API Gateway

Preguntas frecuentes

Edición 01

Fecha 2025-03-05

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Índice

1 Preguntas frecuentes comunes

Apertura de API

- ¿Puedo especificar una dirección de balanceador de carga de red privada para el servicio backend?
- ¿Puedo especificar la dirección de backend como una dirección IP de subred?
- ¿Puedo vincular nombres de dominio privados para el acceso a la API?

Invocación a las API

- ¿Cuáles son las posibles causas de un error de invocación a la API?
- ¿Por qué veo el mensaje de error "The API does not exist or has not been published in the environment" cuando invoco a una API?
- ¿Por qué veo el mensaje de error "No backend available" cuando invoco a una API?
- ¿Por qué aparece el mensaje de error "Backend unavailable" o "Backend timeout" cuando invoco el servicio backend?

Autenticación de API

- ¿APIG admite la autenticación bidireccional?

Políticas de API

- ¿Puedo configurar el número máximo de solicitudes simultáneas?
- ¿Tiene APIG límites de ancho de banda?
- ¿Cómo puedo proporcionar una API abierta a los usuarios específicos?

Importación y exportación de API

- ¿Cuáles son las posibles causas de un error de importación de API?
- ¿Hay una plantilla para importar las API con un archivo Swagger?

2 Preguntas frecuentes de consultoría de productos

2.1 ¿Cuáles son las relaciones entre una API, un entorno y una credencial?

Una API se puede publicar en diferentes entornos, como RELEASE (entorno en línea) y BETA (entorno de prueba).

Una aplicación (credencial) se refiere a la identidad de un llamador de API. Después de crear una aplicación (credencial), el sistema genera automáticamente una clave y un secreto para autenticar la aplicación (credencial). Después de publicar una API y asignarla a una aplicación (credencial), el propietario de la aplicación (credencial) puede invocar a la API.

Después de publicar una API en diferentes entornos, puede definir diferentes políticas de limitación de solicitudes y autorizar diferentes aplicaciones (credenciales) para invocar a la API. Por ejemplo, durante el proceso de prueba, la API v2 se publica en el entorno BETA y se autoriza a probar las aplicaciones (credenciales). API v1 es estable y se puede autorizar a todos los usuarios o aplicaciones (credenciales) en el entorno RELEASE.

2.2 ¿Puedo actualizar el gateway compartido a un gateway dedicado?

Actualmente, no puede actualizar el gateway compartido a un gateway dedicado. Sin embargo, puede hacer lo siguiente para lograr el mismo propósito:

1. Compre un gateway dedicado.
2. Exporte API desde el gateway compartido.
3. Importe las API al gateway dedicado.
4. Vincule un nuevo nombre de dominio para las API y cambie el registro de DNS a CNAME el nombre de dominio a la dirección IP de acceso público del gateway dedicado.

2.3 ¿Por qué no se pueden hacer clic en todos los botones de la consola de APIG?

Comprueba si su cuenta está en mora y recarga su cuenta si es necesario.

Para obtener más información, véase **Facturación**.

2.4 ¿Cómo garantizo la seguridad de las invocaciones a API?

- Autenticación de identidades

  Configure la autenticación de IAM o App para las API para evitar invocaciones maliciosas.
- Políticas de control de acceso

  Configure una lista blanca o una lista negra de direcciones IP/rangos de direcciones IP o cuentas para que las API protejan el acceso.
- Políticas de limitación de solicitudes

  Por defecto, se puede invocar una API hasta 200 veces por segundo. Si su servicio de backend no admite esta tasa de acceso, disminuya la cuota en consecuencia.

2.5 ¿Cómo puedo garantizar la seguridad de los servicios de backend invocados por APIG?

Puede garantizar la seguridad de los servicios backend invocados por APIG mediante los siguientes métodos:

- Vincular las claves de firma a las API

  Después de vincular una clave de firma a una API, APIG agrega información de firma a cada solicitud enviada al servicio de backend. El servicio backend calcula la información de firma en cada solicitud y comprueba si la información de firma es consistente con la de APIG.
- Cifrar solicitudes mediante HTTPS

  Asegúrese de que existe el certificado SSL requerido.
- Realizar autenticación de backend

  Habilite la autenticación de seguridad para los servicios de backend de las API deseadas para procesar solo las solicitudes de API que contienen información de autenticación correcta.

3 Apertura de API

3.1 ¿Por qué no puedo crear API?

La creación de las API es gratuita. Si no puede crear API, su cuenta debe estar en mora. **Recarga** su cuenta a tiempo.

Para más detalles, véase **Facturación**.

3.2 ¿Cómo defino los códigos de respuesta para una API?

Hay dos tipos de respuestas:

- Códigos de respuesta de gateway: devueltos por el gateway para solicitudes de API que se limitan, deniegan o fallan en la autenticación. Para obtener más información, véase **Personalizar respuesta de error para API**.
- Respuestas de servicio de backend: definidas por los servicios de API backend (proveedores de API) y transmitidas de forma transparente por APIG.

3.3 ¿Puedo especificar una dirección de balanceador de carga de red privada para el servicio backend?

- Para los gateway dedicados, puede utilizar direcciones de balanceador de carga de red privada.
- El gateway compartido en la consola antigua solo admite canales de VPC.
- Alternativamente, puede utilizar la EIP vinculada a un balanceador de carga de red pública.

3.4 ¿Puedo especificar la dirección de backend como una dirección IP de subred?

Si utiliza un gateway dedicado, puede especificar una dirección IP que pertenece a la misma subred donde se despliega el gateway, o la dirección privada de un centro de datos local conectado al gateway con Direct Connect.

Segmentos de red no admitidos:

- 0.0.0.0/8
- 10.0.0.0/8
- 100.125.0.0/16
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12
- 192.0.0.0/24
- 192.0.2.0/24
- 192.88.99.0/24
- 192.168.0.0/16
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

Si utiliza el gateway compartido en la consola antigua, no puede especificar la dirección de backend como dirección IP de subred. Para un servicio backend desplegado en varios ECS que se encuentran en la misma región pero no están vinculados a ninguna EIP, **cree un canal de VPC** y asocie los ECS con él.

3.5 ¿APIG admite varios puntos de conexión backend?

Sí

APIG admite la configuración de varios puntos de conexión backend con un canal de VPC (también llamado "canal de equilibrio de carga"). Puede agregar varios servidores en la nube a cada canal de VPC.

Para obtener más información, véase **Canales de equilibrio de carga**.

3.6 ¿Puedo vincular nombres de dominio privados para el acceso a la API?

En el gateway compartido de la consola antigua, el nombre de dominio que se va a enlazar debe haberse registrado y debe haber registros de CNAME que apunten el nombre de dominio al nombre de subdominio del grupo al que pertenece la API de destino. No puede vincular nombres de dominio privados o nombres de dominio que no admitan el acceso público a los grupos de API.

En un gateway dedicado, puede agregar un nombre de dominio privado (no es necesario archivar) y agregar un registro A para apuntar el nombre de dominio a la dirección de acceso entrante del gateway.

3.7 ¿Por qué no puedo invocar a una API entre dominios?

Causas posibles

La configuración de CORS de la API es incorrecta.

Solución

1. Asegúrese de que CORS se ha habilitado para la API.

   Vaya a la página de detalles de la API, haga clic en **Edit** y compruebe si CORS está habilitado. Si no lo es, habilítelo.

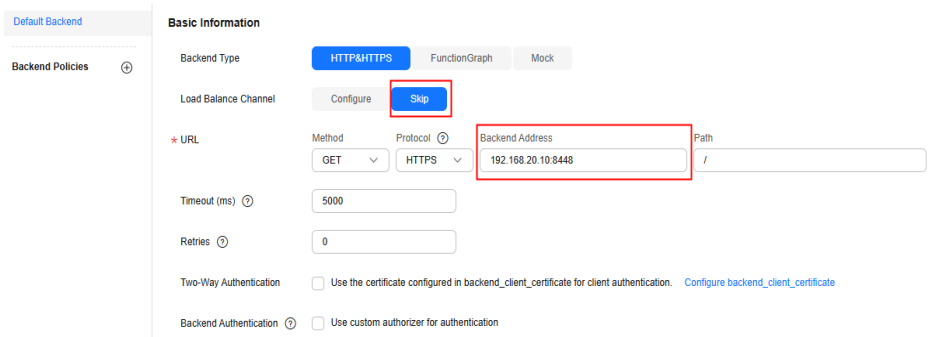
2. Compruebe si se ha creado una API con el método OPTIONS. Solo se requiere una API de este tipo para cada grupo de API.

   Los parámetros son los siguientes:

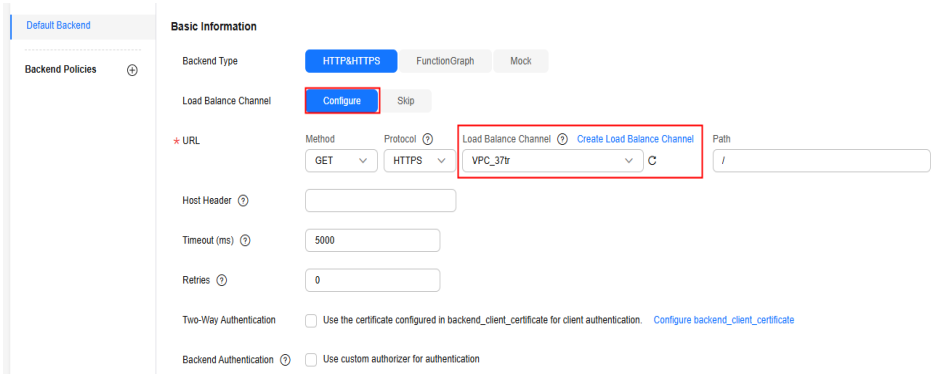
   - **API Group**: El mismo grupo al que pertenece la API con CORS habilitado.
   - **Method**: Seleccione **OPTIONS**.
   - **Protocol**: El mismo protocolo utilizado por la API con CORS habilitado.
   - **Path**: Igual que la ruta de la solicitud establecida para la API con CORS habilitada o que coincida con el prefijo.
   - **Matching**: seleccione **Prefix match**.
   - **Authentication Mode**: **None** significa que se concederá acceso a todos los usuarios. No se recomienda.
   - **CORS**: Habilite esta opción.

3.8 ¿Cómo uso APIG para abrir servicios desplegados en Huawei Cloud?

- Para un servicio desplegado en Huawei Cloud con una **dirección IP de red pública**, especifique la dirección IP como la dirección del servicio backend al crear una API en APIG. Si el servicio ha estado vinculado con un nombre de dominio, utilice el nombre de dominio como la dirección del servicio de backend. Para obtener más información sobre cómo crear una API, véase **Creación de una API**.



- Para un servicio desplegado en Huawei Cloud sin una dirección IP de red pública, especifique un canal de VPC para acceder al servicio de backend al crear una API en APIG. Para obtener más información sobre cómo crear un canal de VPC y una API, véase **Creación de un canal de equilibrio de carga** y **Creación de una API**



4 Publicación de una API

4.1 ¿Necesito publicar una API de nuevo después de la modificación?

Sí.

Después de modificar los parámetros de una API publicada, debe publicar la API de nuevo para sincronizar las modificaciones en el entorno.

Para obtener más información, véase **Publicación de una API**.

4.2 ¿Puedo acceder a una API publicada en un entorno Non-RELEASE?

Sí. Para acceder a una API publicada en un entorno que non-RELEASE, agregue el encabezado **x-stage** a la solicitud de API.

Ejemplo:

```
r.Header.Add("x-stage", "RELEASE")
```

También puede consultar los ejemplos en **Apertura e invocación rápida a las API**.

4.3 ¿Puedo invocar diferentes servicios de backend publicando una API en diferentes entornos?

Sí, puede invocar diferentes servicios de backend publicando una API en diferentes entornos mientras especifica variables de entorno y parámetros de backend.

Para obtener más información, véase **(Opcional) Configuración de entorno y variables de entorno**.

4.4 ¿Puedo especificar un entorno para la depuración de API?

Durante la depuración de API, el entorno de depuración específico de APIG se utiliza de forma predeterminada. Por lo tanto, no puede especificar otros entornos.

Una vez completada la depuración, debe publicar su API en un entorno y usar código o Postman para agregar el encabezado X-Stage para especificar el entorno donde desea invocar a la API.

5 Invocación a las API

5.1 ¿Cuáles son las posibles causas de un error de invocación a la API?

Red

Las fallas de invocación a la API pueden ocurrir en tres escenarios: dentro de una VPC, entre VPC y en una red pública.

- Dentro de una VPC: Compruebe si el nombre de dominio es el mismo que el asignado automáticamente para la API.
- Entre VPC: Compruebe si las dos VPC están conectadas. Si no están conectados, cree una interconexión de VPC para conectar las dos VPC.

  Para obtener más información sobre cómo crear y usar interconexiones de VPC, véase **Descripción de interconexiones de VPC** y **Exposición de servicios backend en todas las VPC**.
- En una red pública:
  - La API no está vinculada con una EIP y no tiene una dirección válida para el acceso a la red pública.

    Vincule una EIP a la API e inténtala de nuevo. Para obtener más detalles, véase **Entorno de red**.
  - Las reglas de entrada están configuradas incorrectamente.

    Para obtener más información acerca de cómo configurar reglas entrantes, consulte **Entorno de red**.
  - El encabezado de solicitud "host:*Group domain name*" no se agrega cuando se invoca a la API. Agregue el encabezado de solicitud e inténtelo de nuevo.

Nombre de dominio

- Compruebe si el nombre de dominio vinculado al grupo de API al que pertenece la API se ha licenciado correctamente y se puede resolver.
- Compruebe si el nombre de dominio está vinculado al grupo de API correcto.

- Se accede demasiadas veces al nombre de subdominio (nombre de dominio de depuración) asignado automáticamente al grupo de API. El nombre del subdominio se puede acceder solo 1000 veces al día. Es único y no se puede modificar. Agregue nombres de dominio independientes para el grupo para que las API del grupo sean accesibles.

Publicación de API

Compruebe si la API se ha publicado. Si la API ha sido modificada, publíquela de nuevo. Si la API se ha publicado en un entorno que no sea RELEASE, especifique el encabezado **X-Stage** como nombre del entorno.

Autenticación de API

Si la API usa autenticación de aplicaciones, compruebe si los AppKey y AppSecret utilizados para invocar a la API son correctos.

Políticas de control de API

- Compruebe si la política de control de acceso vinculada a la API es correcta.
- Compruebe si se ha alcanzado el límite de limitación de solicitudes de la API. Si no se crea ninguna política de limitación de solicitudes para una API, se puede acceder a la API 200 veces por segundo de forma predeterminada. Para cambiar este límite de gateways dedicados, vaya a la página **Gateway Information**, haga clic en la pestaña **Parameters** y modifique el parámetro **ratelimit_api_limits**.

5.2 ¿Por qué veo el mensaje de error "414 Request URI demasiado grande" cuando invoco a una API?

La URL de solicitud (incluidos los parámetros de solicitud) es demasiado larga. Coloque los parámetros de solicitud en el cuerpo de la solicitud e inténtelo de nuevo.

Para obtener detalles sobre los errores de invocación a la API, véase **Códigos de error**.

5.3 ¿Por qué veo el mensaje de error "The API does not exist or has not been published in the environment" cuando invoco a una API?

Si no se puede invocar a una API abierta en APIG, solucione el error realizando las siguientes operaciones:

1. El nombre de dominio, el método de solicitud o la ruta utilizada para invocar a la API es incorrecto.
   - Por ejemplo, se invoca con GET una API creada usando el método POST.
   - Si falta una barra diagonal (/) en la URL de acceso, se producirá un error en la coincidencia de la URL en los detalles de la API. Por ejemplo, las URL **http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test/** y **http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test** representan dos API diferentes.

2. La API no se ha publicado. Las API solo se pueden invocar después de que se hayan publicado en un entorno. Para obtener más información, véase **Publicación de una API**. Si la API se ha publicado en un entorno no de producción, compruebe si el encabezado **X-Stage** de la solicitud es el nombre del entorno.
3. El nombre de dominio se ha resuelto incorrectamente. Si el nombre de dominio, el método de solicitud y la ruta para invocar a la API son correctos y la API se ha publicado en un entorno, es posible que la API no se resuelva correctamente en el grupo al que pertenece la API. Por ejemplo, si tienes varios grupos de API y cada grupo tiene un nombre de dominio independiente, se puede invocar a la API usando el nombre de dominio independiente de otro grupo. Asegúrese de que se está llamando a la API usando el nombre de dominio correcto.
4. Comprueba si la API permite solicitudes OPTIONS entre regiones. En caso afirmativo, habilite el uso compartido de recursos de origen cruzado (CORS) para la API y cree una API que utilice el método OPTIONS. Para obtener más información, véase **CORS**.

5.4 ¿Por qué veo el mensaje de error "No backend available" cuando invoco a una API?

- Compruebe si el servicio de backend es accesible y modifique el servicio de backend si es inaccesible.
- Compruebe las configuraciones del grupo de seguridad de ECS del servicio de backend y verifique que se ha habilitado el puerto requerido.
- Compruebe si la dirección del servicio backend es una dirección IP pública. De ser así, habilite el acceso saliente en la página **Gateways** > **Access Console** > **Gateway Information**.
- Compruebe si las configuraciones de ACL de la VPC restringen la comunicación entre el gateway de API y la subred donde se encuentra el servicio de backend.
- Si utiliza un canal de VPC, compruebe si el puerto de servicio, el puerto de comprobación de estado y los servidores backend del canal VPC se han configurado correctamente.

  Si el tipo de canal de VPC es un microservicio, verifique si se ha agregado un enrutamiento al gateway. Para obtener más detalles, véase **Canal de carga de balanceo**. **Los backends del gateway compartido no admiten balanceadores de carga de red privada.**

5.5 ¿Por qué aparece el mensaje de error "Backend unavailable" o "Backend timeout" cuando invoco el servicio backend?

En la siguiente tabla se enumeran las posibles causas si un servicio backend no puede ser invocado o si se agota el tiempo de invocación.

Causa posible	Solución
La dirección del servicio de backend es incorrecta.	Cambie la dirección del servicio de backend en la definición de la API. Si se utiliza el nombre de dominio, asegúrese de que el nombre de dominio se puede resolver correctamente con la dirección IP del servicio de backend.
La duración del tiempo de espera es incorrecta. Si un servicio backend no devuelve una respuesta dentro de la duración de tiempo de espera configurada, APIG muestra un mensaje que indica que no se puede invocar el servicio backend.	Aumente la duración del tiempo de espera del servicio backend o acorte el tiempo de procesamiento en la definición de API.
Si la dirección backend es una dirección de ECS, el grupo de seguridad al que pertenece el ECS puede bloquear la solicitud en la dirección de entrada o de salida.	Compruebe el grupo de seguridad al que pertenece el ECS y asegúrese de que las reglas y protocolos de puerto entrante y saliente de este grupo de seguridad son correctos.
El protocolo de solicitud es incorrecto. Por ejemplo, el servicio backend utiliza HTTP, pero HTTPS está seleccionado en APIG.	Asegúrese de que el protocolo de la API creada es el mismo que el del servicio de backend.
La URL del servicio de backend es inalcanzable.	Compruebe la URL.

5.6 ¿Por qué veo el mensaje de error "Backend domain name resolution failed" cuando invoco el servicio backend?

Se muestra un mensaje de error que indica un error de resolución de nombre de dominio cuando se invoca al servicio backend, aunque se completa la resolución de nombre de dominio privado para la VPC donde se encuentra el gateway de API.

Causa posible

La VPC del gateway de la API está aislada de la del servicio backend. Los nombres de dominio privados solo se pueden resolver para la VPC del servicio backend.

Solución

- Método 1: Al crear una API, establezca **Backend Address** en un nombre de dominio de red pública.
- Método 2: Al crear una API, no utilice un canal de VPC (canal de equilibrio de carga). En su lugar, establezca **Backend Address** en la dirección IP del servicio backend y agregue un parámetro constante para especificar el campo **Host** en el encabezado.

- Método 3: Al crear una API, especifique un canal de VPC (canal de equilibrio de carga).
  a. Cree un canal de VPC (canal de balanceo de carga).
  b. Agregue la dirección del servicio backend.
  c. Al crear una API, seleccione el canal de VPC (canal de equilibrio de carga) y configure un encabezado personalizado.

5.7 ¿Por qué veo el mensaje de error "Incorrect IAM authentication information" Cuando invoco a una API?

Puede encontrar los siguientes errores relacionados con la información de autenticación de IAM:

- **Incorrect IAM authentication information: verify aksk signature fail**
- **Incorrect IAM authentication information: AK access failed to reach the limit,forbidden**
- **Incorrect IAM authentication information: decrypt token fail**
- **Incorrect IAM authentication information: Get secretKey failed**

Incorrect IAM authentication information: verify aksk signature fail

```
{
  "error_msg": "Incorrect IAM authentication information: verify aksk signature fail, ......
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

Causa posible

El algoritmo de firma es incorrecto, y la firma calculada por el cliente es diferente de la calculada por APIG.

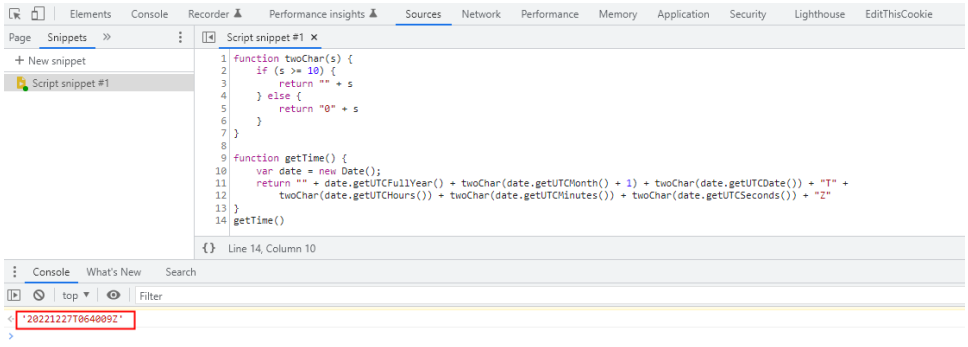
Solución

Paso 1 Descargue el **SDK de JavaScript**, vea el SDK de firma visualizado y obtenga la firma.

Paso 2 Descomprima el paquete y abra el archivo **demo.html** usando un navegador.

Paso 3 Obtenga el valor de **x-sdk-date** y compruebe si la diferencia entre este valor y la hora actual es de 15 minutos.

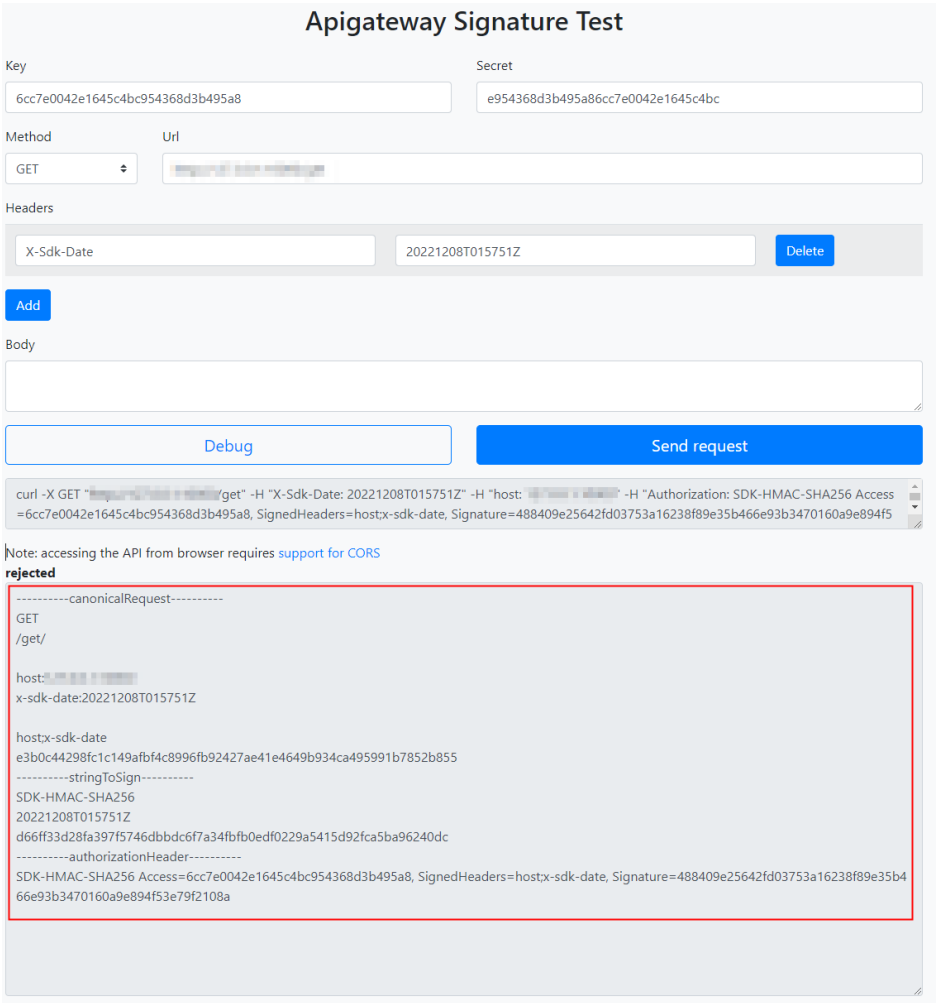
1. Presione **F12** en el teclado y elija **Sources** > **Snippets** > **New snippet**.
2. Copie el siguiente código en el fragmento de script de la derecha, haga clic con el botón derecho en el nombre del fragmento de la izquierda y seleccione **Run** en el menú contextual. El valor que se muestra en la ficha **Console** es el valor de **x-sdk-date**.




```
function twoChar(s) {
    if (s >= 10) {
        return "" + s
    } else {
        return "0" + s
    }
}

function getTime() {
    var date = new Date();
    return "" + date.getUTCFullYear() + twoChar(date.getUTCMonth() + 1) +
twoChar(date.getUTCDate()) + "T" +
        twoChar(date.getUTCHours()) + twoChar(date.getUTCMinutes()) +
twoChar(date.getUTCSeconds()) + "Z"
}
getTime()
```

Paso 4 Agregue **x-sdk-date** a **Headers** y establezca otros parámetros y haga clic en **Debug** para obtener la firma.



Para todas las solicitudes excepto get, delete y head, agregue un cuerpo en el área **Body** utilizando el mismo formato que un cuerpo de solicitud real.

Paso 5 Copie el comando **curl** en la figura de **Paso 4**, ejecútelo en una interfaz de línea de comandos y, a continuación, vaya al siguiente paso.

```
curl -X GET "http://192.168.0.1:10000/get" -H "X-Sdk-Date: 20221208T015751Z" -H
"host: 192.168.0.1:10000" -H "Authorization: SDK-HMAC-SHA256 Access=6cc7***95a8,
SignedHeaders=host;x-sdk-date, Signature=4884***108a" -d $''
```

Si se utiliza un autorizador personalizado, reemplace **Authorization** en el comando **curl** por el nombre del autorizador.

Paso 6 Compare la firma en el código local con la firma visualizada de JavaScript.

Por ejemplo, compruebe si los valores de **canonicalRequest**, **stringToSign** y **authorizationHeader** en el código de firma Java son los mismos que en la firma visualizada de JavaScript.


```
public void sign(Request request) throws UnsupportedEncodingException {
    String singerDate = getHeader(request, X_SDK_DATE);
    SimpleDateFormat sdf = new SimpleDateFormat( pattern: "yyyyMMdd'T'HHmmss'Z'");
    sdf.setTimeZone(TimeZone.getTimeZone("UTC"));

    if (singerDate == null) {
        singerDate = sdf.format(new Date());
        request.addHeader(X_SDK_DATE, singerDate);
    }
    addHostHeader(request);

    String messageDigestContent = calculateContentHash(request);

    String[] signedHeaders = getSignedHeaders(request);

    final String canonicalRequest = createCanonicalRequest(request, signedHeaders, messageDigestContent);

    final byte[] signingKey = deriveSigningKey(request.getSecrect());

    String stringToSign = createStringToSign(canonicalRequest, singerDate);
    byte[] signature = computeSignature(stringToSign, signingKey);
    String signatureResult = buildAuthorizationHeader(signedHeaders, signature, request.getKey());

    request.addHeader(AUTHORIZATION, signatureResult);
}
```

----Fin

Incorrect IAM authentication information: AK access failed to reach the limit,forbidden

```
{
  "error_msg": "Incorrect IAM authentication information: AK access failed to
reach the limit,forbidden." ......
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

Causas posibles

- El cálculo de la firma AK/SK es incorrecto.
- Las AK y SK no coinciden. Verifique si el SK es correcto.
- La autenticación de AK/SK falla durante más de cinco veces consecutivas, y el par AK/SK se bloquea durante cinco minutos. (Las solicitudes de autenticación se rechazan dentro de este período). Espere 5 minutos y reintente.
- Se utiliza un token caducado para la autenticación de token. Obtenga un nuevo token.

Solución

- Consulte **Incorrect IAM authentication information: verify aksk signature fail** para resolver el problema.
- Verifique si el SK es correcto.
- Espere 5 minutos y reintente.
- Obtenga un nuevo token.

Incorrect IAM authentication information: decrypt token fail

```
{
  "error_msg": "Incorrect IAM authentication information: decrypt token fail",
  "error_code": "APIG.0301",
  "request_id": "******"
}
```


Causa posible

El token no se puede analizar para la autenticación de IAM de la API.

Solución

- Compruebe si el token obtenido es el token de la cuenta de IAM correspondiente.
- Compruebe si el token es correcto.
- Compruebe si el token se ha obtenido en el entorno donde se invoca a la API.

Incorrect IAM authentication information: Get secretKey failed

```
{
"error_msg": "Incorrect IAM authentication information: Get secretKey
failed,ak:******,err:ak not exist",
"error_code": "APIG.0301",
"request_id": "******"
}
```

Causa posible

La AK utilizada para la autenticación de IAM de la API no existe.

Solución

Compruebe si la AK es correcta.

5.8 ¿Por qué veo el mensaje de error "Incorrect app authentication information" cuando invoco a una API?

Es posible que aparezcan los siguientes errores relacionados con la información de autenticación de aplicaciones:

- **Incorrect app authentication information: app not found, appkey xxx**
- **Incorrect app authentication information: verify signature fail, canonicalRequest**
- **Incorrect app authentication information: signature expired**

Incorrect app authentication information: app not found, appkey xxx

```
{
  "error_msg": "Incorrect app authentication information: app not found, appkey
0117***e5e1",
  "error_code": "APIG.0303",
  "request_id": "a532***5aca"
}
```

Causas posibles

El AppKey es incorrecto.

Solución

Paso 1 En el panel de navegación de la consola de APIG, seleccione **API Management** > **Credentials**.

Paso 2 Haga clic en el nombre de credencial correspondiente para ir a la página de detalles.

Paso 3 Verifique la **Key** y vuelva a configurar el AppKey.

----Fin

Incorrect app authentication information: verify signature fail, canonicalRequest

```
{
  "error_msg": "Incorrect app authentication information: verify signature fail,
canonicalRequest:GET|/test/||host:d7da***3df7.example.com|x-sdk-
date:20230527T015431Z||host;x-sdk-date|e3b0c***52b855",
  "error_code": "APIG.0303",
  "request_id": "cb14***62dc"
}
```

Causas posibles

El algoritmo de firma es incorrecto, y la firma calculada por el cliente es diferente de la calculada por APIG.

Solución

Para más detalles, véase **Incorrect IAM authentication information: verify aksk signature fail**.

Incorrect app authentication information: signature expired

```
{
  "error_msg": "Incorrect app authentication information: signature expired,
signature time:20230527T000431Z,server time:20230527T020608Z",
  "error_code": "APIG.0303",
  "request_id": "fd65***b8ad"

}
```

Causas posibles

La diferencia entre la marca de hora del cliente **x-sdk-date** y el tiempo del servidor APIG supera los 15 minutos.

Solución

Compruebe si la hora del cliente es correcta.

5.9 ¿Por qué la modificación del parámetro backend_timeout no tiene efecto?

Descripción del problema

La modificación del parámetro **backend_timeout** en los gateways no tiene efecto.

Causas posibles

El parámetro **Timeout (ms)** de la página **Define Backend Request** no se modifica.

Solución

Inicie sesión en la consola de APIG, vaya a la página de detalles de la API, haga clic en **Edit** y modifique el parámetro **Timeout (ms)** en la página **Define Backend Request**.

5.10 ¿Tiene APIG un límite en el tamaño del cuerpo de solicitud de API?

Compartido gateway en la consola antigua: APIG reenvía solo las solicitudes de API cuyo cuerpo no supera los 12 MB y rechaza las solicitudes con un cuerpo más grande. En este caso, cargue el cuerpo de la solicitud en Object Storage Service (OBS).

Gateway dedicado: APIG reenvía solo las solicitudes de API cuyo cuerpo no supere los 12 MB. Si su gateway recibirá solicitudes con un cuerpo superior a 12 MB, modifique el parámetro **request_body_size** en la página de detalles del gateway. Este parámetro indica el tamaño máximo permitido del cuerpo de la solicitud. El valor oscila entre 1 MB y 9536 MB.

5.11 ¿Hay un límite en el tamaño de la respuesta a una solicitud de API?

No.

Pero hay un límite en el tamaño del cuerpo de la solicitud. Para obtener más información, véase **request_body_size**.

5.12 ¿Cómo invoco a una API usando la autenticación de aplicaciones en el sistema iOS?

APIG proporciona los SDK y demostraciones en varios idiomas, como Java, Python, C, PHP y Go, para la autenticación de aplicaciones.

Para usar Objective-C (para iOS) u otros idiomas, véase **Autenticación de aplicaciones**.

5.13 ¿Por qué no puedo crear un parámetro de encabezado llamado x-auth-token para una API invocada con la autenticación de IAM?

El parámetro de cabecera **x-auth-token** ya se ha definido en APIG.

Para usar este parámetro para invocar a una API, agregue el parámetro y su valor al encabezado de la solicitud.

5.14 ¿Pueden las aplicaciones móviles invocar a las API?

Sí, las aplicaciones móviles pueden invocar a las API.

En el modo de autenticación de aplicaciones, los AppKey y AppSecret de una aplicación móvil se sustituyen por los del SDK correspondiente para firmar la aplicación.

5.15 ¿Las aplicaciones desplegadas en una VPC pueden invocar a las API?

Sí, las aplicaciones desplegadas en una VPC pueden invocar a las API de forma predeterminada. Si la resolución de nombres de dominio falla, configure un servidor de DNS en el punto de conexión actual siguiendo las instrucciones de **Configuración de un servidor de DNS de intranet**. Después de la configuración, las aplicaciones desplegadas en la VPC pueden invocar a las API.

Configuración de un servidor de DNS de intranet

Para configurar un servidor de DNS, especifique su dirección IP en el archivo **/etc/resolv.conf**.

La dirección IP del servidor de DNS de intranet depende de la región en la que se encuentre. Busque la dirección IP del servidor DNS de la intranet de su región en **direcciones de servidor DNS privado**.

Agregue un servidor de DNS de intranet con cualquiera de los dos métodos siguientes:

- Método 1: Modificar la información de subred de la VPC.
- Método 2: Editar el archivo **/etc/resolv.conf**.

Las configuraciones del servidor de DNS de intranet no son válidas después de reiniciar ECS y el servidor de DNS de intranet debe configurarse de nuevo. Por lo tanto, se recomienda el método 1.

Método 1: Modificar la información de subred de la VPC.

Realice el siguiente procedimiento para agregar una dirección IP de servidor de DNS a las configuraciones de subred del ECS en la VPC.

Paso 1 Haga clic en en la esquina superior izquierda para seleccionar una región.

Paso 2 En la lista de servicios, seleccione **Compute** > **Elastic Cloud Server**.

Paso 3 Haga clic en el nombre del ECS que desea utilizar.

Paso 4 En la pestaña **Network Interfaces**, haga clic en para ver el nombre de la subred.

Paso 5 En la pestaña **Summary**, vea el nombre de la VPC.

Paso 6 Haga clic en el nombre de la VPC para visitar la consola de la VPC.

Paso 7 Elija **Subnets** en el panel de navegación izquierdo.

Paso 8 Localice la subred mencionada en **Paso 4** y haga clic en el nombre de la subred.

Paso 9 Cambie la dirección del servidor de DNS de la subred y haga clic en **OK**.

Por ejemplo, cambie la dirección a **100.125.1.250**.

Paso 10 Reinicie el ECS. Compruebe que el archivo **/etc/resolv.conf** contiene la dirección IP del servidor de DNS que se va a configurar y que la dirección IP es menor que la de todos los demás servidores de DNS.

La siguiente figura muestra la dirección IP **100.125.1.250** del servidor de DNS que se va a configurar.

```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 114.114.115.115
```

La modificación de la información de subred de una VPC afectará a todos los ECS creados con la subred.

----Fin

Método 2: Editar el archivo /etc/resolv.conf.

Agregue la dirección IP del servidor de DNS de intranet al archivo **/etc/resolv.conf**.

Por ejemplo, si se encuentra en **CN-Hong Kong**, agregue un servidor de DNS de intranet con dirección IP **100.125.1.250** al archivo **/etc/resolv.conf**.

- La dirección IP del nuevo servidor de DNS debe ser menor que la de todos los demás servidores de DNS.
- Las configuraciones de DNS tienen efecto inmediatamente después de guardar el archivo **/etc/resolv.conf**.

5.16 ¿APIG admite la transmisión de datos de WebSocket?

Sí.

Al crear una API, puede seleccionar HTTP, HTTPS o HTTP&HTTPS. HTTP es equivalente a WebSocket (ws), y HTTPS es equivalente a WebSocket seguro (wss).

5.17 ¿Cómo se igualarán y ejecutarán las solicitudes de una API con varias políticas de backend?

Si se configuran varias políticas de backend para una API, APIG coincidirá con las políticas de backend en secuencia. Si una solicitud de API coincide con una de las políticas de backend, APIG reenvía inmediatamente la solicitud al backend correspondiente y deja de coincidir.

Si no coincide ninguna política de backend, la solicitud de API se reenvía al servidor de backend predeterminado.

5.18 ¿Cómo puedo acceder a los servicios backend por las redes públicas con APIG?

Habilite **acceso público** para permitir que los servicios externos invoquen a las API.

Si encuentra un problema de red al invocar a las API, véase **¿Cuáles son las posibles causas de un error de invocación a la API?**

6 Autenticación de API

6.1 ¿APIG admite la autenticación bidireccional?

Gateway dedicado: Sí.

- Autenticación bidireccional de frontend: al vincular un nombre de dominio independiente, seleccione un **certificado de SSL** que contenga un certificado CA. Se puede habilitar la autenticación del cliente, es decir, la autenticación bidireccional.
- Autenticación de dos vías de backend: Al crear una API, habilite la autenticación de dos vías para el servicio de backend. Para obtener más información, véase la descripción del parámetro de autenticación bidireccional en **Creación de una API**.

Gateway compartido en la consola antigua: No. Solo se admite la autenticación unidireccional de HTTPS.

6.2 ¿Se firmará el cuerpo de la solicitud?

Sí. El cuerpo de la solicitud es otro elemento que necesita ser firmado además de los parámetros obligatorios del encabezado de la solicitud. Por ejemplo, cuando se llama a una API utilizada para cargar un archivo mediante el método POST, se calcula el valor hash del archivo que se va a cargar para generar una firma.

Para obtener más información sobre las firmas, véase la **descripción del algoritmo de autenticación de firma**.

6.3 Preguntas frecuentes de credenciales de API

¿Cuántas aplicaciones (credenciales) puedo crear?

Puede crear un máximo de 50 aplicaciones (credenciales).

¿Cómo aíslo la información de invocaciones entre los terceros que invocan a la misma API a través de la autenticación de la aplicación?

Cree múltiples aplicaciones (credenciales) para diferentes terceros y vincule las aplicaciones (credenciales) a la misma API.

¿Hay alguna restricción en el número máximo de terceros que pueden invocar a la misma aplicación a través de la autenticación de la aplicación?

Sin restricciones.

¿Necesito crear una aplicación (credencial) para una API para que se pueda invocar con la autenticación de aplicaciones?

Sí, debe crear una aplicación (credencial) y vincularla a la API. Una vez creada la aplicación (credencial), se crean automáticamente una AppKey y una AppSecret. Proporcione AppKey y AppSecret para que terceros invoquen a la API.

¿Cómo se invoca una API por terceros a través de la autenticación de aplicaciones?

Proporcionar a terceros el AppKey y AppSecret de la aplicación que ha creado para acceder a la API. Los terceros pueden usar AppKey y AppSecret para invocar a la API con un SDK. Para obtener más información sobre cómo utilizar un SDK, véase **Invocación a las API con la autenticación de aplicaciones**.

7 Políticas de API

7.1 ¿Puedo configurar el número máximo de solicitudes simultáneas?

No.

- Sin embargo, puede definir el número máximo de invocaciones a la API dentro de un período de tiempo específico.
- Se puede acceder a una sola API durante un máximo de 6,000 veces por segundo. Para obtener más información, véase **Notas y restricciones**.
- El número de invocaciones a la API se puede controlar mediante una política de limitación de solicitudes. Para obtener más información, véase **Configuración de una política de limitación de solicitudes**.

7.2 ¿Se aplica la restricción de solicitudes de 1,000 por día a un nombre de dominio de depuración a las cuentas empresariales?

Sí.

Para obtener detalles sobre el nombre de subdominio (depurar nombre de dominio), véase **Configuración del nombre de dominio para invocar API**.

7.3 ¿Tiene APIG límites de ancho de banda?

El gateway compartido no tiene límites en el ancho de banda. Acelera las solicitudes según las políticas de limitación de solicitudes y limita el tamaño máximo del cuerpo a 12 MB.

Los gateway dedicados tienen límites de ancho de banda. Cuando crea un gateway dedicada, puede establecer el ancho de banda para el acceso público entrante y saliente.

7.4 ¿Por qué no entra en vigor una política de limitación de solicitudes?

- Si la limitación de solicitudes para la API o la dirección IP de origen no tiene efecto, compruebe si la política de limitación de solicitudes está vinculada a la API.
- Si la limitación de solicitudes de usuario no tiene efecto, compruebe si el modo de autenticación de la API es App o IAM.
- Si la limitación de la solicitud de credenciales no tiene efecto, compruebe si la API utiliza la autenticación de aplicaciones.

7.5 ¿Cómo puedo proporcionar una API abierta a los usuarios específicos?

Puede proporcionar una API abierta a usuarios específicos de cualquiera de las siguientes maneras:

- Seleccione la autenticación de la aplicación cuando cree la API y comparta AppKey y AppSecret con los usuarios de destino.
- Configure una política de control de acceso para permitir el acceso desde direcciones IP o nombres de cuenta específicos y vincule la política de control de acceso a la API.

7.6 ¿Se verifican las direcciones IP del cliente para el control de acceso?

No siempre.

En APIG, el control de acceso se basa en el valor de **$remote_addr**. **$remote_addr** indica una dirección IP del cliente y está determinada por el modo de acceso. Si un cliente accede a APIG sin usar ningún proxy, la dirección IP del cliente es **remote_addr**. Si un cliente accede a APIG usando un proxy, el cliente accede primero al proxy y, a continuación, el proxy reenvía la solicitud a APIG. En este caso, **remote_addr** es la dirección IP del proxy.

8 Importación y exportación de API

8.1 ¿Cuáles son las posibles causas de un error de importación de API?

- Posible causa 1: El número de las API excede el límite máximo permitido para una sola importación. Para más API (300), impórtelas por lotes o envía un ticket de servicio para aumentar el límite.
- Posible causa 2: Los parámetros son incorrectos. Compruebe y rectifique los parámetros. Se recomienda crear una API en la consola de APIG, exportarla y luego usarla como plantilla para importar API.
- Posible causa 3: El archivo YAML está en formato incorrecto. Compruebe y modifique el archivo.
- Posible causa 4: La red proxy local tiene restricciones. Cambie el entorno de red.
- Posible causa 5: El encabezado de la solicitud de API contiene **X-Auth-Token**. Quite **X-Auth-Token** del encabezado.

8.2 ¿Hay una plantilla para importar las API con un archivo Swagger?

Se está desarrollando la plantilla.

Actualmente, puede configurar una o dos API en APIG y, a continuación, exportarlas para usarlas como plantillas.

