatibilidad con Swift a todas las referencias de configuración: compatibilidad con AWS SDKstablas.	17 de septiembre de 2024
<a href="#">SDKpara las propiedades del sistema Java 1.x</a>	Añada detalles sobre las opciones de configuración JVM del sistema compatibles mediante el AWS SDK for Java 1.x.	30 de mayo de 2024
<a href="#">Actualizaciones de configuraciones</a>	Añada los ajustes JVM de configuración del sistema.	27 de marzo de 2024
<a href="#">Actualizaciones de la tabla de compatibilidad</a>	Actualizaciones de la compatibilidad para SDK brindar soporte, actualizaciones de los procedimientos del Centro de IAM Identidad.	20 de febrero de 2024
<a href="#">Actualización de credenciales del contenedor. IMDSactualización.</a>	Añadir soporte para AmazonEKS. Se ha añadido una configuración para deshabilitar la opción IMDSv1 alternativa.	29 de diciembre de 2023

<a href="#">Compresión de solicitudes</a>	Agregar configuración para la característica de compresión de solicitudes.	27 de diciembre de 2023
<a href="#">Tablas de compatibilidad</a>	Se actualizaron las tablas de compatibilidad SDK y las funciones de las herramientas para SDK incluirlas para Kotlin, SDK Rust y AWS Tools for PowerShell.	10 de diciembre de 2023
<a href="#">Actualizaciones de autenticación</a>	Actualizaciones de los métodos de autenticación SDKs y las herramientas compatibles.	1 de julio de 2023
<a href="#">IAM actualizaciones de mejores prácticas</a>	Guía actualizada para alinearla con las IAM mejores prácticas. Para obtener más información, consulte <a href="#">las mejores prácticas de seguridad en IAM</a> .	27 de febrero de 2023
<a href="#">SSO actualizaciones</a>	Actualizaciones de SSO las credenciales para la nueva configuración del SSO token.	19 de noviembre de 2022
<a href="#">Actualizaciones de configuraciones</a>	Actualizaciones de la tabla de soporte para configuración general y puntos de acceso de varias regiones de Amazon S3.	17 de noviembre de 2022
<a href="#">Actualizaciones de configuraciones</a>	Actualizaciones en cuanto a la claridad del IMDS cliente y IMDS las credenciales. Actualizaciones de las variables de entorno.	4 de noviembre de 2022

---

<a href="#">Actualización de la página de bienvenida</a>	Anunciamos Amazon CodeWhisperer.	22 de septiembre de 2022
<a href="#">Cambio de nombre de servicio para inicio de sesión único</a>	Actualizaciones para reflejar eso AWS SSO ahora se conoce como AWS IAM Identity Center.	26 de julio de 2022
<a href="#">Actualización de configuraciones</a>	Actualizaciones menores en los detalles del archivo de configuración y en los ajustes compatibles.	15 de junio de 2022
<a href="#">Actualización</a>	Actualización masiva de casi todas las partes de esta guía.	1 de febrero de 2022
<a href="#">Versión inicial</a>	La primera versión de esta guía está disponible para el público.	13 de marzo de 2020

# Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el [Glosario de AWS](#) en la Referencia de Glosario de AWS.

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