API Gateway

Preguntas frecuentes

Edición 01

Fecha 2023-10-18

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

Creación de API

- ¿Cómo configuro la dirección de backend si no usaré un canal de VPC (o un canal de balanceo de carga)?
- ¿Cómo puedo configurar la dirección del servicio backend?
- ¿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 API

- ¿Cuáles son las posibles causas de un error de invocación a la API?
- ¿Qué debo hacer si se devuelve un código de error durante las invocaciones a la API?
- ¿Qué debo hacer si se muestra "The API does not exist or has not been published in the environment."?
- ¿Por qué veo el mensaje "No backend available"?
- ¿Cuáles son las posibles causas si se muestra el mensaje "Backend unavailable" o "Backend timeout"?

Autenticación de API

- ¿Admite APIG la autenticación bidireccional de HTTPS?
- ¿Cómo invoco a una API que no requiere autenticación?

Políticas de control 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?
- ¿Cómo puedo excluir una dirección IP específica para la autenticación de identidad de una API?

Importación y exportación de API

2 Creación de API

2.1 ¿Por qué no puedo crear API?

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

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

Las respuestas de API son definidas por los servicios de backend (proveedores de API). API Gateway (APIG) solo transmite respuestas de forma transparente a los llamantes de API.

2.3 ¿Cómo especifico el puerto de host para un canal de VPC (o canal de equilibrio de carga)?

Utilice el puerto del servicio de backend de la API.

2.4 ¿Cómo configuro la dirección de backend si no usaré un canal de VPC (o un canal de balanceo de carga)?

Puede especificar la dirección de backend como un nombre de dominio público o una dirección IP pública, como la Elastic IP (EIP) de un Elastic Cloud Server (ECS).

2.5 ¿Cómo puedo configurar la dirección del servicio backend?

Configure la dirección del servicio backend como una EIP de ECS, o la dirección IP pública o el nombre de dominio de su propio servidor.

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

- No. El gateway compartido solo admite canales de VPC.
- Para los gateway dedicados, puede utilizar direcciones de balanceador de carga de red privada.
- Alternativamente, puede utilizar la EIP vinculada a un balanceador de carga de red pública.

2.7 ¿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, 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 con EIP, **cree un canal de Virtual Private Cloud (VPC)** y asocie los ECS con él.

2.8 ¿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.

2.9 ¿Qué debo hacer después de solicitar un nombre de dominio independiente?

Si utiliza el gateway compartido, agregue un registro de CNAME que apunte el nombre de dominio independiente al nombre de subdominio del grupo de API de destino. Si utiliza un gateway dedicado, agregue un registrode de A que apunte el nombre de dominio independiente a la dirección de acceso entrante del gateway. Puede vincular cinco nombres de dominio independientes a un grupo de API, pero puede vincular cada nombre de dominio independiente solo a un grupo de API.

NOTA

Para usar un nombre de dominio público, agregue un registro de CNAME (gateway compartido) o un registro de A (gateway dedicado) en Domain Name Service (DNS).

Para utilizar un nombre de dominio privado, agregue un registro de CNAME (gateway compartido) o un registro de A (gateway dedicado) en el servicio DNS y asocie el nombre de dominio con la VPC en la que se encuentra su servicio de backend.

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

En el gateway compartido, el nombre de dominio que se va a vincular debe haberse registrado y debe haber los 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 y agregar un registro de A para apuntar el nombre de dominio a la dirección de acceso entrante del gateway.

2.11 ¿Por qué no se puede invocar a una API entre los dominios?

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, actívelo.

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.

NOTA

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 o coincide con la ruta establecida para la API con CORS habilitado.

Matching: Seleccione **Prefix match**.

Authentication Mode: **None** significa que todos los usuarios tendrán acceso. No se recomienda.

CORS: Habilite esta opción.

3 Invocación a API

3.1 ¿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 detalles acerca de cómo crear y usar conexiones de interconexión de VPC, consulte **Descripción de la interconexión de VPC** o **Exposición de servicios de backend entre 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 información, consulte **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, vaya a la página **Gateway Information**, haga clic en la ficha **Configuration Parameters** y modifique el parámetro **ratelimit_api_limits**.

3.2 ¿Qué debo hacer si se devuelve un código de error durante las invocaciones a la API?

Si se devuelve un código de error al invocar a sus propias API, **encuentre la solución en "Códigos de error"**.

Si se devuelve un código de error cuando gestiona sus API, **encuentre la solución en "Códigos de error"**.

3.3 ¿Por qué veo el mensaje de error "414 Request-URI Too Large" cuando invoco a una API?

El 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.

3.4 ¿Qué debo hacer si se muestra "The API does not exist or has not been published in the environment."?

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 el URL de acceso, se producirá un error en la coincidencia del URL en los detalles de la API. Por ejemplo, los 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, consulte **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 entre orígenes (CORS) para la API y cree una nueva API que utilice el método OPTIONS. Para obtener más información, consulte la sección **CORS**.

3.5 ¿Por qué veo el mensaje "No backend available"?

- 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 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.

  NOTA

  Los backends del gateway compartido no admiten la configuración de balanceadores de carga de red privada.

3.6 ¿Cuáles son las posibles causas si se muestra el mensaje "Backend unavailable" o "Backend timeout"?

En la siguiente tabla se enumeran las posibles causas si un servicio de 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 de backend en la definición de la 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.
El URL del servicio de backend es inalcanzable.	Compruebe el URL.

3.7 ¿Por qué veo el mensaje "Backend domain name resolution failed" cuando se invoca a un 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 balanceo 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 balanceo de carga.

a. Cree un canal de equilibrio de carga.

b. Agregue la dirección del servicio backend.

c. Al crear una API, seleccione el canal de balanceo de carga y configure un encabezado personalizado.

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

Descripción del problema

La modificación del parámetro **backend_timeout** en un gateway dedicado 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**.

3.9 ¿Cómo cambio el entorno para las invocaciones a la API?

De forma predeterminada, se invoca a la API en el entorno RELEASE. Si desea invocar a la misma API en otro entorno, agregue el encabezado de solicitud **X-Stage** para especificar el nombre del entorno.

3.10 ¿Cuál es el tamaño máximo de un paquete de solicitud de API?

Gateway compartido: APIG solo reenvía solicitudes de API cuyo cuerpo no sea mayor que 12 MB, y rechaza solicitudes con un cuerpo más grande. Para enviar solicitudes con un cuerpo más grande, 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.

3.11 ¿Cómo realizo 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, consulte **Principio de autenticación de aplicaciones**.

3.12 ¿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.

3.13 Preguntas frecuentes sobre credencial

¿Cuántas credenciales puedo crear?

Puede crear un máximo de 50 credenciales.

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

Cree múltiples credenciales para diferentes terceros y vincule las 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 credencial para una API para que se pueda invocar a través de la autenticación de la aplicación?

Sí, necesita crear una credencial y vincularla a la API. Una vez creada la credencial, se crean automáticamente una AppKey y un 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 usar un SDK, consulte la **Invocación a las API con la autenticación de aplicaciones**.

3.14 ¿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.

3.15 ¿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. Encuentre la dirección IP del servidor de DNS de la intranet en su región a partir de **direcciones de servidor de DNS privadas**.

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**.

  NOTA

  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

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

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda para seleccionar una región.

Paso 3 En la lista de servicios, elija **Compute** > **Elastic Cloud Server**.

Paso 4 Haga clic en el nombre del ECS que desea utilizar.

Paso 5 En la página de detalles de ECS, vea la información de NIC y haga clic en para ver el nombre de subred del ECS.

Paso 6 En la página de información básica de ECS, vea el nombre de la VPC del ECS.

Paso 7 Haga clic en el nombre de la VPC para visitar la consola de la VPC.

Paso 8 Elija **Subnets** en el panel de navegación izquierdo.

Paso 9 Busque la subred mencionada en **Paso 5** y haga clic en el nombre de la subred.

Paso 10 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 11 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
```

NOTA

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

----Fin

Método 2

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**.

NOTA

- 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**.

3.16 ¿Cómo implemento la transmisión de datos de WebSocket?

APIG admite la transmisión de datos de WebSocket. 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).

3.17 ¿APIG admite las conexiones persistentes?

Sí. Pero debes usar las conexiones persistentes correctamente para evitar ocupar demasiados recursos.

3.18 ¿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.

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

No.

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

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

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

4 Autenticación de API

4.1 ¿Admite APIG la autenticación bidireccional de HTTPS?

Gateway dedicado: Sí.

- Autenticación bidireccional frontend: al vincular un nombre de dominio independiente, seleccione un **certificado de SSL** que contenga un certificado de CA. La autenticación de cliente, es decir, la autenticación bidireccional, está habilitada de forma predeterminada.
- 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, consulte la descripción acerca de la **autenticación bidireccional** en **Creación de una API**..

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

4.2 ¿Cómo invoco a una API que no requiere autenticación?

Para invocar a las API que no requieren autenticación, construya solicitudes HTTP estándar y envíelas a APIG.

NOTA

APIG **transmite de forma transparente** solicitudes para invocar a una API que no requiere la autenticación al servicio de backend. Si desea que las solicitudes se autentifiquen en el servicio de backend de la API, puede establecer **Security Authentication** en **None**. El llamante de la API transfiere los campos necesarios para la autenticación al servicio de backend, y el servicio de backend realiza la autenticación.

4.3 ¿Qué versiones de TLS soporta APIG?

APIG soporta TLS 1.1 y TLS 1.2, pero no soporta TLS 1.0 ni TLS 1.3.

4.4 ¿APIG admite la autenticación personalizada?

Sí. Para obtener más información, consulte "Autorizadores personalizados" en la *Guía de usuario de API Gateway*.

4.5 ¿Se firmará el organismo de solicitud para la autenticación de seguridad?

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, consulte **la descripción del algoritmo de autenticación de firma**.

4.6 Errores comunes relacionados con la información de autenticación de IAM

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

Método 1: Ver logs.

Paso 1 Obtener la canonicalRequest calculada por APIG.

Obtenga **request_id** del cuerpo del mensaje de error, busque **error.log** (puede ver este archivo en CLS) del nodo shubao basado en el **request_id** y obtenga **canonicalRequest** de **error.log**.

```
2019/01/26 11:34:27 [error] 1211#0: *76 [lua] responses.lua:170: rewrite():
473a4370fbaf69e42f9da243eb8f8c52;app-1;Incorrect IAM authentication information:
```



```
verify signature fail;SDK-HMAC-SHA256 Access=071fe245-9cf6-4d75-822d-
c29945a1e06a, SignedHeaders=host;x-sdk-date,
Signature=b2ef2cddcef89cbfe22974c988909c1a94b1ac54114c30b8fe083d34a259e0f5;canonic
alRequest:GET
/app1/

host:test.com
x-sdk-date:20190126T033427Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, client:
192.168.0.1, server: shubao, request: "GET /app1 HTTP/1.1", host: "test.com"
```

Paso 2 Obtenener la canonicalRequest calculada por el cliente imprimiendo logs o usando interrupciones de depuración. En la siguiente tabla se describen las funciones utilizadas para calcular la canonicalRequest en los SDK de diferentes idiomas.

Tabla 4-1 Funciones para calcular la canonicalRequest en los SDK de idiomas comunes

Idioma	Función
Java	Función de Sign en com.cloud.sdk.auth.signer.DefaultSigner.class de **libs/java-sdk-core-*.jar**
C	Función sig_sign de **signer.c**
C++	Función Signer::createSignature de **signer.cpp**.
C#	Función de Sign en **signer.cs**
Go	Función de Sign en el **signer.go**
JavaScript	Función de Signer.prototype.Sign de **signer.js**
Python	Función de Sign en el **signer.py**
PHP	Función de Sign en el **signer.php**

Ejemplo: canonicalRequest obtenida en una interrupción de depuración

```
POST
/app1/

host:test.com
x-sdk-date:20190126T033950Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

Paso 3 Compruebe si el canonicalRequest de **Paso 1** es el mismo que el de **Paso 2**.

- Sí: Compruebe si las AK y SK son correctas, por ejemplo, sin espacios.
- No:
  - Diferente en la línea 1: El método de solicitud debe ser el mismo.
  - Diferente en la línea 2: La ruta de la solicitud debe ser la misma.
  - Diferente en la línea 3: Los parámetros de solicitud deben ser los mismos.
  - Diferente en las líneas 4 a 5: El encabezado de solicitud debe ser el mismo en cada línea.

- Diferente en la línea 7: El número de parámetros de cabecera de solicitud debe ser el mismo que el número de líneas de cabecera de solicitud.
- Diferente en la línea 8: El cuerpo de la solicitud debe ser el mismo.

Tabla 4-2 canonicalRequest de APIG y un cliente

N.º de línea	Parámetro	APIG	Cliente
1	Request method	GET	POST
2	Request path	/app1/	/app1/
3	Request parameters	No hay	No hay
4	Request header	host:test.com	host:test.com
5	Request header	x-sdk-date: 20190126T033427Z	x-sdk-date:20190126T033950Z
6	Blank line	-	-
7	Request header parameters	host;x-sdk-date	host;x-sdk-date
8	Request body hash value	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

----Fin

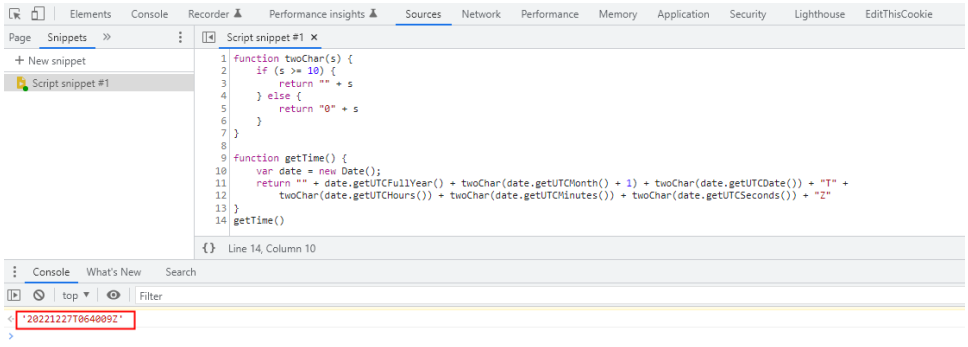
Method 2: Compare the local signature with the obtained one.

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.

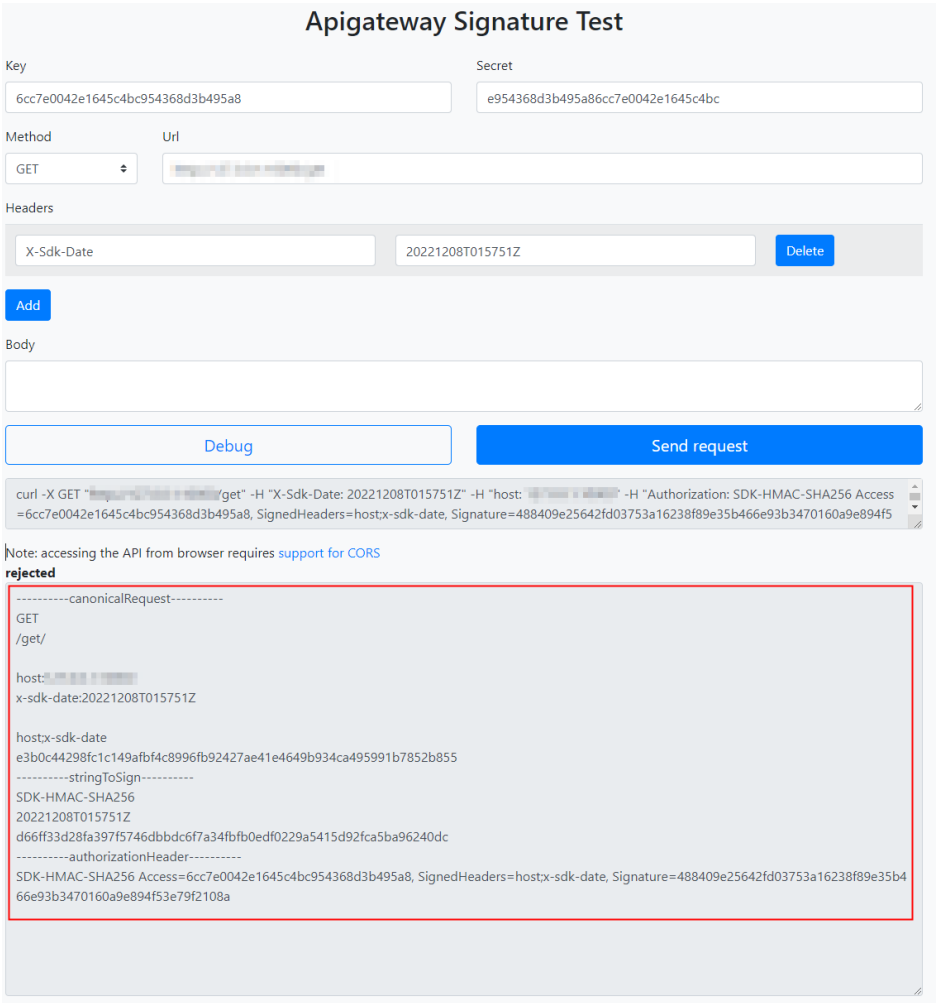
1. Presione **F12** en el teclado y elija **Sources** > **Snippets** > **New snippet**.
2. Copie el siguiente código en el fragmento de script de la derecha, haga clic con el botón derecho en el nombre del fragmento de la izquierda y seleccione **Run** en el menú contextual. El valor que se muestra en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

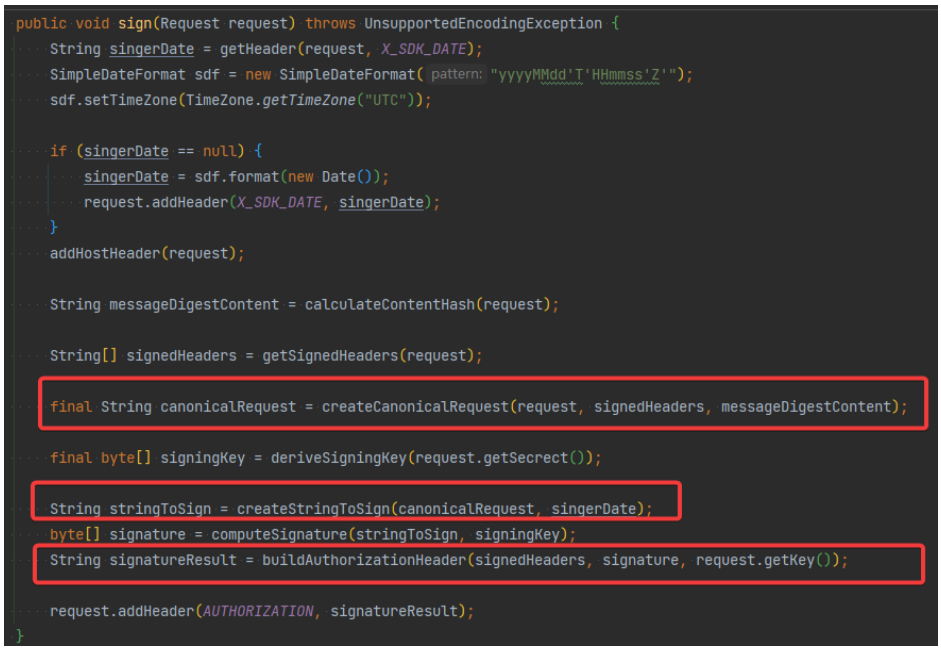
Paso 5 Copie el comando **curl** en la figura de **Paso 4**, ejecútelo en una interfaz de línea de comandos y, a continuación, vaya al siguiente paso.

```
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=6cc7e0042e1645c4bc954368d3b495a8, SignedHeaders=host;x-sdk-date,
Signature=488409e25642fd03753a16238f89e35b466e93b3470160a9e894f53e79f2108a" -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. Resuelva el problema haciendo referencia a **Incorrect IAM authentication information: verify aksk signature fail**.
- Las AK y SK no coinciden.
- 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).
- Se utiliza un token caducado para la autenticación de 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 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 Políticas de control de API

5.1 Limitación de solicitudes

5.1.1 ¿Puedo configurar el número máximo de solicitudes simultáneas?

No, pero puedes limitar el número máximo de invocaciones de API permitidas dentro de un período de tiempo específico.

5.1.2 ¿Se aplica la restricción de 1000 solicitudes a un nombre de subdominio (nombre de dominio de depuración) a cuentas de empresa?

Sí.

5.1.3 ¿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.

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

- El límite de invocación a la API o el límite de solicitud de dirección IP de origen de la política no tiene efecto.

  Compruebe si la política está vinculada a una API.
- El límite de solicitud de usuario de la política no entra en vigor.

  Compruebe si la API vinculada con la política usa la autenticación de aplicación o la de IAM.

- El límite de solicitud de aplicación de la política no entra en vigor.

  Compruebe si la API vinculada con la política usa autenticación credencial.

5.2 Control de acceso

5.2.1 ¿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.

5.2.2 ¿Cómo puedo excluir una dirección IP específica para la autenticación de identidad de una API?

Puede elegir cualquiera de las siguientes soluciones:

- Solución 1: cree una API que no requiera autenticación y configure una política de control de acceso para incluir en la lista blanca la dirección IP.
- Solución 2: cree dos API, una que utiliza la autenticación de IAM o la de aplicación y otra que no requiere autenticación, y configure una política de control de acceso para incluir en la lista blanca la dirección IP de la API que no requiere autenticación.

5.2.3 ¿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.

6 Publicación de API

6.1 ¿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.

6.2 ¿Por qué no se puede acceder a las API publicadas en un entorno que no sea RELEASE?

Para hacer accesible una API publicada en un entorno que no sea RELEASE, agrega el encabezado **x-stage** a la solicitud de API.

Ejemplo:

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

6.3 ¿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.

6.4 ¿Cómo especifico un entorno para la depuración de API?

APIG depura APIs en un entorno de depuración específico. Después de completar la depuración, debe publicar su API en un entorno y usar código o correo para agregar el encabezado **X-Stage** para especificar el entorno donde quiere invocar a la API.

7 Importación y exportación de API

7.1 ¿Por qué falla la 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.

7.2 ¿Proporciona APIG una plantilla para importar API desde los archivos Swagger?

Se está desarrollando la plantilla.

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

8 Seguridad de API

8.1 ¿Cómo puedo proteger mis API?

- Autenticación de identidad

  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/intervalos 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.

8.2 ¿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.

8.3 ¿Puedo controlar el acceso a las direcciones IP privadas de los ECS en un canal de VPC (o canal de equilibrio de carga)?

No.

9 Otras preguntas frecuentes

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

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

Una credencial se refiere a la identidad de una persona que invoca a la API. Después de crear una credencial, el sistema genera automáticamente una AppKey y un AppSecret para autenticar la credencial. Después de publicar una API y asignarla a una credential, el propietario de la credential puede invocar a la API.

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

9.2 ¿Cómo puedo usar APIG?

Puede usar APIG para gestionar e invocar a las API de las siguientes maneras:

- Consola de gestión, una plataforma de gestión de servicios basada en web

  Si ya ha registrado una cuenta, inicie sesión en la consola de gestión, haga clic en  en la esquina superior izquierda y elija **APIG**.

  Para obtener más información sobre las funciones y operaciones de la consola de APIG, consulte la *Guía de usuario de API Gateway*.

- SDK de Java, Go, Python, C#, JavaScript, PHP, C++, C y Android

  Descargue un SDK y utilícelo para invocar a las API. Para obtener más información, consulte la *Guía de desarrollador de API Gateway*.

9.3 ¿Qué idiomas del SDK admite APIG?

APIG admite Java, Go, Python, C#, PHP, JavaScript, C++, C y SDK de Android.

9.4 ¿Puedo cargar archivos con el método POST?

Sí.

APIG reenvía solo las solicitudes de API cuyo cuerpo no supere los 12 MB.

Si utiliza los gateway dedicados, configure el tamaño máximo de cuerpo de solicitud permitido mediante el parámetro **request_body_size**. El valor oscila entre 1 MB y 9536 MB.

NOTA

Actualmente, solo el cuerpo de solicitud puede transmitirse de forma transparente.

9.5 ¿Cómo son los mensajes de error devueltos por APIG?

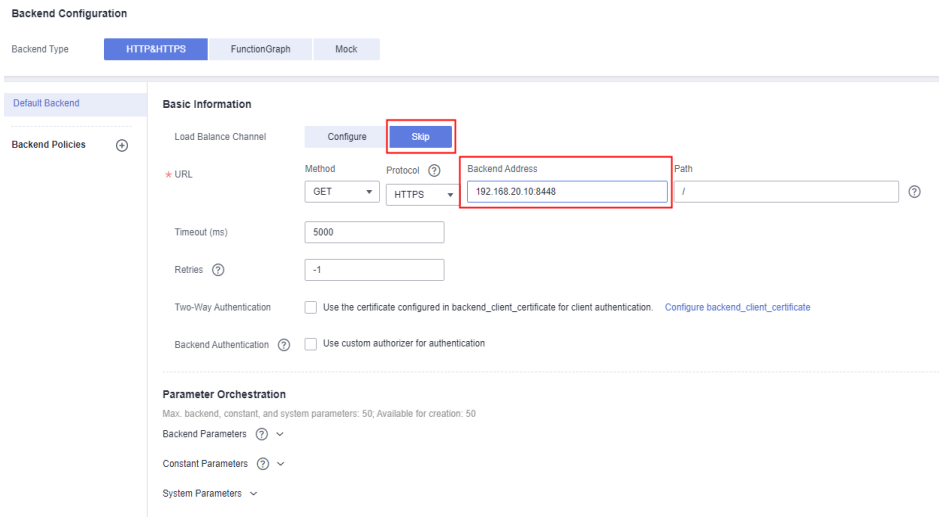
Al recibir una solicitud de API, APIG devuelve una respuesta. Un cuerpo de respuesta similar es el siguiente:

```
{
    "error_code": "APIG.0101",
    "error_msg": "API does not exist or is not published in the environment.",
    "request_id": "acbc548ac6f2a0dbdb9e3518a7c0ff84"
}
```

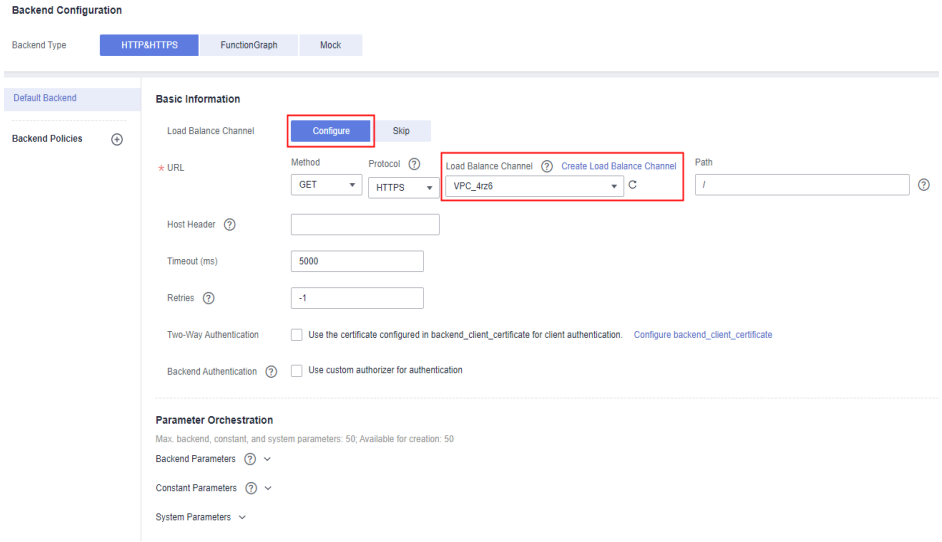
- **"error_code"**: código de error
- **"error_msg"**: descripción del error

9.6 ¿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, consulte **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 y una API de VPC, consulte **Creación de un canal de balanceo de carga** y **Creación de una API**.



9.7 ¿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.

9.8 ¿Por qué no están disponibles todos los botones de la consola de APIG?

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

9.9 ¿Se puede desplegar APIG en un centro de datos local?

No. APIG no se puede desplegar en un centro de datos local.

