API Gateway

Guía del usuario

Edición 01

Fecha 2022-12-27

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

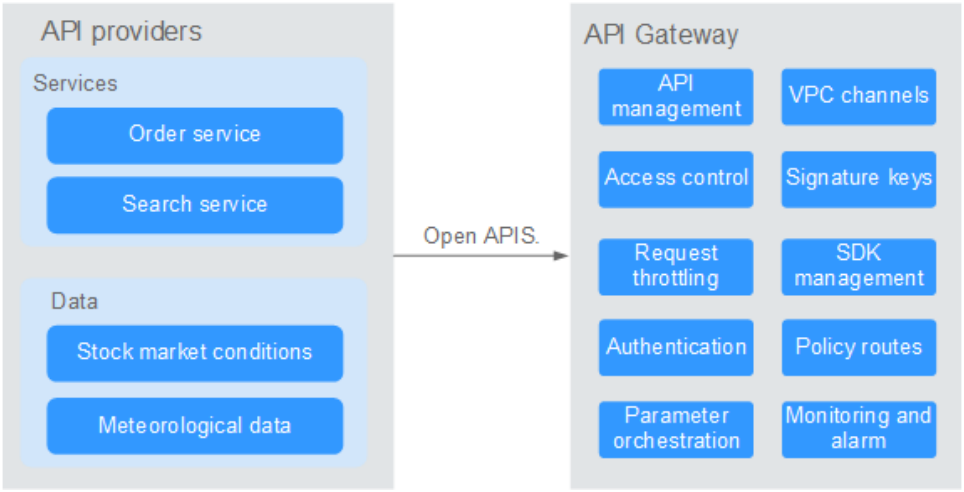
1 Descripción general

API Gateway es un servicio totalmente gestionado que le permite crear, gestionar e implementar API de forma segura a cualquier escala con alto rendimiento y disponibilidad. Con API Gateway, puede integrar fácilmente sus sistemas de servicio internos y exponer selectivamente sus capacidades de servicio a través de sus funciones de apertura y llamada de API.

- **API Opening**

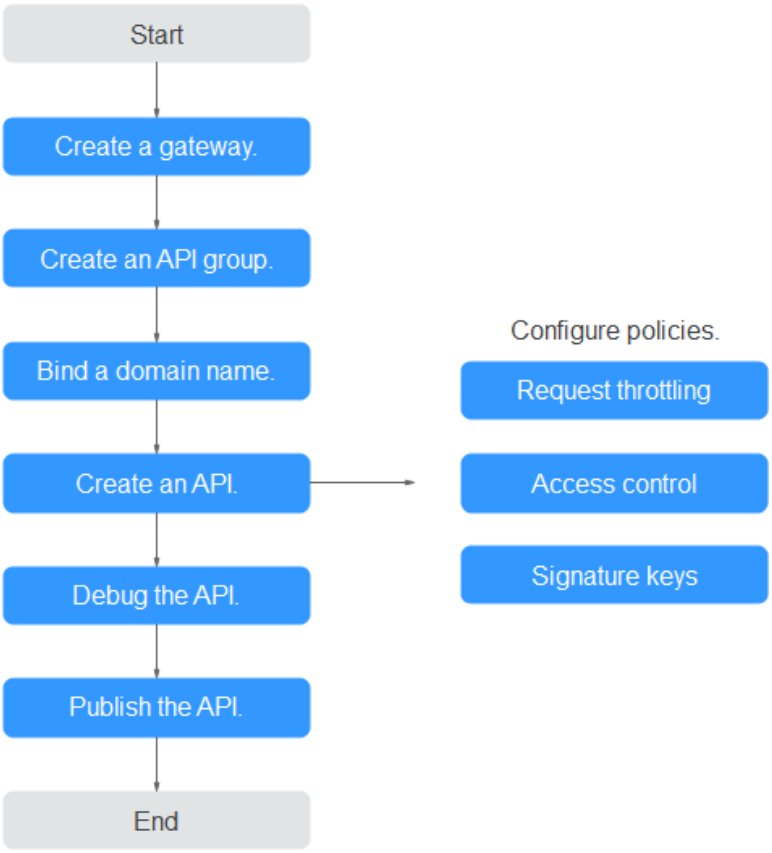
  Empresas y desarrolladores exponen selectivamente sus servicios y datos a través de API Gateway.

  Figura 1-1 API opening



La siguiente figura muestra el proceso de apertura de la API.

Figura 1-2 Proceso de API opening



a. Cree una puerta de enlace.

Compre una puerta de enlace dedicada.

Alternativamente, utilice la **puerta de enlace compartida**.

b. **Cree un grupo de API**.

Cada API pertenece a un grupo de API. Cree un grupo antes de crear una API.

c. **Enlace un nombre de dominio**.

Antes de exponer una API, vincula un nombre de dominio independiente al grupo para que los usuarios puedan acceder a la API.

Puede depurar la API usando el nombre de subdominio predeterminado asignado al grupo al que pertenece la API. El nombre del subdominio se puede llamar un máximo de 1000 veces al día.

d. **Cree una API**.

Encapsular los servicios de backend existentes en RESTful APIs estándar y exponerlos a sistemas externos.

Después de crear una API, configure las siguientes opciones para controlar el acceso a la API:

- **Solicitar limitación**

  Establezca el número máximo de veces que se puede llamar a la API dentro de un período de tiempo para proteger los servicios de backend.

- **Control de acceso**

Establezca una lista de bloqueo o de confianza para denegar o permitir el acceso a la API desde direcciones IP o cuentas específicas.

- **Claves de firma**

  Los servicios de backend utilizan las claves de firma para verificar la identidad de API Gateway y garantizar un acceso seguro.

e. **Depura la API**.

Verifique si la API funciona normalmente.

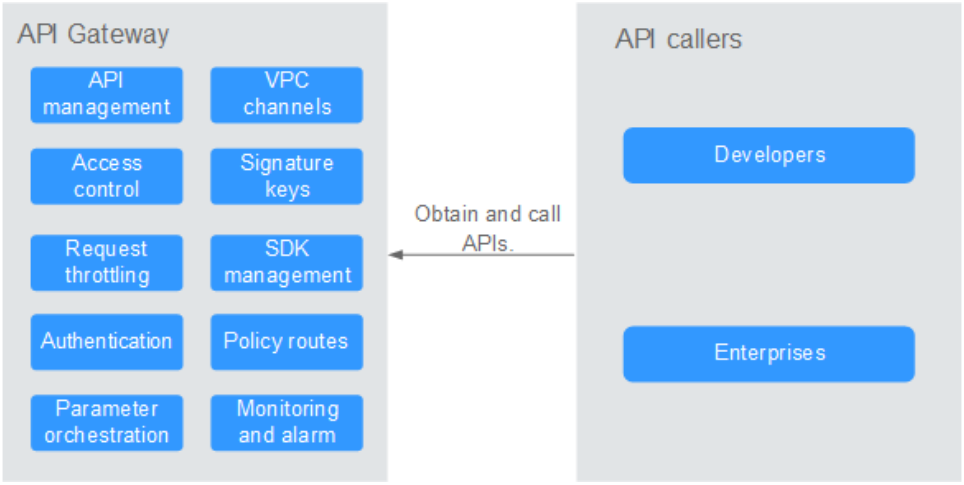
f. **Publicar la API**.

La API solo se puede llamar después de que se haya publicado en un entorno.

- **API calling**

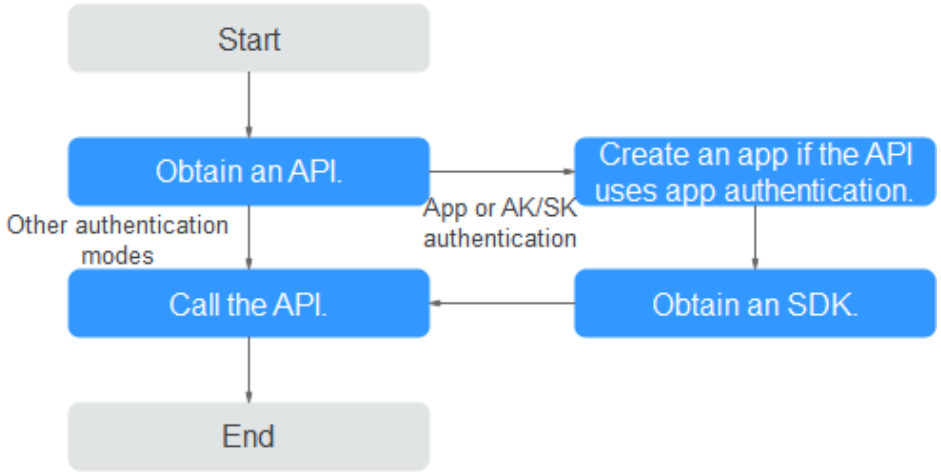
Las empresas y los desarrolladores obtienen y llaman APIs de otros proveedores, reduciendo así el tiempo y los costos de desarrollo.

Figura 1-3 API calling



La siguiente figura muestra el proceso de llamada a la API.

Figura 1-4 Proceso de llamada a la API



a. **Obtener una API**.

Obtenga la información de solicitud de API, incluidos el nombre de dominio, el protocolo, el método, la ruta de acceso y el modo de autenticación.

b. **Crear una aplicación**.

   Para una API que usa autenticación de aplicaciones, cree una aplicación para generar un AppKey y un AppSecret. Enlace la aplicación a la API para que pueda llamar a la API a través de la autenticación de la aplicación.

c. **Obtener un SDK**.

   Utilice el SDK para generar una firma para el AK/SK y llamar a la API.

d. **Llamar a la API**.

   Obtenga la API mediante su dirección de acceso y realice la autenticación en función de su modo de autenticación.

2 Gestión de Gateway

2.1 Compra de una puerta de enlace dedicada

Esta sección describe cómo comprar una puerta de enlace dedicada. Puede crear API y usarlas para proporcionar servicios solo después de crear una puerta de enlace dedicada. Si no tiene requisitos de alto rendimiento, omita esta sección y use la puerta de enlace compartida para **Crear y gestionar APIs**.

Para conocer las diferencias entre las puertas de enlace compartidas y dedicadas, consulte **Especificaciones**.

Información sobre la compra de una puerta de enlace dedicada

Hay algunas limitaciones en la compra de una puerta de enlace dedicada. Si no puede comprar una puerta de enlace dedicada o no se puede crear una puerta de enlace, compruebe los siguientes elementos:

- Cuota de puerta de enlace

  De forma predeterminada, su cuenta se puede utilizar para crear cinco puertas de enlace dedicadas en un proyecto. Para crear más puertas de enlace dedicadas, envíe un ticket de servicio para aumentar la cuota.

- Permisos

  Se deben asignar los roles de **APIG Administrator** y **VPC Administrator** o asignarse la política de **APIG FullAccess** para comprar una puerta de enlace dedicada.

  También se pueden conceder permisos mediante políticas personalizadas. Para más detalles, consulte **Políticas personalizadas de API Gateway**.

- Número de direcciones IP privadas disponibles en la subred

  Las ediciones básica, profesional, empresarial y platino de API Gateway requieren 3, 5, 6 y 7 direcciones IP privadas en una subred, respectivamente. Asegúrese de que la subred que elija tiene suficientes direcciones IP privadas en la consola de Virtual Private Cloud (VPC).

Entorno de red

- VPC

Las puertas de enlace dedicadas se implementan en las VPC. Los recursos en la nube, como Elastic Cloud Servers (ECSs), en la misma VPC pueden llamar a las API mediante la dirección IP privada de la puerta de enlace dedicada implementada en la VPC.

Se recomienda implementar sus puertas de enlace dedicadas en la misma VPC que sus otros servicios para facilitar la configuración de la red y el acceso seguro a la red.

NOTA

Las VPC de las puertas de enlace dedicadas no se pueden modificar.

- EIP

  Para permitir el acceso público entrante a las API desplegadas en una puerta de enlace dedicada, compre una IP elástica (EIP) y vincúlela a la puerta de enlace dedicada.

  NOTA

  Para las API cuyos servicios de backend se implementan en una red pública, API Gateway genera automáticamente una dirección IP para el acceso público saliente y no es necesario comprar un EIP.

- Grupo de seguridad

  Similar a un firewall, un grupo de seguridad controla el acceso a una pasarela a través de un puerto específico y la transmisión de datos de comunicación desde la pasarela a una dirección de destino específica. Por motivos de seguridad, cree reglas de entrada para el grupo de seguridad para permitir el acceso solo en puertos específicos.

  El grupo de seguridad vinculado a una puerta de enlace dedicada debe cumplir los siguientes requisitos:

  – Acceso entrante: Para permitir el acceso a las API de la puerta de enlace dedicada a través de redes públicas o desde otros grupos de seguridad, agregue reglas entrantes para el grupo de seguridad para permitir el acceso en los puertos 80 (HTTP) y 443 (HTTPS).
  – Acceso saliente: si el servicio backend de una API se implementa en una red pública o en otro grupo de seguridad, agregue reglas salientes para el grupo de seguridad para permitir el acceso a la dirección del servicio backend a través del puerto de llamada a la API.
  – Si los servicios front-end y back-end de una API están vinculados con el mismo grupo de seguridad y VPC que la puerta de enlace dedicada, no se necesitan reglas entrantes o salientes para permitir el acceso a través de los puertos anteriores.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**.

Paso 5 Haga clic en **Buy Dedicated Gateway**.

Tabla 2-1 Parámetros para crear una puerta de enlace dedicada

Parámetro	Descripción
Billing Mode	Modo de facturación de la puerta de enlace dedicada. Actualmente, solo se admite la facturación de pago por uso.
Region	Un área geográfica donde se desplegará la puerta de enlace. Implemente la puerta de enlace en la misma región que los otros servicios para permitir que todos los servicios se comuniquen entre sí a través de subredes dentro de una VPC. Esto reduce los costos de ancho de banda público y la latencia de la red.
AZ	Una región física en la que los recursos utilizan redes y fuentes de alimentación independientes. Las zonas de disponibilidad (AZs) están físicamente aisladas pero interconectadas a través de una red interna. Para mejorar la disponibilidad de la puerta de enlace, implemente la puerta de enlace en varias Zonas de disponibilidad.
Gateway Name	Nombre de la puerta de enlace.
Edition	Las ediciones básicas, profesionales, empresariales y platino están disponibles. El número de solicitudes simultáneas permitidas varía dependiendo de la edición de la puerta de enlace. Para obtener más información, consulte **Especificaciones**.
Scheduled Maintenance	Período de tiempo en el que se puede mantener la puerta de enlace. El personal de soporte técnico se pondrá en contacto con usted antes del mantenimiento. Seleccione un período de tiempo con demandas de servicio bajas.
Enterprise Project	Seleccione un proyecto de empresa al que pertenece la puerta de enlace dedicada. Este parámetro solo está disponible si su cuenta es una cuenta de empresa. Para obtener más información sobre el uso de recursos, la migración y los permisos de usuario de proyectos de empresa, consulte **Guía de usuario de gestión de empresa**.

Parámetro	Descripción
Public Inbound Access	Determine si permite que los servicios externos que utilizan un EIP llamen a las API creadas en la puerta de enlace dedicada. Para habilitar esta función, asigne un EIP a la puerta de enlace dedicada. Tendrá que **pagar** por usar el EIP. Las API en la puerta de enlace dedicada se pueden llamar usando nombres de dominio independientes o nombres de subdominio. Existe una limitación en el número de veces que se pueden llamar a las API de un grupo de API por día usando el nombre de subdominio. Para superar la limitación, vincular nombres de dominio independientes al grupo de API y asegurarse de que los nombres de dominio independientes ya han sido CNAMEd al EIP de la puerta de enlace dedicada a la que pertenece el grupo de API. Por ejemplo, tiene una API HTTPS (ruta: **/apidemo**) con acceso público habilitado. La API se puede llamar usando "**https://***{domain}*/**apidemo**", donde *domain* indica un nombre de dominio independiente enlazado al grupo API al que pertenece la API. El nombre de dominio independiente ya debe haber sido CNAMEd al EIP de la puerta de enlace dedicada. El puerto predeterminado es 443.
Public Outbound Access	Determine si desea permitir que los servicios de backend de las API creadas en la puerta de enlace dedicada se implementen en redes públicas. Si habilita esta opción, establezca un ancho de banda que cumpla con sus requisitos de servicio. El ancho de banda oscila entre 1 y 2000 Mbit/s y se facturará por hora según el precio del servicio EIP.
IPv6	**Este parámetro solo está disponible cuando se establece el modo de facturación en Pago por uso.** Si el servicio backend de una API se implementa en una red pública y solo se puede acceder mediante una dirección IPv6, seleccione **IPv6 Access**. **NOTA** Esta función solo está disponible en ciertas regiones.
Network	Seleccione una VPC y una subred para la puerta de enlace dedicada. Los recursos de la nube (como los ECS) dentro de la misma VPC pueden llamar a las API mediante la dirección IP privada de la puerta de enlace dedicada. Implemente la puerta de enlace dedicada en la misma VPC que sus otros servicios para facilitar la configuración de la red y el acceso seguro a la red.
Security Group	Seleccione un grupo de seguridad para controlar el acceso entrante y saliente. Si el servicio de backend de una API se implementa en una red externa, configure las reglas de grupo de seguridad para permitir el acceso a la dirección de servicio de backend a través del puerto de llamada de API. **NOTA** Si el acceso público entrante está habilitado, agregue reglas entrantes para el grupo de seguridad para permitir el acceso en los puertos 80 (HTTP) y 443 (HTTPS).

Parámetro	Descripción
Description	Descripción de la puerta de enlace.

Paso 6 Haga clic en **Next**.

Paso 7 Compruebe la configuración de la puerta de enlace, lea y confirme su aceptación del acuerdo del cliente y la declaración de privacidad, y haga clic en **Pay Now**. El progreso de la creación de la puerta de enlace se muestra en la pantalla.

Si establece el modo de facturación en **Yearly/monthly**, la puerta de enlace dedicada solo se creará después de realizar el pago.

----Fin

Operaciones de seguimiento

Una vez creada la puerta de enlace, puede crear y gestionar APIs en la consola de la puerta de enlace. La página **Gateway Information** muestra los detalles de la puerta de enlace, las configuraciones de red, los recursos de API y las métricas.

Puede modificar el nombre de la puerta de enlace, la descripción, la ventana de tiempo de mantenimiento programado, el grupo de seguridad y el EIP.

Cambio del modo de facturación de una puerta de enlace dedicada

Puede cambiar el modo de facturación de las puertas de enlace dedicadas de **yearly/monthly** a **pay-per-use** o de **pay-per-use** a **yearly/monthly**. El modo de facturación se puede cambiar de anual/mensual a pago por uso solo cuando las suscripciones de la puerta de enlace hayan caducado.

Paso 1 En el panel de navegación, elija **Dedicated Gateways**.

Paso 2 Haga clic en **More** junto a la puerta de enlace de destino y haga clic en **Change to Yearly/Monthly** o **Change to Pay-per-Use**.

- Cambiar a anual/mensual: Seleccione una duración de renovación y haga clic en **Pay**.
- Cambiar a pago por uso: haga clic en **Change to Pay-per-Use** antes de que caduque la suscripción de la puerta de enlace o durante el período congelado después de que caduque. El cambio entra en vigor solo después de que la suscripción haya caducado.

----Fin

2.2 Modificación de una Gateway dedicada

Puede modificar la información básica y los parámetros de configuración de las puertas de enlace dedicadas.

Modificación de información básica

Para modificar la información básica sobre una puerta de enlace dedicada, haga lo siguiente:

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**.

Paso 5 Haga clic en **Access Console** en la esquina superior derecha de la puerta de enlace dedicada que desea modificar.

Paso 6 En la página de pestaña **Basic Information**, modifique la información básica.

Tabla 2-2 Información básica sobre una puerta de enlace dedicada

Parámetro	Descripción
Gateway Name	Nombre de la puerta de enlace.
Description	Descripción de la puerta de enlace.
Scheduled Maintenance	Periodo de tiempo en que la pasarela puede ser mantenida por el personal de soporte técnico. El personal de soporte técnico se pondrá en contacto con usted si se va a realizar alguna actividad de mantenimiento durante la ventana. Seleccione un período de tiempo con demandas de servicio bajas.
Security Group	Seleccione un grupo de seguridad para controlar el acceso entrante y saliente. Si el servicio de backend de una API se implementa en una red externa, configure las reglas de grupo de seguridad para permitir el acceso a la dirección de servicio de backend a través del puerto de llamada de API. **NOTA** ● Si cambia el grupo de seguridad, el nuevo grupo de seguridad debe cumplir los requisitos para llamar a las API incluidas en la puerta de enlace dedicada y acceder a los servicios de backend de estas API. ● Si el acceso público entrante está habilitado, agregue reglas entrantes para el grupo de seguridad para permitir el acceso en los puertos 80 (HTTP) y 443 (HTTPS).

Parámetro	Descripción
EIP	Determine si permite que los servicios externos que utilizan un EIP llamen a las API creadas en la puerta de enlace dedicada. Para habilitar esta función, asigne un EIP a la puerta de enlace dedicada. Tendrá que **pagar** por usar el EIP. Las API en la puerta de enlace dedicada se pueden llamar usando nombres de dominio independientes o nombres de subdominio. Existe una limitación en el número de veces que se pueden llamar a las API de un grupo de API por día usando el nombre de subdominio. Para superar la limitación, vincular nombres de dominio independientes al grupo de API y asegurarse de que los nombres de dominio independientes ya han sido CNAMEd al EIP de la puerta de enlace dedicada a la que pertenece el grupo de API.
Outbound Access	Determine si desea permitir que los servicios de backend de API se implementen en redes públicas y se acceda a ellos mediante la dirección IP generada automáticamente por API Gateway. Puede habilitar o deshabilitar el acceso saliente en cualquier momento.
Bandwidth	El ancho de banda se factura por hora en función de la tarifa del servicio EIP.
Routes	Configure rutas en sus instalaciones si la subred de su centro de datos se encuentra dentro de los siguientes tres segmentos: 10.0.0.0/8-24, 172.16.0.0/12-24 y 192.168.0.0/16-24.

----Fin

Modificación de parámetros de configuración

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**.

Paso 5 Haga clic en **Access Console** en la esquina superior derecha de la puerta de enlace dedicada que desea modificar.

Paso 6 Haga clic en la pestaña **Configuration Parameters** y haga clic en **Edit** en la fila que contiene el parámetro que desea modificar.

Tabla 2-3 Parámetros de configuración

Nombre del parámetro	Descripción
ratelimit_api_limits	Valor de limitación de solicitud predeterminado aplicado a todas las API. El número total de veces que se puede llamar a una API está determinado por este parámetro solo si no hay ninguna política de limitación de solicitud está vinculada a la API. The **Max.** Las **Max.API Requests** de una política de limitación de solicitudes no pueden superar el valor de este parámetro.
request_body_size	El tamaño máximo de cuerpo permitido para una solicitud de API.
backend_timeout	Tiempo de espera de respuesta de backend. Rango de valores: 1 ms a 600,000 ms.
app_token	Determine si desea habilitar la autenticación de app_token. Si habilita esta función, se puede agregar un access_token a la solicitud de autenticación de la API. ● **app_token_expire_time**: el período de validez de un access_token. Se debe obtener un nuevo access_token antes de que caduque el access_token original. ● **refresh_token_expire_time**: el período de validez de un update_token. Un refresh_token se usa para obtener un nuevo access_token. ● **app_token_uri**: el URI utilizado para obtener un access_token. ● **app_token_key**: la clave de encriptación de un token de acceso.
app_basic	Determine si desea habilitar la autenticación app_basic. Una vez activada esta opción, los usuarios pueden agregar el parámetro de encabezado **Authorization** y establecer el valor del parámetro en "Basic + base64 (*appkey* + : + *appsecret*)", en el que *appkey* y *appsecret* son la clave y el secreto de una aplicación o el AppKey y AppSecret de un cliente.
app_secret	Determine si desea habilitar la autenticación de app_secret. Si habilita esta función, los parámetros **X-HW-ID** y **X-HW-AppKey** se pueden agregar a la solicitud de API para llevar la clave y el secreto de una aplicación (el AppKey y el AppSecret de un cliente) para la autenticación. Si desea habilitar la autenticación de app_secret, la autenticación de app_api_key debe estar deshabilitada.
app_route	Determine si admite el acceso a la API basado en direcciones IP. Si habilita esta función, las API que usan autenticación de aplicaciones en cualquier grupo, excepto **DEFAULT**, pueden llamarse mediante direcciones IP.

Nombre del parámetro	Descripción
backend_client_certificate	Determine si desea habilitar la autenticación bidireccional de back-end. Si habilita esta función, puede configurar la autenticación bidireccional para un backend al crear una API.
ssl_ciphers	Conjunto de cifrado de HTTPS compatibles. Seleccione conjunto de cifrado que cumplan con sus requisitos.
real_ip_from_xff	Determine si desea utilizar las direcciones IP en el encabezado **X-Forwarded-For** para el control de acceso y la limitación de solicitudes. **xff_index**: Número de secuencia de una dirección IP en el encabezado **X-Forwarded-For**. El valor puede ser positivo, negativo o 0. ● Si el valor es 0 o positivo, se obtendrá la dirección IP del índice correspondiente en el encabezado **X-Forwarded-For**. ● Si el valor es negativo, se obtendrá la dirección IP de la secuencia inversa indicada en el encabezado **X-Forwarded-For**. Por ejemplo, supongamos que el encabezado **X-Forwarded-For** de una solicitud recibida por API gateway contiene tres direcciones IP: IP1, IP2 e IP3. Si el valor de **xff_index** es 0, se obtiene IP1. Si el valor es 1, se obtiene IP2. Si el valor es –1, se obtiene IP3. Si el valor es –2, se obtiene IP2.
vpc_name_modifiable	Determine si se pueden modificar los nombres de los canales de balanceo de carga. **AVISO** Si esta opción está habilitada, los canales de equilibrio de carga de la puerta de enlace actual no se pueden administrar mediante API de gestión de canales de equilibrio de carga a nivel de proyecto.
api_prom_metrics	Determine si desea habilitar la interfaz de métricas de Prometheus. Si esta opción está habilitada, puede usar **https://**<*Gateway component IP*>**:1026/metrics** para recopilar estadísticas de llamadas API en formato Prometheus.
app_jwt_enable	Determine si desea habilitar la autenticación app_jwt. Si esta opción está habilitada, los parámetros **Authorization** y **Timestamp** se pueden agregar a las solicitudes de API para llevar la clave y el secreto (o AppKey y AppSecret de un cliente) y una marca de tiempo para la autenticación. **app_jwt_auth_header** es un encabezado incluido en las solicitudes de API para la autenticación app_jwt. El valor predeterminado del encabezado es **Authorization**.

Nombre del parámetro	Descripción
public_key_enable	Determine si desea habilitar la autenticación de public_key. **public_key_uri_prefix** indica el prefijo del URI usado para obtener el secreto de public_key. El formato URI es el siguiente: **https://***{VPC access address}{public_key_uri_prefix}{public_key name}*.

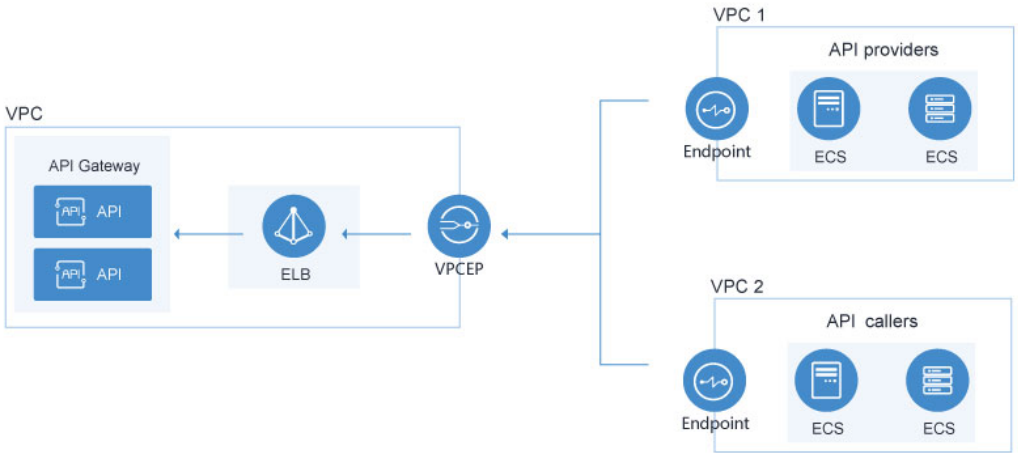
----Fin

2.3 Managing VPC Endpoints

VPC endpoints are secure and private channels for connecting VPCs to VPC endpoint services.

APIs can be exposed and accessed across VPCs in the same region of the same cloud.

Figura 2-1 Cross-VPC access in the same region



Prerequisites

You have enabled ELB-based load balancing for your gateway.

Procedure

Paso 1 Log in to the management console.

Paso 2 Click in the upper left corner and select a region.

Paso 3 Click in the upper left corner and choose **API Gateway**.

Paso 4 In the navigation pane, choose **Dedicated Gateways**.

Paso 5 Click **Access Console** next to a gateway or click the gateway name.

Paso 6 Click **VPC Endpoints** to view details. For details, see .

Tabla 2-4 VPC endpoint information

Parameter	Description
VPC Endpoint Service	Name of the VPC endpoint service. If you enabled ELB-based load balancing when purchasing the gateway, a VPC endpoint service is automatically created and the gateway can be accessed using a VPC endpoint.
Connections	VPC endpoints connected to the gateway. By default, the endpoints are connected to the VPC you selected when purchasing the gateway. ● **VPC Endpoint ID**: ID of a VPC endpoint. ● **Packet ID**: identifier of the VPC endpoint ID. ● **Status**: status of the VPC endpoint. For details about VPC endpoint statuses, see ● **Owner**: of the VPC endpoint creator. ● **Created**: time when the VPC endpoint is created. ● **Operation**: whether to allow the VPC endpoint to connect to the VPC endpoint service. Accept or reject connection from the VPC endpoint to the VPC endpoint service. **AVISO** Once you reject the connection, services that run using the connection may be affected. Exercise caution.
Permissions	Specify accounts allowed to access using the VPC endpoints by adding the account IDs to the whitelist. Click **Add Account** and enter an . ● **Account ID**: ID of an account allowed to access using the VPC endpoints. ● **Created**: time when the whitelist is created. ● **Operation**: Manage access of the account from VPC endpoints. To forbid access of the account, remove it from the whitelist.

----Fin

2.4 Acceso a la puerta de enlace compartida

La puerta de enlace compartida está disponible de inmediato y se puede utilizar directamente.

NOTA

Se ha eliminado la función de puerta de enlace compartida. Utilice puertas de enlace dedicadas en su lugar.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Shared Gateway**.

----Fin

3 API Opening

3.1 Gestión de grupo API

3.1.1 Creación de un grupo de API

Escenario

Antes de crear una API, debe crear un grupo de API. Un grupo de API contiene diferentes API utilizadas para el mismo servicio.

NOTA

Cada API solo puede pertenecer a un grupo de API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **API Groups**.

Paso 6 Haga clic en **Create API Group**, y establezca los parámetros descritos en **Tabla 3-1**.

Tabla 3-1 Parámetros para crear un grupo de API

Parámetro	Descripción
Name	Nombre del grupo API.
Description	Descripción del grupo API.

Paso 7 Haga clic en **OK**.

Después de crear el grupo de API, se muestra en la lista de grupos de API.

NOTA

- El sistema asigna automáticamente un nombre de subdominio al grupo API para realizar pruebas internas. Se puede acceder al nombre del subdominio 1000 veces al día.
- Un grupo de API predeterminado se genera automáticamente para cada puerta de enlace dedicada. Las API en el grupo predeterminado se pueden llamar usando la dirección IP de la VPC donde se implementa la puerta de enlace dedicada.
- Se puede acceder a las API creadas en la puerta de enlace compartida a través de redes públicas mediante el nombre de subdominio del grupo al que pertenecen las API. En una puerta de enlace dedicada, el nombre de subdominio de cada grupo de API debe resolverse en un servidor en la misma VPC que la puerta de enlace. Si desea resolver el nombre de subdominio a una red pública, enlace un EIP a la puerta de enlace.
- Para que sus API estén disponibles para que los usuarios accedan, vincula nombres de dominio independientes al grupo de API al que pertenecen las API.

----Fin

Creación de un grupo de API mediante llamada a una API

También puede crear un grupo de API mediante llamada a una API proporcionada por API Gateway. Para obtener más información, consulta **Creación de un grupo de API**.

Operaciones de seguimiento

Después de crear el grupo de API, enlace nombres de dominio independientes para que los llamantes de API puedan usar los nombres de dominio para llamar a las API del grupo. Para obtener más información, consulte **Vinculación de un nombre de dominio**.

3.1.2 Vinculación de un nombre de dominio

Escenario

Antes de abrir una API, debe vincular uno o más nombres de dominio independientes al grupo al que pertenece la API. Si no hay nombres de dominio enlazados al grupo, se llamará a la API usando el nombre de subdominio predeterminado del grupo y solo se podrá llamar 1000 veces al día.

NOTA

- En una puerta de enlace dedicada o en la puerta de enlace compartida, no puede vincular el mismo nombre de dominio independiente a diferentes grupos de API.

Tenga en cuenta los siguientes puntos antes de vincular un nombre de dominio:

- Nombre de subdominio: Después de crear un grupo API, el sistema le asigna automáticamente un nombre de subdominio único para realizar pruebas internas. Se puede acceder al nombre del subdominio 1000 veces al día, pero no se puede modificar.
- Nombre de dominio independiente: Un nombre de dominio independiente es un nombre de dominio personalizado utilizado para que los llamantes de API llamen a las API abiertas en el grupo al que está enlazado el nombre de dominio.

Prerrequisitos

1. Hay un nombre de dominio independiente disponible.
2. Puerta de enlace compartida: Un registro CNAME apunta el nombre de dominio independiente al nombre de subdominio del grupo API. Para obtener más información, consulte **Adición de un conjunto de registros CNAME**.

   Puerta de enlace dedicada: Un registro A apunta el nombre de dominio independiente a la dirección de la puerta de enlace. Para obtener más información, consulte **Adición de un conjunto de registro**.
3. Si el grupo de API contiene API que se llaman a través de HTTPS, es necesario que haya **certificados de SSL** configurados para el nombre de dominio independiente. Los certificados SSL solo se pueden agregar manualmente con un nombre personalizado, contenido y una clave.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **API Groups**.

Paso 6 Vaya a la página de pestaña **Domain Names** utilizando uno de los métodos siguientes:

- Haga clic en el nombre del grupo de API de destino y haga clic en la pestaña **Domain Names** en la página de detalles del grupo de API que se muestra.
- En la columna **Operation** del grupo API de destino, elija **More** > **Manage Domain Name**.

Paso 7 Haga clic en **Bind Independent Domain Name** e introduzca un nombre de dominio.

Para los grupos de API creados con puertas de enlace dedicadas, especifique la versión mínima de TLS (TLS 1.1 o TLS 1.2) que admiten los nombres de dominio que enlaza a los grupos de API. Se recomienda TLS 1.2.

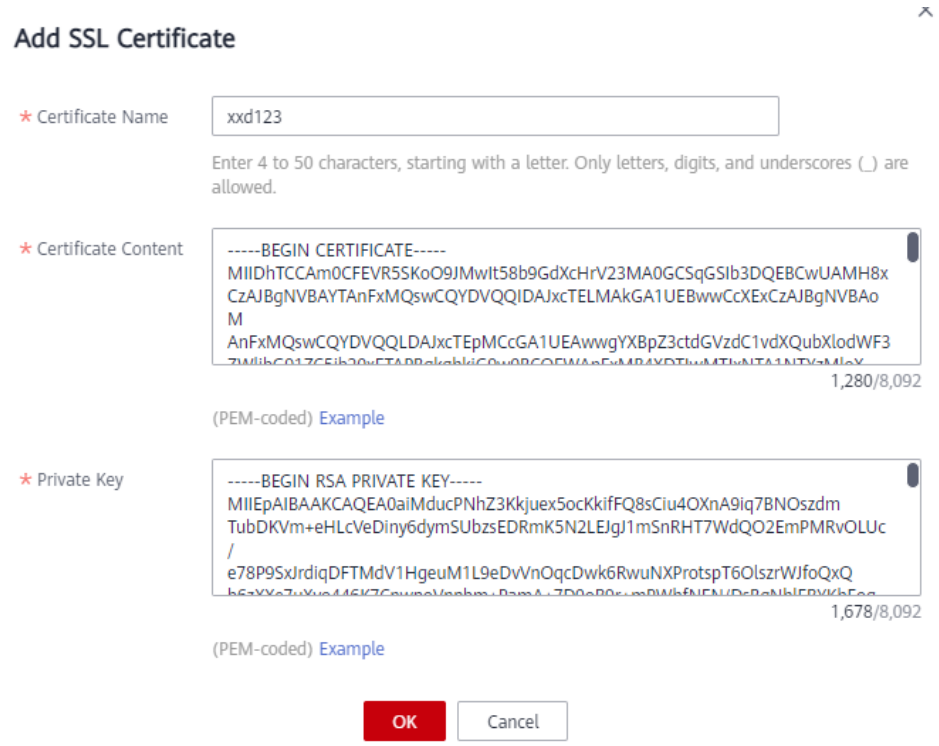
Paso 8 Haga clic en **OK**.

Si el nombre de dominio no es necesario, haga clic en **Unbind** para desvincularlo del grupo de API.

Paso 9 (Opcional) Si el grupo de API contiene API a las que se accede a través de HTTPS, agregue un certificado SSL.

1. Haga clic en **Add SSL Certificate**.
2. Introduzca el nombre, el contenido y la clave del **certificado SSL obtenido**, y haga clic en **OK**.

Figura 3-1 Adición de un certificado SSL



NOTA

- Actualmente, solo puede agregar certificados SSL en formato PEM. Para agregar certificados SSL de otros formatos, convierta primero los certificados al formato PEM.
- Para reemplazar o editar un certificado SSL, haga clic en junto al nombre del certificado. El contenido y la clave del certificado no serán visibles después de hacer clic en **OK** para agregar el certificado. Si el contenido se ha actualizado, agregue todo el contenido o la clave de nuevo.
- Si no necesita un certificado SSL, haga clic en **Delete SSL Certificate** en la fila que contiene el certificado para eliminarlo.

----Fin

Vinculación deun nombre de dominio llamando a una API

También puede vincular un nombre de dominio independiente a un grupo de API llamando a una API proporcionada por API Gateway. Para obtener más información, consulte las siguientes referencias:

Vinculación de un nombre de dominio

Adición de un certificado a un nombre de dominio

Resolución de problemas

- Error al vincular un nombre de dominio independiente: El nombre de dominio independiente no está CNAMEd con el nombre de subdominio del grupo API, o el nombre de dominio independiente ya existe.
- Error al agregar un certificado SSL: El nombre de dominio del certificado SSL es diferente del nombre de dominio para el que se agrega el certificado SSL.

Operaciones de seguimiento

Después de vincular nombres de dominio independientes al grupo API, cree API en el grupo para exponer selectivamente las capacidades de backend. Para más detalles, consulte **Creación de una API**.

3.1.3 Eliminación de un grupo de API

Escenario

Puede eliminar un grupo de API si no lo necesita.

NOTA

Los grupos de API que contienen API no se pueden eliminar.

Prerrequisitos

Ha creado un grupo de API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **API Groups**.

Paso 6 Eliminar un grupo de API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** del grupo API de destino, elija **More** > **Delete**.
- Haz clic en el nombre del grupo de API de destino y haz clic en **Delete Group** en la esquina superior derecha de la página de detalles del grupo de API que se muestra.

Paso 7 Escriba **DELETE** y haga clic en **Yes**.

----Fin

Eliminación de un grupo de API llamando a una API

También puede eliminar un grupo de API llamando a una API proporcionada por API Gateway. Para obtener más información, consulta **Eliminación de un grupo de API**.

3.1.4 Adición de una respuesta de puerta de enlace

Escenario

Se muestra una respuesta de gateway si API Gateway no puede procesar una solicitud de API. API Gateway proporciona un conjunto de respuestas predeterminadas y también le permite crear respuestas de gateway con códigos de estado y contenido personalizados, en la página **API Groups**. El contenido de la respuesta debe estar en formato JSON.

Por ejemplo, el contenido de una respuesta de puerta de enlace predeterminada es el siguiente:

```
{"error_code": "$context.error.code", "error_msg": "$context.error.message",
"request_id": "$context.requestId"}
```

Puede agregar una respuesta con el siguiente contenido:

```
{"errorcode": "$context.error.code", "errormsg": "$context.error.message",
"requestid": "$context.requestId","apiId":"$context.apiId"}
```

Puede agregar más campos o eliminar campos existentes del cuerpo de JSON.

NOTA

- Las respuestas predeterminadas de la puerta de enlace proporcionadas por API Gateway se pueden editar.
- Puede crear respuestas de puerta de enlace y configurar diferentes respuestas para las API en el mismo grupo de API.
- No se puede cambiar el tipo de respuesta de puerta de enlace. Para más detalles, consulte **Tipos de respuesta**.
- Las respuestas de la puerta de enlace pueden contener las variables de contexto de la puerta de enlace de la API (comenzando con **$context**). Para más detalles, consulte **Variables de contexto de API Gateway**.

Prerrequisitos

Ha creado un grupo de API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

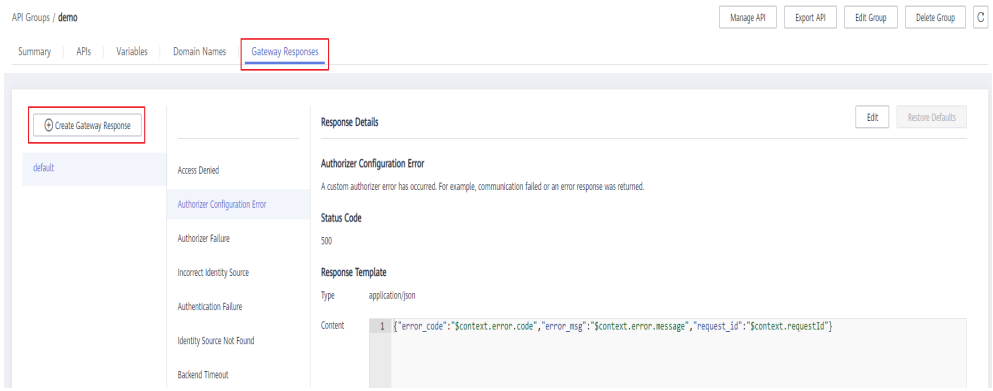
Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **API Groups**.

Paso 6 Busque el grupo de API para el que desea crear o modificar una respuesta de puerta de enlace y haga clic en el nombre del grupo para ir a la página de detalles del grupo de API.

Paso 7 Haga clic en la pestaña **Gateway Responses** y cree una respuesta de puerta de enlace.



NOTA

- Para editar una respuesta, haga clic en el botón **Edit** en la esquina superior derecha y modifique el código de estado y el contenido de la respuesta.
- Sólo puede modificar el código de estado y el contenido de una respuesta de puerta de enlace predeterminada o personalizada, y no puede cambiar el tipo de respuesta.
- La información de error y otros detalles de respuesta se pueden obtener usando variables. Para obtener más información sobre las variables admitidas, consulte **Tabla 3-3**.

----Fin

Tipos de respuesta

Tabla 3-2 enumera los tipos de respuesta admitidos por API Gateway. Puede definir códigos de estado de las respuestas para cumplir con sus requisitos de servicio.

Tabla 3-2 Tipos de respuesta de error compatibles con API Gateway

Nombre de la respuesta	Código de estado predeterminado	Descripción
Access Denied	403	Acceso denegado. Por ejemplo, se activa la política de control de acceso o se detecta un ataque.
Authorizer Configuration Error	500	Se ha producido un error de autorizador personalizado. Por ejemplo, la comunicación falló o se devolvió una respuesta de error.

Nombre de la respuesta	Código de estado predeterminado	Descripción
Authorizer Failed	500	Error en la autorización personalizada.
Incorrect Identity Source	401	Falta la fuente de identidad del autorizador personalizado o no es válida.
Authentication Failure	401	Error en la autenticación de IAM o de la aplicación.
Identity Source Not Found	401	No se ha especificado ningún origen de identidad.
Backend Timeout	504	Se agotó el tiempo de espera de la comunicación con el servicio backend.
Backend Unavailable	502	El servicio de backend no está disponible debido a un error de comunicación.
Default 4XX	-	Ocurrió otro error 4XX.
Default 5XX	-	Ocurrió otro error 5XX.
No API Found	404	No se encuentra ninguna API.
Incorrect Request Parameters	400	Los parámetros de solicitud son incorrectos o el método HTTP no es compatible.
Request Throttled	429	La solicitud fue rechazada debido a la limitación de la solicitud.
Unauthorized App	401	La aplicación que está usando no tiene autorización para llamar a la API.

Variables de contexto de API Gateway

Tabla 3-3 Variables que se pueden usar en el cuerpo del mensaje de respuesta

Variable	Descripción
$context.apiId	ID de API.
$context.appId	ID de la aplicación que llama a la API.
$context.requestId	ID de solicitud generado cuando se llama a la API.
$context.stage	Entorno de implementación en el que se llama a la API.
$context.sourceIp	Dirección IP de origen del llamador API.

Variable	Descripción
$context.authorizer.frontend.property	Valores de los pares de valor-atributo especificados asignados al contexto en la respuesta del autorizador personalizado de frontend
$context.authorizer.backend.property	Valores de los pares de valor-atributo especificados asignados al contexto en la respuesta del autorizador personalizado de back-end
$context.error.message	Mensaje de error.
$context.error.code	Código de error.
$context.error.type	Tipo de error.

3.2 Gestión de API

3.2.1 Creación de una API

Escenario

Puede exponer sus servicios de forma selectiva configurando sus API en API Gateway.

Para crear una API, establezca la información básica y defina la solicitud de API, el servicio de backend y las respuestas.

NOTA

API Gateway utiliza una arquitectura API basada en REST, por lo que la apertura y las llamadas a la API deben cumplir con las especificaciones relacionadas con la RESTful API.

Prerrequisitos

- Ha creado un grupo API. Si no hay ningún grupo de API disponible, cree uno durante la creación de la API.
- Si el servicio backend de la API se implementa en una VPC, ha creado un canal de VPC para acceder al servicio siguiendo el procedimiento de **Creación de un canal de VPC**. También puede crear un canal de VPC durante la creación de la API.

Configuración de información básica

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Haga clic en **Create API** y establezca los parámetros enumerados en **Tabla 3-4**.

Tabla 3-4 Información básica

Parámetro	Descripción
Name	Nombre de la API. Se recomienda que introduzca un nombre basado en reglas de nomenclatura para facilitar la búsqueda.
API Group	El grupo al que pertenece la API. Si no hay ningún grupo de API disponible, haga clic en **Create API Group** para crear uno.
Gateway Response	Se muestra si API Gateway no puede procesar una solicitud de API. API Gateway proporciona un conjunto de respuestas predeterminadas y también le permite **crear respuestas de gateway** con códigos de estado y contenido personalizados, en la página **API Groups**. El contenido de la respuesta debe estar en formato JSON.
Visibility	Determine si la API está disponible para el público. Opciones: ● **Public**
Security Authentication	Los siguientes modos de autenticación están disponibles: ● **App**: las solicitudes para la API serán autenticadas por API Gateway. ● **IAM**: las solicitudes para la API serán autenticadas por Identity and Access Management (IAM). ● **Custom**: las solicitudes de la API se autenticarán mediante su propio sistema o servicio de autenticación (por ejemplo, un sistema de autenticación basado en OAuth). ● **None**: No se requiere autenticación. El método de llamada a la API varía según el modo de autenticación. Para obtener más información, consulte **Guía para desarrolladores**. Se recomienda la autenticación de la aplicación. **AVISO** ● Si estableces el modo de autenticación de una API en **IAM**, cualquier usuario de API Gateway puede acceder a la API, lo que puede resultar en cargos excesivos si la API se bombardea con solicitudes maliciosas. ● Si estableces el modo de autenticación de una API en **None**, cualquier usuario puede acceder a la API a través de redes públicas, lo que puede resultar en cargos excesivos si la API se bombardea con solicitudes maliciosas. ● Si configura el modo de autenticación de una API en **Custom**, puede crear una función de FunctionGraph para interconectarse con su propio sistema o servicio de autenticación. Este modo de autenticación no se admite en las regiones donde FunctionGraph no está disponible.

Parámetro	Descripción
Simple Authentication	Este parámetro solo está disponible si establece **Security Authentication** en **App**. Si selecciona la autenticación de aplicaciones, puede configurar si desea habilitar la autenticación simple. En la autenticación simple, el parámetro **X-Apig-AppCode** se agrega al encabezado de solicitud HTTP para una respuesta rápida. API Gateway verifica solo el AppCode y el contenido de la solicitud no necesita estar firmado. La autenticación simple solo admite solicitudes HTTPS y no admite solicitudes HTTP. Para más detalles, consulte **Adición de un AppCode para una autenticación simple**. **NOTA** Después de habilitar la autenticación simple para una API existente, debe publicar la API de nuevo. Para más detalles, consulte **Publicación de una API**.
Custom Authorizer	Este parámetro es obligatorio si **Security Authentication** está establecida en **Custom**. Seleccione un autorizador personalizado si establece **Security Authentication** en **Custom**. Si no hay ningún autorizador personalizado disponible, haga clic en **Create Custom Authorizer** para crear uno.
Tag Name	Atributo de clasificación utilizado para identificar rápidamente la API de otras API.
Description	Descripción de la API.

Paso 7 Haga clic en **Next**.

----Fin

Definición de solicitud de API

Paso 1 En la página **Define API Request**, establece los parámetros enumerados en **Tabla 3-5**.

Figura 3-2 Definir solicitud de API

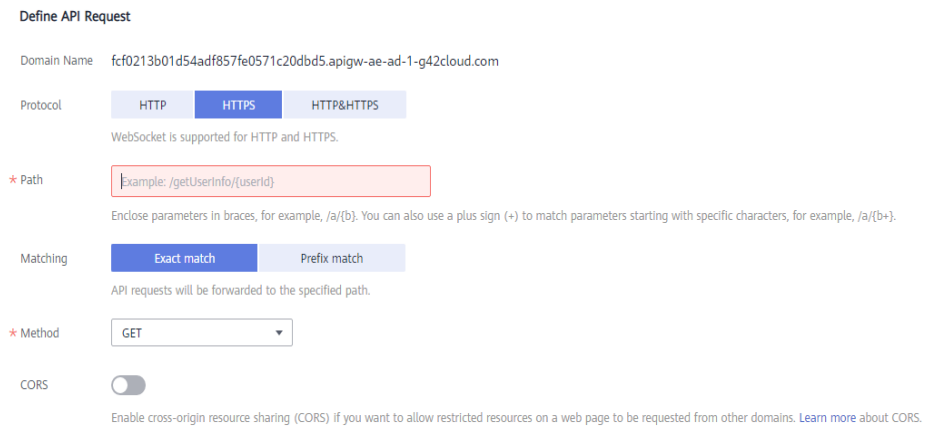


Tabla 3-5 Parámetros para definir solicitudes de API

Parámetro	Descripción
Domain Name	El subdominio asignado automáticamente al grupo API.
Protocol	El protocolo utilizado para llamar a la API. Opciones: ● HTTP ● HTTPS ● HTTP&HTTPS HTTPS se recomienda para transmitir datos importantes o confidenciales.
Path	La ruta para solicitar la API. Enter a path in the format of "/users/*{userId}*/projects". ● La variable en llaves ({}) es un parámetro de solicitud. Asegúrese de que es un segmento completo entre un par de barras diagonales (/). No se admite un segmento que no esté marcado por un par de barras, por ejemplo, **/abc{userId}**. Si establece el modo de coincidencia en **Exact match**, puede agregar un signo más (+) al final del parámetro de solicitud, por ejemplo, **/users/{*p*+}**. La variable *p* coincide con los segmentos entre uno o varios pares de barras diagonales (/). ● Asegúrese de definir los parámetros contenidos en la ruta de acceso de solicitud como parámetros de entrada. ● El contenido distingue entre mayúsculas y minúsculas.
Matching	Opciones: ● **Exact match**: La API solo se puede llamar usando la ruta de solicitud especificada. ● **Prefix match**: se puede llamar a la API usando rutas que comienzan con los caracteres coincidentes. Por ejemplo, si establece la ruta de solicitud en **/test/AA** y el modo de coincidencia en **Prefix match**, se puede llamar a la API usando **/test/AA/CC** pero no se puede llamar usando **/test/AACC**. **NOTA** ● La coincidencia exacta tiene prioridad sobre la coincidencia de prefijo. La coincidencia de prefijo con un prefijo corto tiene una prioridad más baja. Por ejemplo, para la ruta de acceso de solicitud **/a/b/c** (coincidencia exacta), **/a** (coincidencia de prefijo) y **/a/b** (coincidencia de prefijo), el orden de coincidencia es **/a/b/c** > **/a/b** > **/a**. ● Si establece el modo de coincidencia en **Prefix match**, los caracteres de la ruta de solicitud de API que excluye el prefijo se transmiten de forma transparente al servicio de backend. Por ejemplo, si define las rutas de solicitud frontend y backend de una API como **/test/** y **/test2/**, respectivamente, y se llama a la API usando **/test/AA/CC**, los caracteres **AA/CC** se transmitirán de forma transparente al servicio backend. La URL de solicitud recibida por el servicio backend es **/test2/AA/CC/**.

Parámetro	Descripción
Method	El método de llamada a la API. Las opciones son **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS**, y **ANY**. ● **ANY** indica que se puede llamar a la API usando cualquier método de solicitud. ● Si establece **Method** en **POST**, **PUT**, **PATCH**, o **ANY**, establezca el cuerpo de la solicitud.
CORS	Determine si desea habilitar el uso compartido de recursos entre orígenes (CORS). CORS permite que los navegadores envíen XMLHttpRequest a servidores de otros dominios, superando la limitación de que los JavaScript asíncronos y XML (AJAX) solo pueden usarse dentro del mismo dominio. Hay dos tipos de solicitudes CORS: ● Solicitudes simples: solicitudes que tienen el campo **Origin** en el encabezado. ● Solicitudes no tan simples: solicitudes HTTP enviadas antes de la solicitud real. Si habilita CORS, necesita crear otra API que use el método OPTIONS. Para más detalles, consulte **CORS**.

Paso 2 (Opcional) Establecer parámetros de entrada.

Los parámetros de entrada se transmiten junto con la solicitud cuando se llama a la API.

1. Haga clic en **Add Input Parameter**.
2. Establezca los parámetros enumerados en **Tabla 3-6**.

Tabla 3-6 Definición del parámetro de entrada

Parámetro	Descripción
Name	Nombre del parámetro de entrada. Si establece la ubicación del parámetro en **PATH**, asegúrese de que el nombre del parámetro es el mismo que el definido en la ruta de acceso de la solicitud. **NOTA** – El nombre del parámetro no distingue entre mayúsculas y minúsculas. No puede comenzar con **x-apig-** o **x-sdk-**. – El nombre del parámetro no puede ser **x-stage**. – Si establece la ubicación del parámetro en **HEADER**, asegúrese de que el nombre del parámetro no sea **Authorization** o **X-Auth-Token** y no contenga guiones bajos (_).
Location	Posición del parámetro en las solicitudes. Las opciones son **PATH**, **HEADER**, y **QUERY**. **NOTA** Si establece la ubicación del parámetro en **PATH**, debe incluir el parámetro en la ruta de acceso de solicitud.

Parámetro	Descripción
Type	Tipo del valor del parámetro. Opciones: **STRING** y **NUMBER**. **NOTA** Establezca el tipo de parámetros booleanos en **STRING**.
Mandatory	Determine si el parámetro de entrada es necesario en cada solicitud enviada para llamar a la API. Si selecciona **Yes**, se rechazarán las solicitudes de API que no contengan el parámetro de entrada.
Passthrough	Determine si desea transmitir de forma transparente el parámetro de entrada al servicio de backend.
Default Value	El valor que se utilizará si no se especifica ningún valor para el parámetro de entrada cuando se llama a la API. Si el parámetro de entrada no se especifica en una solicitud, API Gateway enviará automáticamente el valor predeterminado al servicio de backend.
Enumerated Value	Valor enumerado del parámetro de entrada. Utilice comas (,) para separar varios valores enumerados. El valor de este parámetro de entrada solo puede ser uno de los valores enumerados.
Minimum Length	La longitud mínima del valor del parámetro. Solo se permiten números.
Maximum Length	La longitud máxima del valor del parámetro. Solo se permiten números.
Example	Ejemplo de valor para el parámetro.
Description	Descripción del parámetro.

3. Haga clic en **OK**.

Paso 3 Haga clic en **Next**.

----Fin

Definición del servicio de backend

API Gateway le permite definir varias políticas de backend para diferentes escenarios. Las solicitudes que cumplan con las condiciones especificadas se enviarán al backend correspondiente. Por ejemplo, puede hacer que ciertas solicitudes a una API se reenvíen a un backend específico especificando la dirección IP de origen en las condiciones de la política del backend.

Puede definir un máximo de cinco políticas de backend para una API además del backend predeterminado.

Paso 1 Defina el backend predeterminado.

Las solicitudes de API que no cumplan las condiciones de ningún backend se reenviarán al backend predeterminado.

En la página **Define Backend Request**, seleccione un tipo de backend.

Tabla 3-7, **Tabla 3-8**, y **Tabla 3-9** describa los parámetros del servicio backend.

Tabla 3-7 Parámetros para definir un servicio backend HTTP/HTTPS

Parámetro	Descripción
Protocol	HTTP o HTTPS. Este protocolo debe ser el utilizado por el servicio backend. **NOTA** ● WebSocket es compatible con HTTP y HTTPS. ● HTTPS se recomienda para transmitir datos importantes o confidenciales.
Method	El método de llamada a la API. Las opciones son **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS**, y **ANY**. **ANY** indica que se puede llamar a la API usando cualquier método de solicitud.
VPC Channel	Determine si se accederá al servicio backend mediante un canal VPC. ● **En caso afirmativo, seleccione un canal de VPC.** **NOTA** – Para garantizar una comprobación del estado y la disponibilidad del servicio con éxito, configure los grupos de seguridad de los servidores en la nube en cada canal de VPC para permitir el acceso desde 100.125.0.0/16. ● **Si no, configure la dirección del servicio de backend.** Introduzca una dirección de back-end en el formato de "dirección IP del host o nombre de dominio":"número de puerto". El puerto predeterminado (80 para HTTP y 443 para HTTPS) se usará si no especifica un puerto. Puertos disponibles: 1 a 65535. Si desea utilizar una variable, incluya el nombre de la variable en signos numéricos (#), por ejemplo, **#ipaddress#**. Puede usar varias variables, por ejemplo, **#ipaddress##test#**.
Host Header (if applicable)	Este parámetro sólo está disponible si establece **VPC Channel** en **Configure**. Defina un encabezado de host para las solicitudes que se enviarán a los servidores en la nube asociados con el canal de VPC. De forma predeterminada, se utilizará el encabezado del host original en cada solicitud.
Path	La ruta de solicitud (URI) del servicio backend. Asegúrese de que todos los parámetros de la ruta estén encerrados entre llaves ({}). Por ejemplo, **/getUserInfo/{userId}**. Si la ruta contiene una variable de entorno, incluya la variable de entorno en signos numéricos (#), por ejemplo, **/#path#**. Puede usar varias variables de entorno, por ejemplo, **/#path##request#**.

Parámetro	Descripción
Timeout (ms)	Tiempo de espera de la solicitud de backend. Si se produce un error de tiempo de espera de backend durante la depuración de la API, aumente el tiempo de espera para localizar el motivo. **NOTA** Para las puertas de enlace dedicadas, puede modificar el tiempo de espera máximo haciendo referencia a **Parámetros de configuración**. El intervalo de valores es de 1 ms a 600,000 ms.
Two-way Authentication	Determine si desea permitir que API Gateway autentifique el servicio de backend de API a través de HTTPS. Para obtener más información acerca de cómo configurar el certificado para la autenticación bidireccional, consulte **Parámetros de configuración**. **NOTA** La autenticación bidireccional solo está disponible para puertas de enlace dedicadas en ciertas regiones.
Backend Authentication	Determine si el servicio de backend necesita autenticar las solicitudes de API. Si habilita esta opción, seleccione un autorizador personalizado para la autenticación de back-end. **Autorizadores personalizados** son funciones que se crean en el FunctionGraph para implementar una lógica de autenticación o para invocar un servicio de autenticación. **NOTA** La autenticación de backend se basa en FunctionGraph y solo está disponible en ciertas regiones.

Tabla 3-8 Parámetros para definir un servicio de backend de FunctionGraph

Parámetro	Descripción
FunctionURN	Identificador de la función solicitada. Haga clic en **Select Function URN** para especificar un URN de función.
Version/Alias	Seleccione una versión de función o alias. Para obtener más información, consulte las secciones "Administración de versiones" y "Administración de alias" en la *Guía del usuario del FunctionGraph*.
Invocation Mode	● **Synchronous**: invocación síncrona. Al recibir una solicitud de invocación, el FunctionGraph procesa inmediatamente la solicitud y devuelve un resultado. El cliente cierra la conexión una vez que ha recibido una respuesta del backend. ● **Asynchronous**: invocación asincrónica. Los resultados de la invocación de función de las solicitudes del cliente no importan para los clientes. Cuando recibe una solicitud, el FunctionGraph pone en cola la solicitud, devuelve una respuesta y, a continuación, procesa las solicitudes una por una en estado inactivo.
Timeout (ms)	Tiempo de espera de la solicitud de backend. Para más detalles, consulte **Tabla 3-7**.

Parámetro	Descripción
Backend Authentication	Para obtener más información, consulte la descripción sobre la autenticación de backend en **Tabla 3-7**.

Tabla 3-9 Parámetros para definir un servicio de backend de Mock

Parámetro	Descripción
Status Code	Este parámetro solo está disponible después de actualizar el componente Shubao.
Response	Puede usar Mock para el desarrollo, depuración y verificación de API. Permite que API Gateway devuelva una respuesta sin enviar la solicitud al backend. Esto es útil si necesita probar las API cuando el backend no está disponible.
Backend Authentication	Para obtener más información, consulte la descripción sobre la autenticación de backend en **Tabla 3-7**.
Header Parameters	Encabezados de respuesta de API. Haga clic en **Add Header**, e introduzca el nombre, el valor y la descripción del parámetro.

NOTA

- Si ha definido una variable de entorno en la ruta de solicitud de backend, la API no se puede depurar en la página de depuración de API.
- Para las variables definidas en la ruta de solicitud de backend de una API, se deben configurar las variables de entorno correspondientes y sus valores. De lo contrario, la API no se puede publicar porque no habrá valores que se puedan asignar a las variables.
- Los nombres de las variables de entorno distinguen entre mayúsculas y minúsculas.

Paso 2 (Opcional) Agregue una política de backend.

Puede agregar políticas de backend para reenviar solicitudes a diferentes servicios de backend.

1. Haga clic en **Add Backend Policy**.
2. Establezca los parámetros haciendo referencia a **Tabla 3-10** y **Tabla 3-7**.

Figura 3-3 Adición de una política de backend

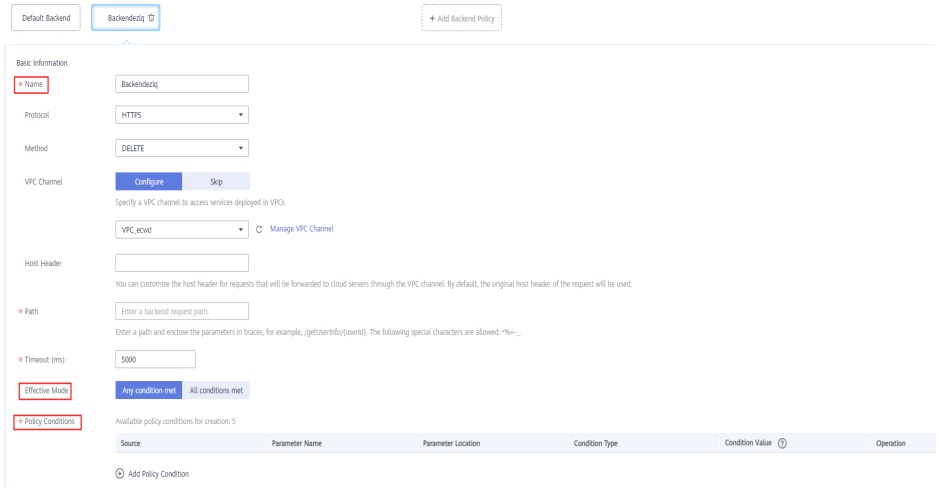


Tabla 3-10 Parámetros de política de backend

Parámetro	Descripción
Name	Nombre de la política de backend.
Effective Mode	– **Any condition met**: La política de backend entra en vigor si se cumple alguna de las condiciones de la política. – **All conditions met**: La política de backend solo entra en vigor cuando se cumplen todas las condiciones de la política.
Policy Conditions	Condiciones que deben cumplirse para que la política de backend entre en vigor. Establezca las condiciones haciendo referencia a **Tabla 3-11**.

Tabla 3-11 Condiciones de la política

Parámetro	Descripción
Source	– Dirección IP de origen – Parámetro de entrada – Parámetro del sistema: parámetros de tiempo de ejecución utilizados por API Gateway para procesar solicitudes de API **AVISO** Los parámetros de entrada (por ejemplo, encabezados) definidos como condiciones de política deben haberse definido ya en la configuración de solicitud de API. Solo gateways dedicadas admiten el uso de parámetros del sistema como condiciones de política. Si no se muestra **System parameter**, póngase en contacto con el soporte técnico para actualizar su gateway.

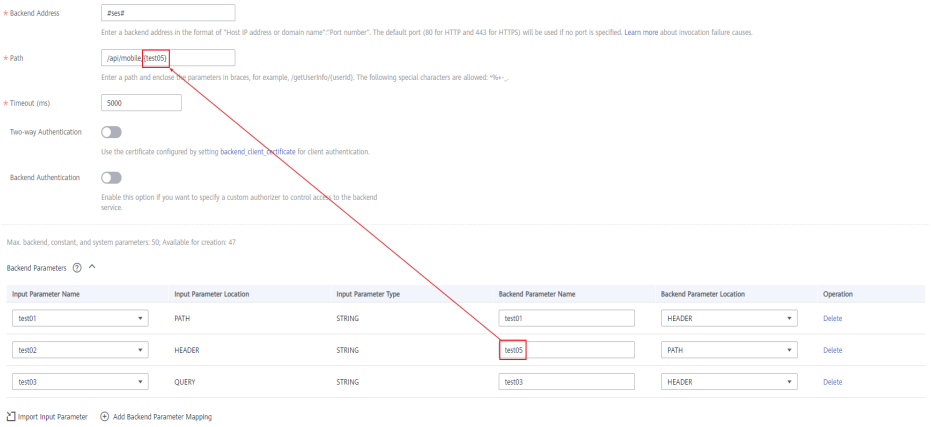
Parámetro	Descripción
Parameter Name	– Cuando establezca **Source** en **Input parameter**, seleccione un parámetro de entrada. – Al establecer **Source** en **System parameter**, seleccione un parámetro del sistema. ■ **reqPath**: Solicitar URI, por ejemplo, **/a/b/c**. ■ **reqMethod**: Método de solicitud, por ejemplo, **GET**.
Parameter Location	La ubicación del parámetro sólo se muestra si se establece el parámetro **Source** en **Input parameter**.
Condition Type	Este parámetro sólo es necesario si establece **Source** en **Input parameter** o **System parameter**. – **Equal**: el parámetro de solicitud debe ser igual al valor especificado. – **Enumerated**: el parámetro request debe ser igual a cualquiera de los valores enumerados. – **Matching**: el parámetro de solicitud debe ser igual a cualquier valor de la expresión regular. **NOTA** Cuando establece el parámetro **Source** en **System parameter** y selecciona un parámetro denominado **reqMethod**, puede establecer el tipo de condición sólo en **Equal** o **Enumerated**.
Condition Value	Establezca un valor de condición según el tipo de condición. – **Equal**: introduzca un valor. – **Enumerated**: Introduzca varios valores y sepárelos con comas. – **Matching**: Introduzca un rango, por ejemplo, **[0-5]**. Si ha establecido **Source** en **Source IP address**, introduzca una o más direcciones IP y sepárelas con comas.

Paso 3 (Opcional) Establecer parámetros de backend.

Los parámetros de entrada de la API se asignan a los parámetros de backend correspondientes en las solicitudes de backend.

1. Haga clic en ⌄ junto a **Backend Parameters**, y defina los parámetros de backend. Puede utilizar uno de los métodos siguientes:
   – Haga clic en **Import Input Parameter**. Todos los parámetros de entrada definidos se muestran automáticamente.
   – Haga clic en **Add Backend Parameter Mapping**, y agregue los parámetros de backend necesarios.
2. Modifique las asignaciones en función de los parámetros y sus ubicaciones en las solicitudes de backend. **Figura 3-4** resalta los parámetros del backend.

Figura 3-4 Configuración de parámetros de backend



a. Si establece la ubicación del parámetro en **PATH**, asegúrese de que el nombre del parámetro es el mismo que el definido en la ruta de solicitud de backend.

b. El nombre y la ubicación de un parámetro de entrada pueden ser diferentes de los del parámetro de solicitud de back-end asignado.

   NOTA

   - El nombre del parámetro no distingue entre mayúsculas y minúsculas. No puede comenzar con **x-apig-** o **x-sdk-**.
   - El nombre del parámetro no puede ser **x-stage**.
   - Si establece la ubicación del parámetro en **HEADER**, asegúrese de que el nombre del parámetro no contiene guiones bajos (_).

c. En la figura anterior, los parámetros **test01** y **test03** están situados en las posiciones de ruta y consulta de las solicitudes de API, y sus valores se recibirán en la cabecera de las solicitudes de backend. **test02** se encuentra en el encabezado de las solicitudes de API, y su valor se recibirá a través de **test05** en la ruta de las solicitudes de backend.

   Por ejemplo, **test01** es **abc**, **test02** es **def**, y **test03** es **xyz**.

   Solicitud de API:

   ```
   curl -ik -H 'test02:def' -X GET https://www.example01.com/v1.0/abc?
   test03=xyz
   ```

   Solicitud de backend:

   ```
   curl -ik -H 'test01:abc' -H 'test03:xyz' -X GET https://
   www.example02.com/v1.0/def
   ```

Paso 4 (Opcional) Establecer parámetros constantes.

Puede definir parámetros constantes para que el servicio de backend reciba constantes que son invisibles para los que llaman a la API. API Gateway agrega parámetros constantes a las posiciones especificadas en la solicitud enviada al servicio de backend.

1. Haga clic en ⌄ junto a **Constant Parameters**.
2. Haga clic en **Add Constant Parameter**, y defina los parámetros enumerados en **Tabla 3-12**.

Figura 3-5 Adición de parámetros constantes

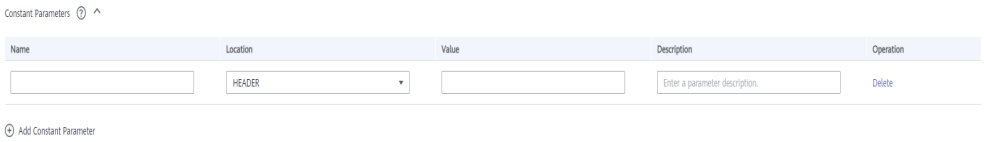


Tabla 3-12 Definición de parámetros constantes

Parámetro	Descripción
Name	Nombre del parámetro constante. Si establece la ubicación del parámetro en **PATH**, asegúrese de que el nombre del parámetro es el mismo que el definido en la ruta de solicitud de backend. **NOTA** – El nombre del parámetro no distingue entre mayúsculas y minúsculas. No puede comenzar con **x-apig-** o **x-sdk-**. – El nombre del parámetro no puede ser **x-stage**. – Si establece la ubicación del parámetro en **HEADER**, asegúrese de que el nombre del parámetro no contiene guiones bajos (_).
Location	Posición del parámetro en las solicitudes. Las opciones son **PATH**, **QUERY**, y **HEADER**.
Value	Valor del parámetro.
Description	Descripción del parámetro constante.

NOTA

- API Gateway envía solicitudes que contienen parámetros constantes a los servicios de backend después de la codificación porcentual de valores de parámetros especiales. Asegúrese de que los servicios de backend admitan la codificación porcentual. Por ejemplo, el valor del parámetro **[apig]** se convierte en **%5Bapig%5D** después de la codificación porcentual.
- Para los valores de los parámetros de ruta, los siguientes caracteres serán codificados porcentualmente: códigos ASCII 0-31, símbolos en blanco, códigos ASCII 127-255, y caracteres especiales ?></%#"[\]^` {|}
- Para los valores de las cadenas de consulta, los siguientes caracteres serán codificados porcentualmente: códigos ASCII 0-31, símbolos en blanco, códigos ASCII 127-255, y caracteres especiales >=<+&%#"[\]^` {|}

Paso 5 (Opcional) Establezca los parámetros del sistema.

Los parámetros del sistema se refieren a los parámetros de tiempo de ejecución con respecto a la ejecución de la puerta de enlace y a las autentificaciones front-end y back-end. Los parámetros se transfieren al servicio de backend de la API para el control de acceso y la autenticación personalizada.

1. Haga clic en junto a **System Parameters**.
2. Haga clic en **Add System Parameter**, y defina los parámetros enumerados en **Tabla 3-13**.

Figura 3-6 Adición de un parámetro del sistema

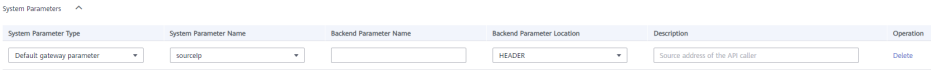


Tabla 3-13 Parámetros del sistema

Parámetro	Descripción
System Parameter Type	– **Default gateway parameter**: parámetros predeterminados compatibles con API Gateway. – **Frontend authentication parameter**: Parámetros que se mostrarán en el resultado de autenticación personalizada de frontend. Esta opción sólo está disponible si selecciona **Custom** para **Security Authentication** en la página **Set Basic Information**. – **Backend authentication parameter**: Parámetros que se mostrarán en el resultado de autenticación personalizada de backend. Esta opción solo está disponible si habilita **Backend Authentication** en la página **Define Backend Request**.
System Parameter Name	– Si **System Parameter Type** es **Default gateway parameter**, seleccione cualquiera de los siguientes parámetros. ■ **sourceIp**: dirección IP de origen del llamador de la API ■ **stage**: entorno en el que se llama la API ■ **apiId**: ID de la API ■ **appId**: ID de la aplicación que llama a la API ■ **requestId**: ID de solicitud generado cuando se llama a la API ■ **serverAddr**: dirección IP del servidor de gateway ■ **serverName**: nombre del servidor de gateway ■ **handleTime**: tiempo de procesamiento de la solicitud de API ■ **providerAppId**: ID de la aplicación del proveedor de API – Asegúrese de que los parámetros de autenticación front-end y back-end sean coherentes con los parámetros de resultado de retorno definidos para la función de autorizador personalizado correspondiente. Para obtener más información acerca de cómo crear una función de autorizador personalizada y obtener parámetros de resultado devueltos, consulte **Guía para desarrolladores de API Gateway**.
Backend Parameter Name	Nombre del parámetro backend al que se asignará el parámetro del sistema. **NOTA** – El nombre del parámetro no distingue entre mayúsculas y minúsculas. No puede comenzar con **x-apig-** o **x-sdk-**. – El nombre del parámetro no puede ser **x-stage**. – Si establece la ubicación del parámetro en **HEADER**, asegúrese de que el nombre del parámetro no contiene guiones bajos (_).

Parámetro	Descripción
Backend Parameter Location	Posición del parámetro backend en las solicitudes.
Description	Descripción del parámetro del sistema.

Paso 6 Haga clic en **Next**.

----Fin

Definición de respuestas

Paso 1 En la página **Define Response**, establezca los parámetros enumerados en **Tabla 3-14**.

Tabla 3-14 Definición de respuestas

Parámetro	Descripción
Example Success Response	Un ejemplo de una respuesta devuelta cuando se llama correctamente a la API.
Example Failure Response	Un ejemplo de una respuesta devuelta cuando no se puede llamar a la API.

Paso 2 Haga clic en **Finish**.

Una vez creada la API, haga clic en su nombre en la lista de API para ver los detalles.

----Fin

Creación de una API llamando a una API

También puede crear una API llamando a una API proporcionada por API Gateway.

Para obtener más información, consulta **Registro de una API**.

Preguntas frecuentes sobre la creación de API

¿Admite API Gateway múltiples endpoints de backend?

¿Cuáles son las posibles causas si un servicio de backend falla en ser invocado o si la invocación se agota?

¿Por qué estoy viendo el mensaje "No backend available"?

Operaciones de seguimiento

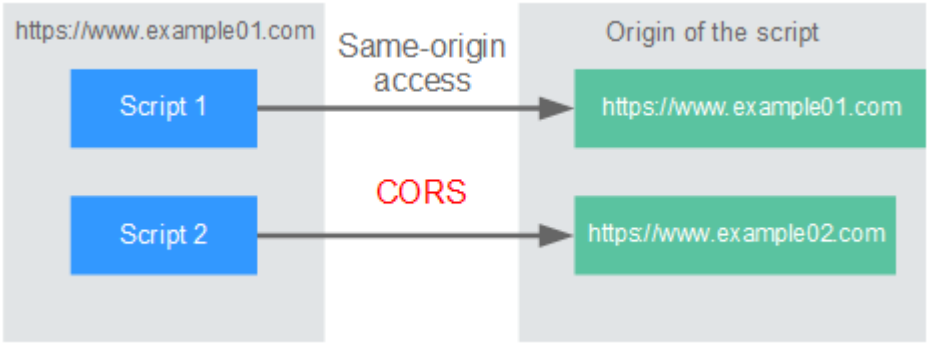
Después de crear una API, compruébala siguiendo el procedimiento en **Depuración de una API**.

3.2.2 CORS

¿Qué es el CORS?

Por razones de seguridad, los navegadores restringen las solicitudes de origen cruzado iniciadas desde scripts. Esto significa que una aplicación web solo puede solicitar recursos desde su origen. El mecanismo CORS permite a los navegadores enviar XMLHttpRequest a servidores en otros dominios y solicitar acceso a los recursos allí.

Figura 3-7 Flujo de proceso del mecanismo CORS



Hay dos tipos de solicitudes CORS:

- **Simple requests**

  Las solicitudes simples deben cumplir las siguientes condiciones:

  a. El método de solicitud es HEAD, GET o POST.

  b. El encabezado de solicitud contiene solo los siguientes campos:

  - Accept
  - Accept-Language
  - Content-Language
  - Last-Event-ID
  - Content-Type (**application/x-www-form-urlencoded**, **multipart/form-data**, or **text/plain**)

  En el encabezado de una solicitud simple, los navegadores agregan automáticamente el campo **Origin** para especificar el origen (incluidos el protocolo, el dominio y el puerto) de la solicitud. Después de recibir tal solicitud, el servidor de destino determina si la solicitud es segura y puede aceptarse basándose en el origen. Si el servidor envía una respuesta que contiene el campo **Access-Control-Allow-Origin**, el servidor acepta la solicitud.

- **Not-so-simple requests**

  Las solicitudes que no cumplen las condiciones para solicitudes simples son solicitudes no tan simples.

  Antes de enviar una solicitud no tan simple, los navegadores envían una solicitud de comprobación previa HTTP al servidor de destino para confirmar si el origen desde el que se carga la página web está en la lista de origen permitido, y para confirmar qué métodos de solicitud HTTP y campos de encabezado se pueden usar. Si la solicitud de comprobación previa se realiza correctamente, los navegadores envían solicitudes simples al servidor.

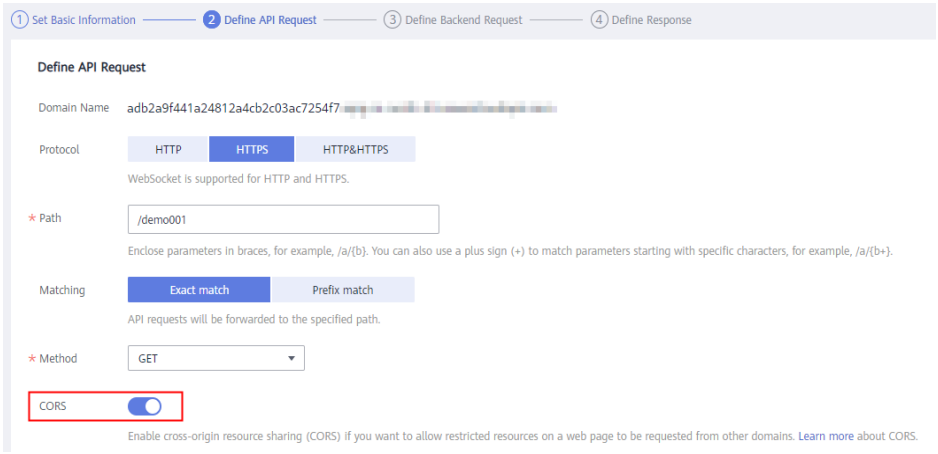
Configuración de CORS

CORS está deshabilitado por defecto. Para habilitar CORS para una API, realice las operaciones descritas en esta sección. Para personalizar los encabezados de solicitud, los métodos de solicitud y los orígenes permitidos para el acceso entre dominios, cree un **plug-in CORS**.

- **Simple CORS requests**

  Al crear una API, habilite CORS en la página de configuración de solicitud de API. Para obtener más información, consulte **Solicitud simple**.

  Figura 3-8 CORS



- **Not-so-simple CORS requests**

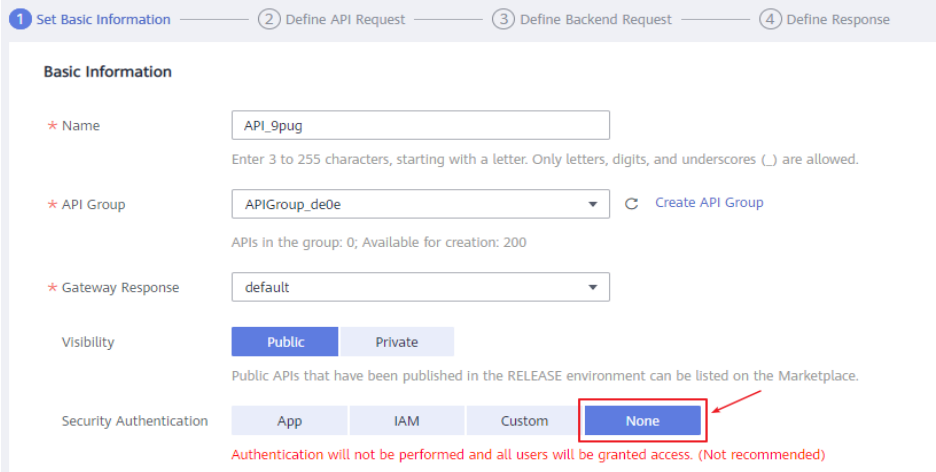
  AVISO

  Si tu API recibirá solicitudes no tan sencillas, **cree otra API a la que se accederá mediante el método OPTIONS** en el mismo grupo que la API de destino para recibir solicitudes de comprobación previa.

  Siga este procedimiento para definir la API de solicitud de comprobación previa. Para obtener más información, consulte **Not-So-Simple Request**.

  a. En la página **Set Basic Information**, seleccione **None** para omitir la autenticación de seguridad.

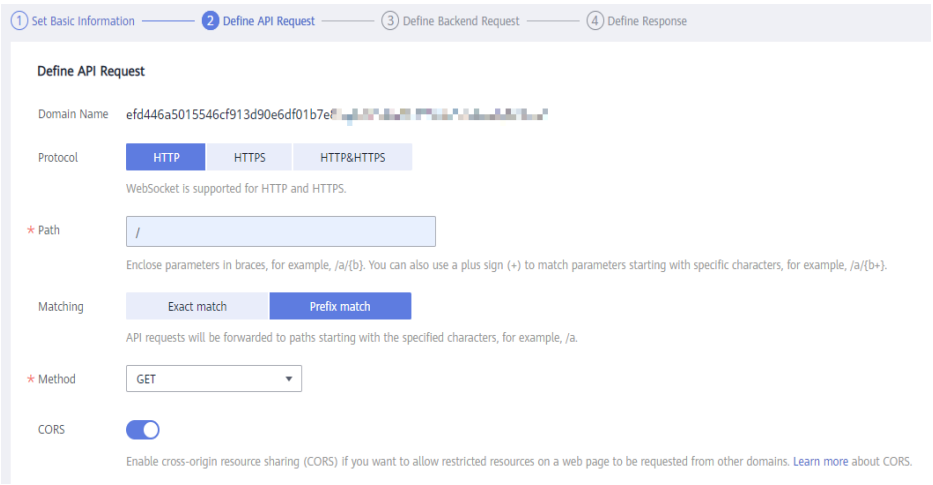
Figura 3-9 None authentication



b. En la página **Define API Request**, realice la siguiente configuración:

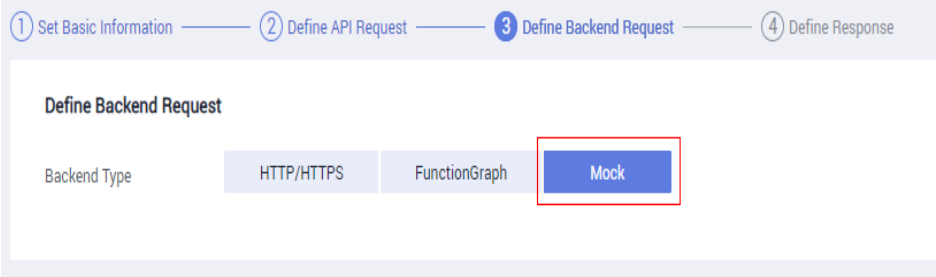
- **Protocol**: El mismo protocolo utilizado por la API con CORS habilitado.
- **Path**: escriba una barra diagonal (/).
- **Method**: Seleccione **OPTIONS**.
- **CORS**: Habilitado.

Figura 3-10 Definición de la solicitud de API



c. Seleccione el tipo de backend **Mock**.

Figura 3-11 Mock backend service



Solicitud simple

Al crear una API que recibirá solicitudes simples, **habilite CORS** para la API.

Escenario 1: Si CORS está habilitado y la respuesta del backend no contiene un encabezado CORS, API Gateway maneja las solicitudes de cualquier dominio y devuelve el encabezado **Access-Control-Allow-Origin**. Por ejemplo:

Solicitud enviada por un navegador y que contiene el campo Encabezado Origen:

```
GET /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin: This field is required to specify the origin (**http://www.cors.com** in this example) of the request. API Gateway and the backend service determine based on the origin whether the request is safe and can be accepted.

Response sent by the backend service:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

Respuesta enviada por API Gateway:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

Access-Control-Allow-Origin: Este campo es requerido. El asterisco (*) significa que API Gateway gestiona las solicitudes enviadas desde cualquier dominio.

Escenario 2: Si CORS está habilitado y la respuesta del backend contiene un encabezado CORS, el encabezado sobrescribirá el agregado por API Gateway. Los siguientes mensajes se utilizan como ejemplos:

Solicitud enviada por un navegador y que contiene el campo Encabezado Origen:

```
GET /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin: Este campo es obligatorio para especificar el origen (el **http://www.cors.com** en este ejemplo) de la solicitud. API Gateway y el servicio de backend determinan en función del origen si la solicitud es segura y puede aceptarse.

Respuesta enviada por el servicio backend:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
```



```
Content-Type: application/json
Content-Length: 16
Server: api-gateway
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

Access-Control-Allow-Origin: Indica que el servicio backend acepta solicitudes enviadas desde **http://www.cors.com**.

Respuesta enviada por API Gateway:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

El encabezado CORS en la respuesta de backend sobrescribe eso en la respuesta de API Gateway.

Not-So-Simple Request

Cuando cree una API que recibirá solicitudes no tan simples, habilite CORS para la API siguiendo las instrucciones en **Configuración de CORS**, y cree otra API a la que se accederá mediante el método OPTIONS.

NOTA

Si usa el plug-in CORS para una API, no necesita crear otra API que use el método OPTIONS.

Los parámetros de solicitud de una API a la que se accede mediante el método OPTIONS deben establecerse de la siguiente manera:

- **API Group**: El mismo grupo al que pertenece la API con CORS habilitado.
- **Security Authentication**: seleccione **None**. No se requiere autenticación para las solicitudes recibidas por la nueva API, independientemente del modo de autenticación de seguridad seleccionado.
- **Protocol**: El mismo protocolo utilizado por la API con CORS habilitado.
- **Path**: Ingrese un (/) de barra diagonal o seleccione la ruta para la que se ha establecido o coincide con la API con CORS habilitada.
- **Method**: Seleccione **OPTIONS**.
- **CORS**: Habilitado.

Las siguientes son solicitudes y respuestas de ejemplo enviadas a o desde un backend simulado.

Solicitud enviada desde un navegador a una API a la que se accede mediante el método OPTIONS:

```
OPTIONS /HTTP/1.1
User-Agent: curl/7.29.0
Host: localhost
Accept: */*
Origin: http://www.cors.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Sdk-Date
```


- **Origin**: Este campo es obligatorio para especificar el origen desde el que se ha enviado la solicitud.
- **Access-Control-Request-Method**: Este campo es necesario para especificar los métodos HTTP que se usarán en las solicitudes simples posteriores.
- **Access-Control-Request-Headers**: Este campo es opcional y se utiliza para especificar los campos de encabezado adicionales en las solicitudes simples posteriores.

Response sent by the backend: ninguno

Respuesta enviada por API Gateway:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 02:38:48 GMT
Content-Type: application/json
Content-Length: 1036
Server: api-gateway
X-Request-Id: c9b8926888c356d6a9581c5c10bb4d11
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Stage,X-Sdk-Date,X-Sdk-Nonce,X-Proxy-Signed-
Headers,X-Sdk-Content-Sha256,X-Forwarded-For,Authorization,Content-
Type,Accept,Accept-Ranges,Cache-Control,Range
Access-Control-Expose-Headers: X-Request-Id,X-Apig-Latency,X-Apig-Upstream-
Latency,X-Apig-RateLimit-Api,X-Apig-RateLimit-User,X-Apig-RateLimit-App,X-Apig-
RateLimit-Ip,X-Apig-RateLimit-Api-Allenv
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Max-Age: 172800
```

- **Access-Control-Allow-Origin**: Este campo es requerido. El asterisco (*) significa que API Gateway gestiona las solicitudes enviadas desde cualquier dominio.
- **Access-Control-Allow-Headers**: Este campo es obligatorio si está contenido en la solicitud. Indica todos los campos de encabezado que se pueden usar durante el acceso de origen cruzado.
- **Access-Control-Expose-Headers**: Estos son los campos de encabezado de respuesta que se pueden ver durante el acceso entre regiones.
- **Access-Control-Allow-Methods**: Este campo es necesario para especificar qué métodos de solicitud HTTP admite la API Gateway.
- **Access-Control-Max-Age**: Este campo es opcional y se utiliza para especificar el tiempo (en segundos) durante el cual el resultado de la comprobación previa permanece válido. No se enviarán más solicitudes de comprobación previa dentro del período especificado.

Solicitud enviada por un navegador y que contiene el campo Encabezado Origen:

```
PUT /simple HTTP/1.1
Host: www.test.com
Origin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Respuesta enviada por el backend:

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

Respuesta enviada por API Gateway:


```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

3.2.3 Depuración de una API

Escenario

Después de crear una API, depurarla en la consola API Gateway estableciendo los encabezados HTTP y los parámetros del cuerpo para verificar si la API se está ejecutando normalmente.

NOTA

- Las API con rutas de solicitud de backend que contienen variables no se pueden depurar.
- Si una API se ha vinculado con una política de limitación de solicitudes, la política no funcionará durante la depuración de la API.

Prerrequisitos

- Ha creado un grupo de API y una API.
- Ha configurado el servicio de backend de la API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

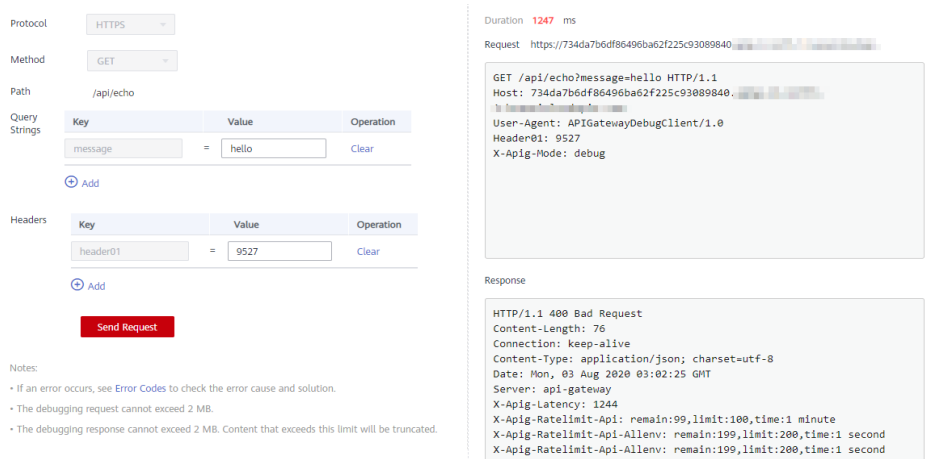
- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Depurar una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la API que desea depurar, elija **More** > **Debug**.
- Haz clic en el nombre de la API de destino y haz clic en **Debug** en la esquina superior derecha de la página de detalles de la API mostrada.

Figura 3-12 Depuración de una API



En el lado izquierdo, establece los parámetros de solicitud de API enumerados en **Tabla 3-15**. En el lado derecho, consulta la información de solicitud y respuesta de la API después de hacer clic en **Send Request**.

Tabla 3-15 Parámetros para la depuración de una API

Parámetro	Descripción
Protocol	Este parámetro solo se puede modificar si se establece **Protocol** en **HTTP&HTTPS** para la API.
Method	Este parámetro solo se puede modificar si estableces **Method** en **ANY** para la API.
Suffix	Puede definir una ruta solo si ha establecido **Matching** a **Prefix match** para la API.
Path	Ruta de solicitud de la API.
Path Parameters	Este parámetro solo se puede modificar si ha definido parámetros de ruta (como **{test}**) para la API.
Headers	Encabezados y valores HTTP.
Query Strings	Parámetros y valores de la cadena de consulta.
Body	Este parámetro solo se puede modificar si establece **Method** en **PATCH**, **POST** o **PUT** para la API.

NOTA

Los campos mostrados en la página de depuración varían según el tipo de solicitud.

Paso 7 Después de establecer los parámetros de solicitud, haga clic en **Send Request**.

El cuadro en la parte inferior derecha muestra la respuesta de la solicitud de API.

- Si la depuración tiene éxito, se muestran el código **200** de estado HTTP y los detalles de respuesta.

- Si la solicitud no se envía, se muestra un código de estado HTTP **4xx** o **5xx**. Para más detalles, consulte **Códigos de error**.

Paso 8 Puede enviar más solicitudes con diferentes parámetros y valores para verificar la API.

NOTA

Para modificar las configuraciones de la API, haz clic en **Edit** en la esquina superior derecha y modifica los parámetros en la página **Edit API**.

----Fin

Operaciones de seguimiento

Una vez que la API se haya depurado correctamente, **publique** la API en un entorno específico para que los usuarios puedan llamar a la API. Para garantizar la seguridad de la API, cree directivas de limitación de solicitudes (consulte **Creación de una política de limitación de solicitudes**), políticas de control de acceso (**Creación de una política de control de acceso**), y claves de firma (**Creación y uso de una clave de firma**) para la API.

3.2.4 Autorización de aplicaciones para llamar a una API

Escenario

APIs que usan autenticación de aplicaciones solo pueden ser llamadas por las aplicaciones que han sido autorizadas para llamarlas.

NOTA

- Solo puede autorizar aplicaciones para llamar a las API publicadas.
- Solo puede autorizar a las aplicaciones para llamar a las API que usan autenticación de aplicaciones.

Prerrequisitos

- Ha creado un grupo de API y una API.
- (Opcional) Ha creado un entorno.
- Ha creado una aplicación.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

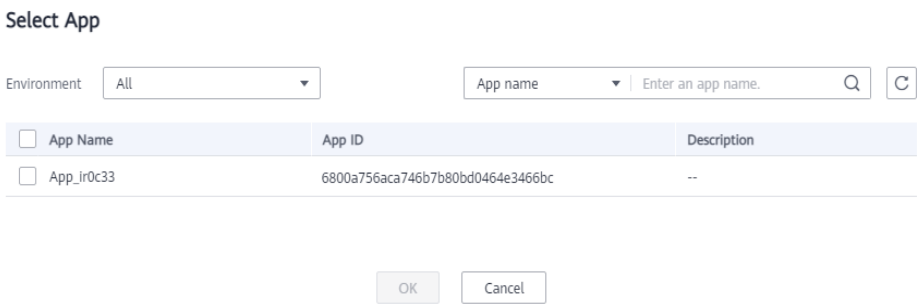
Paso 6 Autorice a las aplicaciones para llamar a una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la API de destino, elija **More** > **Authorize App**, y a continuación, haga clic en **Select App**.
- Selecciona la API de destino, haz clic en **Authorize App** en la lista de API y, a continuación, haz clic en **Select App**.
- Autorice aplicaciones a través de la página de detalles de la API.
  a. Haga clic en el nombre de la API de destino.
  b. Haga clic en la pestaña **Authorization**.
  c. Haz clic en **Select App**.

NOTA

Para autorizar a una aplicación a acceder a varias API, seleccione las API y haga clic en **Authorize App**. Haga clic en **Select App**, seleccione la aplicación que desea autorizar y haga clic en **OK**. Puede conceder acceso a un máximo de 1000 APIs a la vez.

Paso 7 Seleccione un entorno, busque y seleccione las aplicaciones deseadas y haga clic en **OK**.



Paso 8 Una vez completada la autorización, vea las aplicaciones autorizadas en la página de la pestaña **Authorization** o en la página **Authorize App**.

NOTA

Si una aplicación no necesita llamar a la API, haga clic en **Cancel Authorization** en la fila que contiene la aplicación para desvincularla.

----Fin

Autorización de una aplicación mediante llamada a una API

También puede autorizar una aplicación llamando a una API proporcionada por API Gateway. Para obtener más información, consulte las siguientes referencias:

Autorización de aplicaciones

Cancelación de autorización

Operaciones de seguimiento

Después de autorizar una aplicación para llamar a una API, se puede llamar a la API usando SDK de diferentes lenguajes de programación.

3.2.5 Publicación de una API

Escenario

Las API solo se pueden llamar después de que se hayan publicado en un entorno. Puedes publicar APIs en diferentes entornos. API Gateway le permite ver el historial de publicaciones (como la versión, la descripción, la hora y el entorno) de cada API, y admite la reversión de las API a diferentes versiones históricas.

NOTA

- Si modifica una API publicada, debe publicarla de nuevo para que las modificaciones surtan efecto en el entorno en el que se ha publicado la API.
- Un máximo de 10 registros de publicación de una API se conservan en un entorno.

Prerrequisitos

- Ha creado un grupo de API y una API.
- Usted ha creado un entorno.

Publicación de una API

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Publicar una API. Puede utilizar uno de los métodos siguientes:

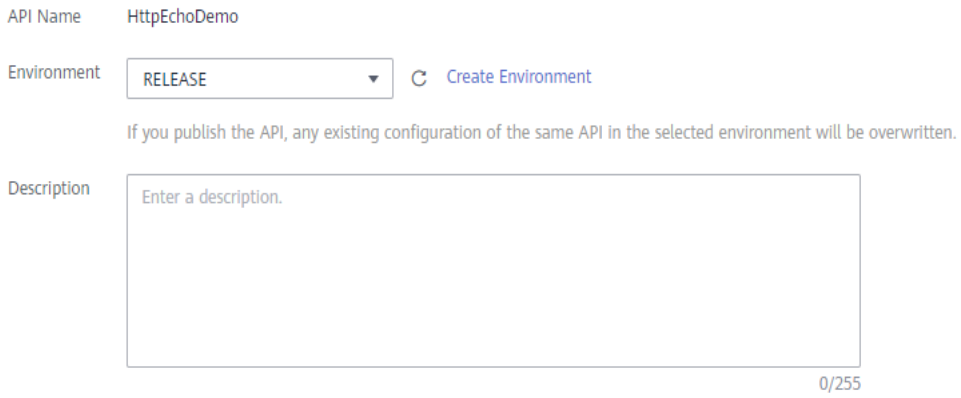
- Haga clic en **Publish** en la fila que contiene la API que deseas publicar.
- Haz clic en el nombre de la API de destino y haz clic en **Publish** en la esquina superior derecha de la página de detalles de la API mostrada.

NOTA

Para publicar varias API, seleccione las API y haga clic en **Publish**. Puede publicar un máximo de 1000 API a la vez.

Paso 7 Seleccione el entorno donde se publicará la API e introduzca una descripción.

Figura 3-13 Publicación de una API



NOTA

- Si la API ya se ha publicado en el entorno, publicarla de nuevo sobrescribirá su definición en ese entorno.
- Si no hay ningún entorno que cumpla con sus requisitos, cree uno nuevo.

Paso 8 Haga clic en **Publish**.

----Fin

Consulta del historial de publicaciones

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

Shared Gateway: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.

Dedicated Gateways: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

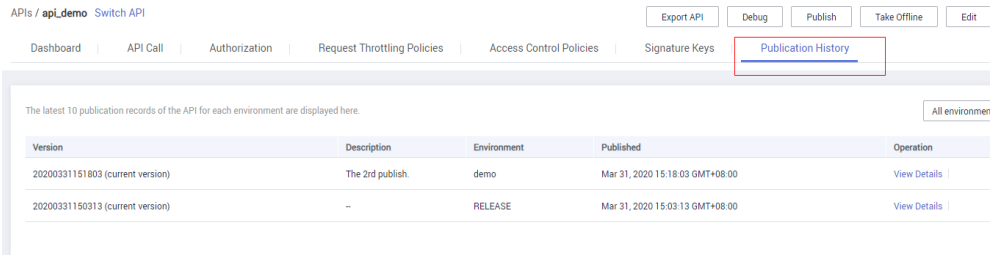
Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Haga clic en el nombre de la API de destino.

Paso 7 Haga clic en la pestaña **Publication History**.

Se muestra el historial de publicaciones de la API.

Figura 3-14 Consulta del historial de publicaciones



Paso 8 Haga clic en **View Details** en la columna **Operation** de una versión.

El cuadro de diálogo **View Details** muestra la información básica, la información de solicitud de front-end y back-end, los parámetros de entrada y constantes, las asignaciones de parámetros y las respuestas de ejemplo de la API.

Paso 9 Para revertir la API a una versión histórica, haga clic en **Switch Version** en la fila que contiene la versión de destino y haga clic en **Yes**.

Si se muestra "current version" junto a la versión de destino, la reversión se realizó correctamente.

Cuando se llama a la API, se utiliza la configuración de la versión actual en lugar de la configuración guardada anteriormente.

Por ejemplo, se publicó una API en el entorno RELEASE el 1 de agosto de 2018. El 20 de agosto de 2018, la API se publicó en el mismo entorno después de la modificación. Si la versión publicada el 1 de agosto se establece como la versión actual, la configuración de esta versión se utilizará cuando se llame a la API.

----Fin

Publicación de una API llamando a una API

También puede publicar una API llamando a una API proporcionada por API Gateway. Para obtener más información, consulte la siguiente referencia:

Publicación de una API

Preguntas frecuentes sobre la publicación de API

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

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

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

3.2.6 Desconexión de una API

Escenario

Puede eliminar las API que no necesite de los entornos donde se han publicado las API.

AVISO

Esta operación hará que las API sean inaccesibles en los entornos. Asegúrese de haber notificado a los usuarios antes de esta operación.

Prerrequisitos

- Ha creado un grupo de API y una API.
- Ha publicado la API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Ponga la API fuera de línea. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la API de destino, elija **More** > **Take Offline**.
- Haz clic en el nombre de la API de destino y haz clic en **Take Offline** en la esquina superior derecha de la página de detalles de la API.

NOTA

Para poner varias API sin conexión, seleccione las API y haga clic en **Take Offline**. Puede tomar un máximo de 1000 API sin conexión a la vez.

Paso 7 Seleccione el entorno desde el que desea tomar la API sin conexión y haga clic en **Yes**.

----Fin

Tomar una API fuera de línea mediante llamada a una API

También puede poner una API fuera de línea llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **poner una API fuera de línea**.

Operaciones de seguimiento

Después de tener una API sin conexión, elimínela según las instrucciones proporcionadas en **Eliminación de una API**.

3.2.7 Eliminación de una API

Escenario

Puede eliminar las API publicadas que ya no necesite.

AVISO

- Las aplicaciones o los usuarios que usaron las API no pueden acceder a las API eliminadas, así que asegúrate de notificar a los usuarios antes de la eliminación.
- Las API publicadas primero deben quitarse desconectadas y luego eliminarse.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Eliminar la API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la API que desea eliminar, elija **More** > **Delete**.
- Haz clic en el nombre de la API de destino y haz clic en **Delete** en la esquina superior derecha de la página de detalles de la API mostrada.

NOTA

Para eliminar varias API, seleccione las API y haga clic en **Delete**. Puede eliminar un máximo de 1000 API a la vez.

Paso 7 Escriba **DELETE** y haga clic en **Yes**.

----Fin

Eliminación de una API mediante llamada a una API

También puede eliminar una API mediante llamada a una API proporcionada por API Gateway. Para obtener más información, consulta **Eliminación de una API**.

3.2.8 Importación de APIs

Escenario

API Gateway le permite importar API de Swagger 2.0 a grupos de API existentes o nuevos. Swagger es una herramienta de código abierto basada en especificaciones OpenAPI para diseñar, construir, registrar y usar REST APIs.

Puede importar API individualmente o en lotes dependiendo del número de API contenidas en un archivo Swagger.

Prerrequisitos

- El archivo API Swagger que se va a importar está disponible y ya tiene definiciones de API extendidas complementadas.
- Tiene suficientes cuotas de grupos de API y API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Haz clic en **Import API**.

Paso 7 Establezca los parámetros enumerados en **Tabla 3-16**.

Figura 3-15 Importación de APIs

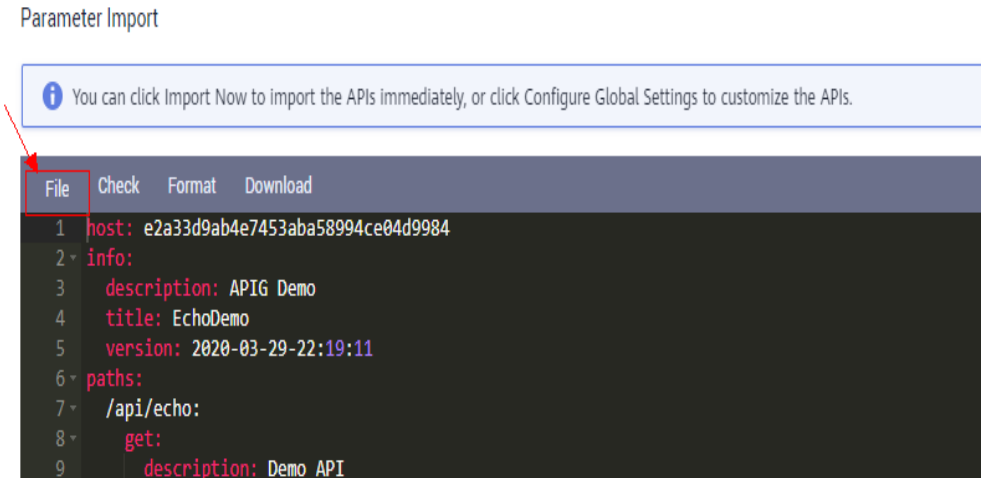
Tabla 3-16 Parámetros para importar API

Parámetro	Descripción
Import	Opciones: ● **New group**: Importar API a un nuevo grupo de API. Si selecciona esta opción, el sistema crea automáticamente un grupo de API e importa las API a este grupo. ● **Existing group**: Importar API a un grupo de API existente. Si selecciona esta opción, el sistema agrega las API al grupo de API seleccionado mientras conserva las API existentes en el grupo de API.
API group	Seleccione un grupo de API si establece **Import** en **Existing group**.
Basic Definition Overwrite	Determine si sobrescribir una API existente si el nombre de la API es el mismo que el de una API importada. Este parámetro sólo está disponible si se establece **Import** a **Existing group**.
Extended Definition Overwrite	Si se selecciona esta opción, los elementos de definición extendida (control de acceso y políticas de limitación de solicitudes) de una API importada sobrescribirán las políticas existentes con el mismo nombre.

Paso 8 En el área **Parameter Import**, haga clic en **File** y seleccione un archivo para importar.

Se admiten archivos YAML y JSON. Puedes obtener una vista previa del contenido de la API que se va a importar en la página **Import API**.

Figura 3-16 Importación de parámetros



Paso 9 (Opcional) Configure la configuración global de las API que se van a importar.

Puede configurar la configuración global de las API, como las solicitudes de frontend y backend, o modificar otros parámetros de las API.

Figura 3-17 Configuración de la ajuste global

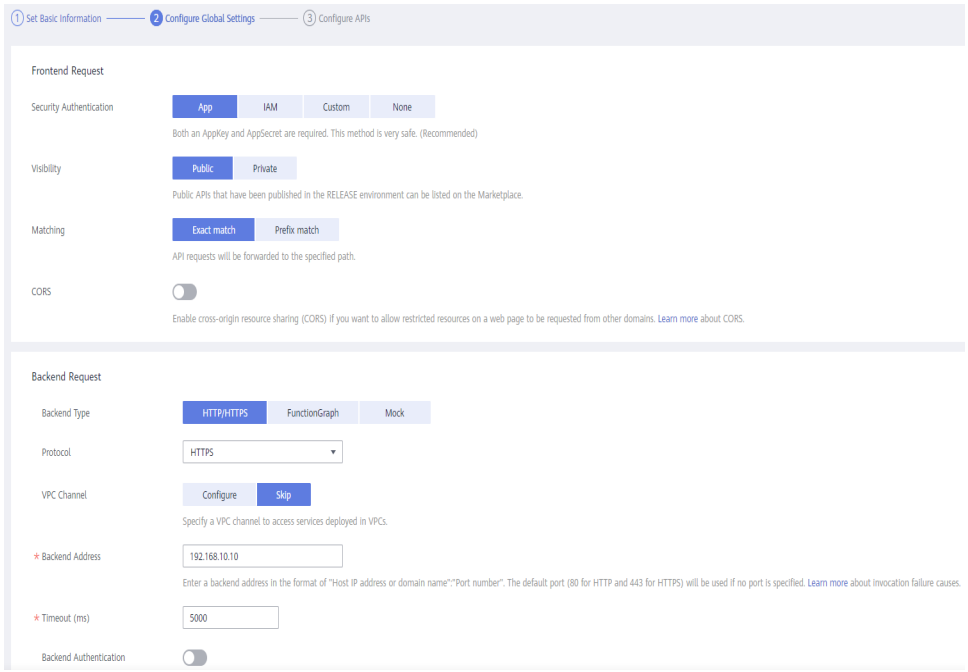
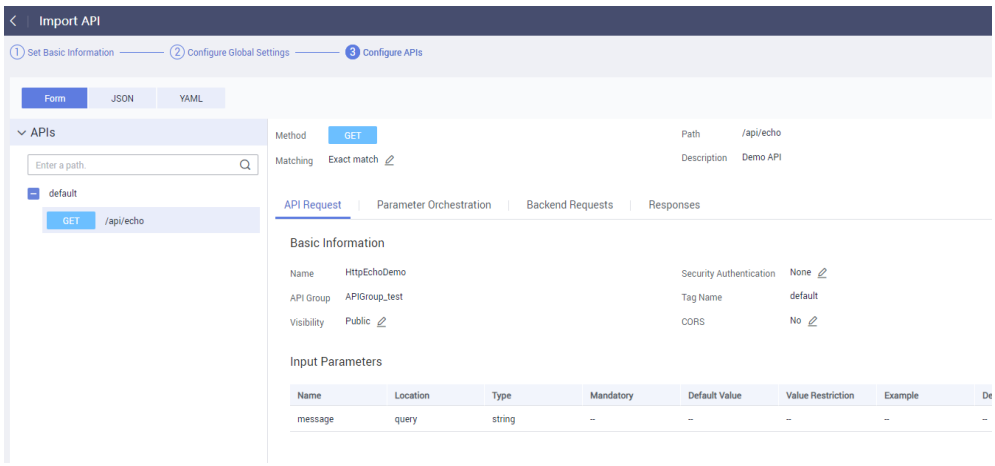


Figura 3-18 Modificación de APIs



Paso 10 Haga clic en **Import Now** para importar las API.

NOTA

Las API importadas deben publicarse manualmente para que los usuarios puedan acceder a ellas.

----Fin

Operaciones de seguimiento

Publique la API importada en un entorno para que pueda ser llamada por los usuarios.

3.2.9 Exportación de APIs

Escenario

Puede exportar API una por una o en lotes como archivos JSON o YAML.

Prerrequisitos

Ha creado un grupo de API y una API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 Haz clic en **Export API**.

Paso 6 Establezca los parámetros enumerados en **Tabla 3-17**.

Figura 3-19 Exportación de APIs

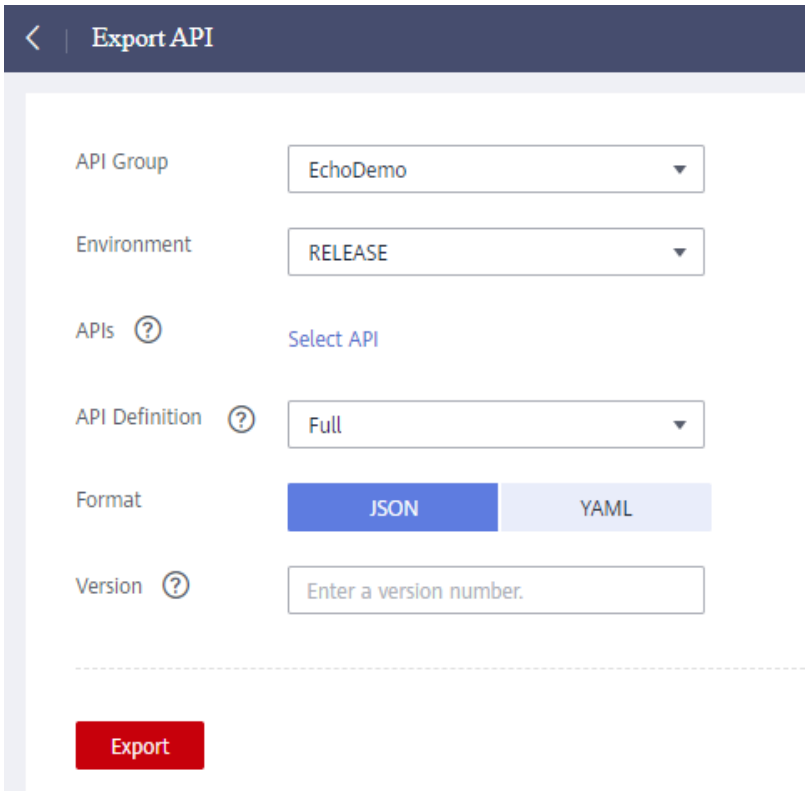


Tabla 3-17 Parámetros para exportar API

Parámetro	Descripción
API Group	Seleccione el grupo de API desde el que se exportarán las API.
Environment	Seleccione el entorno en el que se han publicado las API que se van a exportar.
APIs	De forma predeterminada, se exportan todas las API del grupo de API que se han publicado en el entorno seleccionado. Para exportar solo API específicas, haga clic en **Select API** y especifique las API que desea exportar.
API Definition	● **Basic**: La definición básica de una API se compone de las definiciones de solicitud y respuesta. No incluye la definición de backend. La definición de solicitud incluye campos Swagger estándar y extendido. ● **Full**: La definición completa de una API se compone de las definiciones de solicitud, backend y respuesta. ● **Extended**: la definición extendida de una API se compone de las definiciones de solicitud, backend y respuesta, así como la política de limitación de solicitud, política de control de acceso y otras configuraciones de la API.
Format	Exportar APIs en formato **JSON** o **YAML**.
Version	Establezca la versión de las API que se van a exportar. Si no especifica una versión, la versión se establecerá como la fecha y hora actuales.

Paso 7 Haga clic en **Export**.

El resultado de la exportación se muestra a la derecha.

----Fin

3.2.10 HTTP 2.0

API Gateway supports HTTP/2, which is a major revision of HTTP and was originally named HTTP 2.0. It provides binary encoding, request multiplexing over a single connection, and request header compression, improving transmission performance and throughput with a lower latency.

NOTA

- HTTP 2.0 strongly depends on network stability. To use HTTP 2.0, ensure that your network is stable and your client supports this protocol.
- Only dedicated gateways created after June 22, 2022 support HTTP 2.0. To use this protocol, contact technical support.

- Binary encoding

  Unlike HTTP 1.x where data is transmitted in text format, data in HTTP 2.0 is split into messages and frames for binary encoding. Compared with string (text) parsing, binary parsing is easier and less error-prone and delivers higher transmission performance.

- Multiplexing

  With binary encoding, HTTP 2.0 no longer relies on multiple connections to process and send requests and responses concurrently.

  For the same domain name, all requests are completed on a single connection, and each connection can process any number of messages. A message consists of one or more frames, which can be sent out of order and finally recombined based on the stream ID in the header of each frame. This shortens the latency and improves the efficiency.

- Header compression

  HTTP 2.0 uses an encoder to reduce the size of the headers to transmit. Both the client and server store a header field table to avoid transmitting same headers repeatedly, achieving high throughput.

3.3 Limitación de solicitudes

3.3.1 Creación de una política de limitación de solicitudes

Escenario

La limitación de solicitudes controla el número de veces que se puede llamar a una API dentro de un período de tiempo para proteger los servicios de backend.

Para proporcionar servicios estables e ininterrumpidos, puede crear políticas de limitación de solicitudes para controlar el número de llamadas realizadas a sus API.

Las políticas de limitación de solicitudes entran en vigor para una API solo si están vinculadas a la API.

NOTA

- Una API puede estar vinculada con una sola política de limitación de solicitudes para un entorno determinado, pero cada política de limitación de solicitudes puede estar vinculada a varias API.
- Para la puerta de enlace compartida, el límite de limitación de solicitud predeterminado es de 200 llamadas por segundo. Para una puerta de enlace dedicada, el límite es el valor de **ratelimit_api_limits** que ha configurado en la página **Configuration Parameters**.

Prerrequisitos

Ha **publicado la API** a la que desea vincular una política de limitación de solicitudes.

Creación de una política de limitación de solicitudes

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.

- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

Paso 6 Haga clic en **Create Request Throttling Policy**, y defina los parámetros enumerados en **Tabla 3-18**.

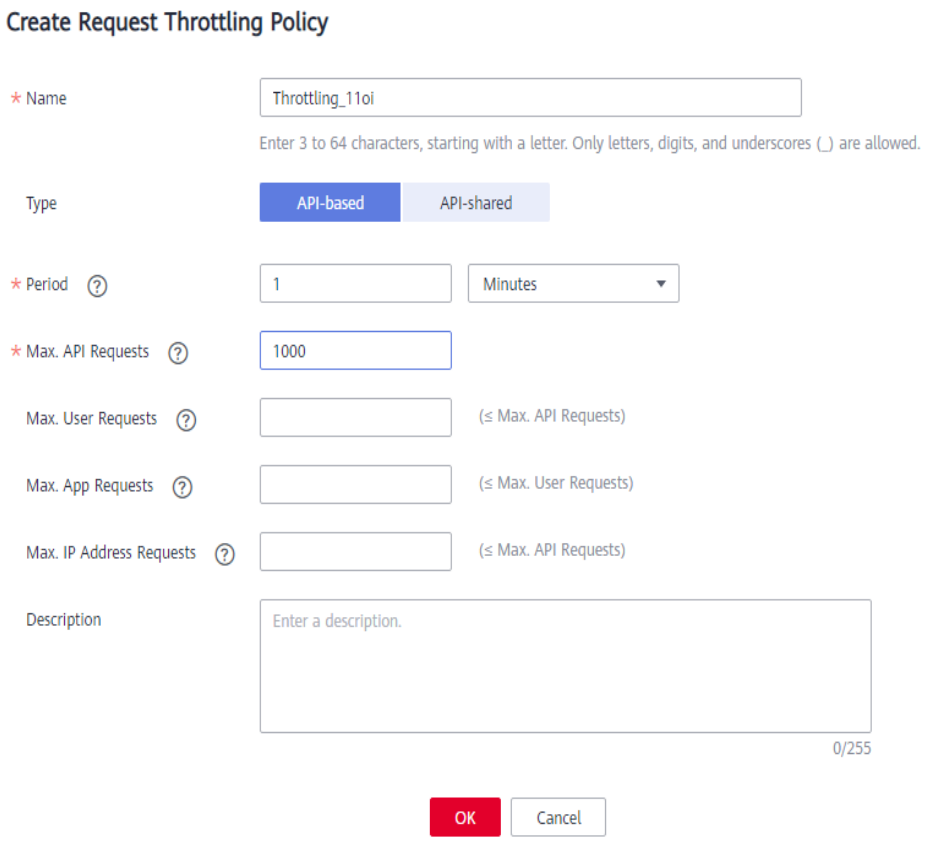


Tabla 3-18 Parámetros para crear una política de limitación de solicitudes

Parámetro	Descripción
Name	Solicitar el nombre de la política de limitación.
Type	Limitación de solicitudes basada en API o compartidas. ● **API-based**: La limitación de solicitudes se basa en cada API a la que está vinculada la política. ● **API-shared**: La limitación de solicitudes se basa en todas las API en su conjunto a las que está vinculada la política.

Parámetro	Descripción
Period	Durante cuánto tiempo desea limitar el número de llamadas a la API. Este parámetro se puede utilizar junto con los siguientes parámetros: ● **Max. API Requests**: Limitar el número máximo de veces que se puede llamar a una API dentro de un período específico. ● **Max. User Requests**: Limitar el número máximo de veces que un usuario puede llamar a una API dentro de un período específico. ● **Max. App Requests**: Limitar el número máximo de veces que una aplicación puede llamar a una API dentro de un período específico. ● **Max. IP Address Requests**: Limita el número máximo de veces que una API puede ser llamada por una dirección IP dentro de un período específico.
Max. API Requests	El número máximo de veces que se puede llamar a cada API enlazada dentro del período especificado. Este parámetro debe usarse junto con **Period**.
Max. User Requests	El número máximo de veces que un usuario puede llamar a cada API enlazada dentro del período especificado. **Este límite solo se aplica a las API a las que se accede a través de la autenticación IAM.** ● El valor de este parámetro no puede exceder el de **Max. API Requests**. ● Este parámetro debe usarse junto con **Period**. ● Si hay muchos usuarios bajo su cuenta que acceden a una API, los límites de limitación de solicitudes de la API se aplicarán a todos estos usuarios.
Max. App Requests	Número máximo de veces que una aplicación puede llamar a cada API enlazada dentro del período especificado. **Este límite solo se aplica a las API a las que se accede a través de la autenticación de aplicaciones.** ● El valor de este parámetro no puede exceder el de **Max. User Requests**. ● Este parámetro debe usarse junto con **Period**.
Max. IP Address Requests	El número máximo de veces que cada API enlazada puede ser llamada por una dirección IP dentro del período especificado. ● El valor de este parámetro no puede exceder el de **Max. API Requests**. ● Este parámetro debe usarse junto con **Period**.
Description	Descripción de la política de limitación de solicitudes.

Paso 7 Haga clic en **OK**.

Una vez creada la política, se muestra en la página **Request Throttling**. Puede vincular esta política a las API para limitar las solicitudes de API.

----Fin

Vinculación de una política de limitación de solicitudes a una API

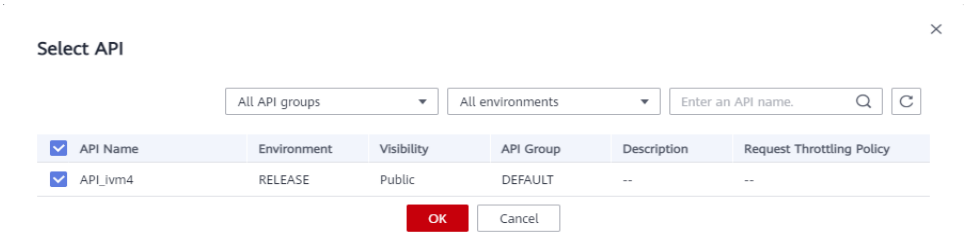
Paso 1 Vaya a la página para vincular una política de limitación de solicitudes a una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la política de limitación de solicitudes que se va a vincular, haga clic en **Bind to API**, y a continuación haga clic en **Select API**.
- Haga clic en el nombre de la política de limitación de la solicitud de destino y haga clic en **Select API** en la página de pestaña **APIs**.

Paso 2 Especifique un grupo de API, un entorno y una palabra clave de nombre de API para buscar la API deseada.

Paso 3 Seleccione la API y haga clic en **OK**.

Figura 3-20 Vinculación de una política de limitación de solicitudes a una API



NOTA

Si ya no se necesita una política de limitación de solicitudes para una API, puede desvincularla. Para desvincular una política de limitación de solicitudes de varias API, seleccione las API y haga clic en **Unbind**. Puede desvincular una política de limitación de solicitudes de un máximo de 1000 API a la vez.

----Fin

Creación, vinculación y desvinculación de una política de limitación de solicitudes llamando a una API

También puede crear una política de limitación de solicitudes, vincularla a las API o desvincularla de las API llamando a una API proporcionada por API Gateway. Para obtener más información, consulte las siguientes referencias:

Creación de una política de limitación de solicitudes

Vinculación de una política de limitación de solicitudes

Desvinculación de una política de limitación de solicitudes

Operaciones de seguimiento

Para controlar el número máximo de llamadas a la API recibidas de una aplicación o un inquilino específico, especifica la aplicación o el inquilino que quieres excluir haciendo referencia a **Adición de una aplicación o inquilino excluido**. Si se excluye una aplicación en una política de limitación de solicitudes, cualquier umbral configurado para esa aplicación tiene prioridad sobre la política de limitación de solicitudes. Los límites de API y de solicitud de usuario de esta política siguen siendo válidos. Si se excluye un inquilino en una política de

limitación de solicitud, se aplicará cualquier umbral configurado para ese inquilino. Los límites de solicitud de API y aplicación de esta política siguen siendo válidos.

3.3.2 Eliminación de una política de limitación de solicitudes

Escenario

Puede eliminar las políticas de limitación de solicitudes que ya no necesite.

Prerrequisitos

Ha creado una política de limitación de solicitudes.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

Paso 6 Eliminar una política de limitación de solicitud. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la política de limitación de solicitudes que desea eliminar, haga clic en **Delete**.
- Haga clic en el nombre de la política de limitación de solicitudes de destino y haga clic en **Delete** en la esquina superior derecha de la página de detalles de política de limitación de solicitudes que se muestra.

  NOTA

  - Si una política de limitación de solicitudes se ha vinculado a una API, desvincule la política y, a continuación, elimínela. Para desvincular una política de limitación de solicitudes, vaya a la página de detalles de la política, haga clic en **Unbind** en la fila que contiene la API de la que desea desvincular la política y haga clic en **Yes**.
  - Para eliminar varias directivas de limitación de solicitudes, seleccione las directivas y haga clic en **Delete**. Puede eliminar un máximo de 1000 políticas de limitación de solicitudes a la vez.

Paso 7 Haga clic en **Yes**.

----Fin

Eliminación de una política de limitación de solicitudes mediante llamada a una API

También puede eliminar una política de limitación de solicitudes llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Eliminación de una política de limitación de solicitudes**.

3.3.3 Adición de una aplicación o inquilino excluido

Escenario

Si quiere controlar el número de llamadas a la API recibidas de una aplicación o un inquilino específico, agregue una aplicación o un inquilino excluido a una política de limitación de solicitudes.

Prerrequisitos

Ha creado una aplicación u obtenido un ID de aplicación de otra cuenta o un ID de cuenta.

Adición de una aplicación excluida

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

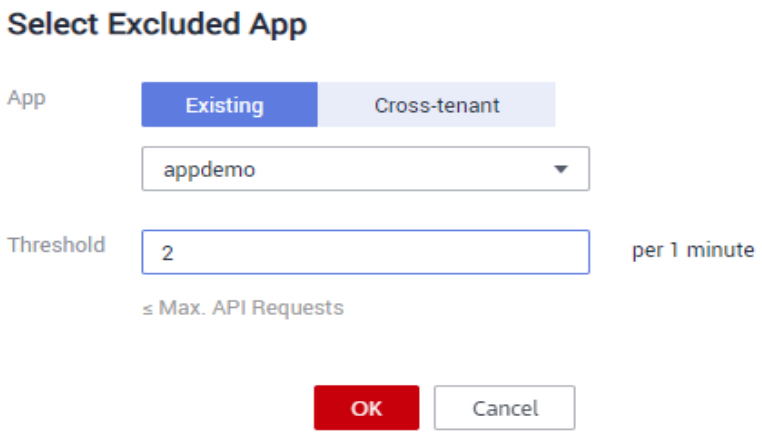
Paso 6 Haga clic en el nombre de la política de limitación de la solicitud de destino.

Paso 7 En la página de detalles de la política de limitación de solicitudes que se muestra, haga clic en la pestaña **Excluded Apps**.

Paso 8 Haz clic en **Select Excluded App**.

Paso 9 Seleccione una aplicación para excluirla. Puede utilizar uno de los métodos siguientes:

Figura 3-21 Adición de una aplicación excluida



- Para seleccionar una aplicación existente, haga clic en **Existing**, seleccione una aplicación e introduzca un umbral.
- Para seleccionar una aplicación de otros inquilinos, haz clic en **Cross-tenant**, e ingrese el ID de la aplicación y un umbral.

NOTA

El umbral debe ser un entero positivo y no puede exceder el valor de **Max. API Requests.**API Requests.

----Fin

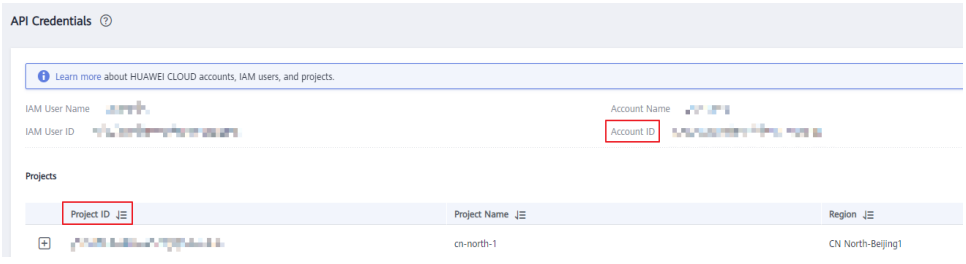
Adición de un inquilino excluido

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Sitúe el puntero del ratón sobre el nombre de usuario y elija **My Credentials** en la lista desplegable.

Paso 3 En la página **API Credentials**, consulte el ID de cuenta y el ID de proyecto.

Figura 3-22 Ver el ID de cuenta y el ID de proyecto



Paso 4 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 5 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 6 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.

- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 7 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

Paso 8 Haga clic en el nombre de la política de limitación de la solicitud de destino.

Paso 9 Haga clic en la pestaña **Excluded Tenants**.

Paso 10 Haga clic en **Select Excluded Tenant**.

Paso 11 En el cuadro de diálogo **Select Excluded Tenant**, establezca los parámetros enumerados en **Tabla 3-19**.

Figura 3-23 Adición de un inquilino excluido

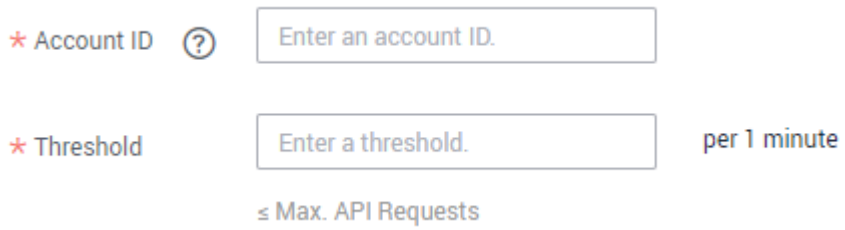


Tabla 3-19 Configuración de inquilino excluido

Parámetro	Descripción
Account ID	ID de cuenta o ID de proyecto obtenido en **Paso 3**. ● Introduzca un ID de proyecto si va a vincular o ha vinculado esta política a una API que utiliza autenticación de aplicación. ● Introduzca un ID de cuenta si va a vincular o ha vinculado esta política a una API que utiliza autenticación IAM.
Threshold	Número máximo de veces que una API puede ser llamada por el inquilino dentro de un período especificado. El valor de este parámetro no puede exceder el de **Max. API Requests**.

Paso 12 Haga clic en **OK**.

NOTA

Los umbrales de inquilinos excluidos tienen prioridad sobre el valor de **Max. API Requests**.User Requests.

Por ejemplo, supongamos que una política de limitación de solicitud está configurada, con **Max. API Requests** ser **10**, **Max. User Requests** ser **3**, **Period** ser 1 minuto, y dos inquilinos excluidos (máx. **2** solicitudes API para inquilino A y máx. **4** solicitudes API para el inquilino B). Si la política de limitación de solicitudes está vinculada a una API, los inquilinos A y B pueden acceder a la API 2 y 4 veces en un minuto, respectivamente.

----Fin

Adición de una aplicación o un inquilino excluidos mediante llamada a una API

También puede agregar una aplicación o un inquilino excluido a una política de limitación de solicitudes llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Creación de una configuración de regulación de solicitudes excluidas**.

3.3.4 Eliminación de una aplicación o un inquilino excluidos

Escenario

Puede eliminar aplicaciones o inquilinos excluidos de una política de limitación de solicitudes. Esta sección toma como ejemplo una aplicación excluida.

Prerrequisitos

- Ha creado una política de limitación de solicitudes.
- Ya ha añadido una aplicación o un inquilino excluido a la política de limitación de solicitudes.

Eliminación de una aplicación excluida

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

Paso 6 Haga clic en el nombre de la política de limitación de la solicitud de destino.

Paso 7 Haga clic en la pestaña **Excluded Apps** en la página de detalles de la política de limitación de solicitudes que se muestra.

Paso 8 En la columna **Operation** de la aplicación que desea eliminar, haga clic en **Remove**.

Paso 9 Haga clic en **Yes**.

----Fin

Eliminación de un inquilino excluido

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en ☰ en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Request Throttling**.

Paso 6 Haga clic en el nombre de la política de limitación de la solicitud de destino.

Paso 7 Haga clic en la pestaña **Excluded Tenants**.

Paso 8 En la columna **Operation** del inquilino que desea eliminar, haga clic en **Remove**.

Paso 9 Haga clic en **Yes**.

----Fin

Eliminación de una aplicación o un inquilino excluidos llamando a una API

También puede eliminar una aplicación o un inquilino excluido de una política de limitación de solicitudes llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Eliminación de una configuración de limitación de solicitudes excluida**.

3.4 Control de acceso

3.4.1 Creación de una política de control de acceso

Escenario

Las políticas de control de acceso son un tipo de medidas de seguridad proporcionadas por API Gateway. Puede usarlos para permitir o denegar el acceso a la API desde direcciones IP o cuentas específicas.

Las políticas de control de acceso entran en vigor para una API solo si están vinculadas a la API.

NOTA

Cada API puede estar vinculada con una sola política de control de acceso para un entorno determinado, pero cada política de control de acceso puede estar vinculada a varias API.

Creación de una política de control de acceso

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en ⌖ en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en ☰ en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Access Control**.

Paso 6 Haga clic en **Create Access Control Policy**.

Paso 7 En el cuadro de diálogo **Create Access Control Policy**, establezca los parámetros enumerados en **Tabla 3-20**.

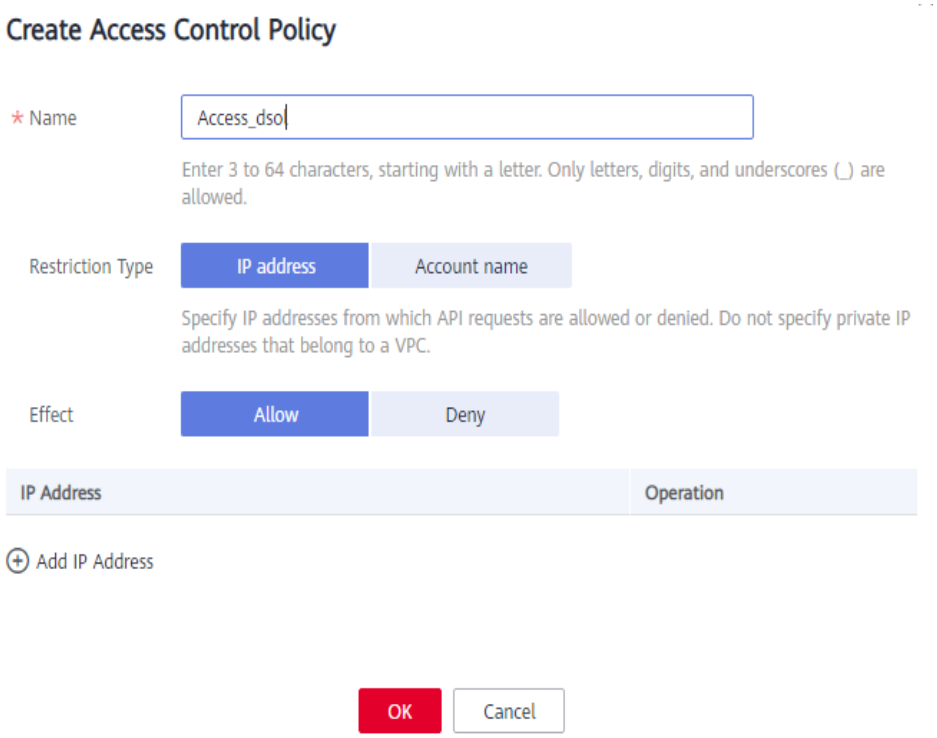


Tabla 3-20 Parámetros para crear una política de control de acceso

Parámetro	Descripción
Name	Nombre de política de control de acceso.
Restriction Type	Tipo de la fuente desde la que se van a controlar las llamadas a la API. ● **IP address** especifique las direcciones IP y los intervalos de direcciones IP a los que se permite o no se permite acceder a una API. ● **Account name**: especifique los nombres de las cuentas a las que se permite o no se permite acceder a una API.

Parámetro	Descripción
Effect	Opciones: **Allow** y **Deny**. Utilice este parámetro junto con **Restriction Type** para controlar el acceso de ciertas direcciones IP o cuentas a una API.
IP Address	Direcciones IP e intervalos de direcciones IP a los que se permite o no se permite acceder a una API Debe establecer este parámetro solo si ha establecido **Restriction Type** en **IP address**. **NOTA** Puede establecer un máximo de 100 direcciones IP respectivamente para permitir o denegar el acceso.
Account Names	Nombres de las cuentas a las que se permite o no se permite acceder a una API. **Este parámetro solo se aplica a las API a las que se accede a través de la autenticación IAM.** Debe establecer este parámetro solo si ha establecido **Restriction Type** en **Account name**. Puede introducir varios nombres de cuentas y separarlos con comas, por ejemplo, **aaa,bbb**. **NOTA** API Gateway realiza el control de acceso en las cuentas, no en los usuarios de IAM creados mediante cuentas.

Paso 8 Haga clic en **OK**. Puede vincular la política a las API para controlar el acceso a la API.

----Fin

Vinculación de una política de control de acceso a una API

Paso 1 Vaya a la página para vincular una política de control de acceso a una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la política de control de acceso que se va a vincular, haga clic en **Bind to API**, y a continuación, haga clic en **Select API**.
- Haga clic en el nombre de la política de control de acceso de destino y haga clic en **Select API**.

Paso 2 Especifique un grupo de API, un entorno y una palabra clave de nombre de API para buscar la API deseada.

Paso 3 Seleccione la API y haga clic en **OK**.

NOTA

Si ya no se necesita una política de control de acceso para una API, puede desvincularla de esa API. Para desvincular una política de control de acceso de varias API, seleccione las API y haga clic en **Unbind**. Puede desvincular una política de limitación de solicitudes de un máximo de 1000 API a la vez.

----Fin

3.4.2 Eliminación de una política de control de acceso

Escenario

Puede eliminar las políticas de control de acceso que ya no necesite.

Prerrequisitos

Ha creado una política de control de acceso.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Access Control**.

Paso 6 Elimine una política de control de acceso mediante uno de los métodos siguientes:

- En la columna **Operation** de la política de control de acceso que desea eliminar, haga clic en **Delete**.
- Haga clic en el nombre de la política de control de acceso de destino y haga clic en **Delete** en la esquina superior derecha de la página de detalles de política de control de acceso que se muestra.

NOTA

- Si una política de control de acceso se ha vinculado a las API, desvinúzcala y, a continuación, elimínela.
- Para eliminar varias directivas de control de acceso, seleccione las políticas y haga clic en **Delete**. Puede eliminar un máximo de 1000 políticas de control de acceso a la vez.

Paso 7 Haga clic en **Yes**.

----Fin

3.5 Gestión de entorno

3.5.1 Crear un entorno y una variable de entorno

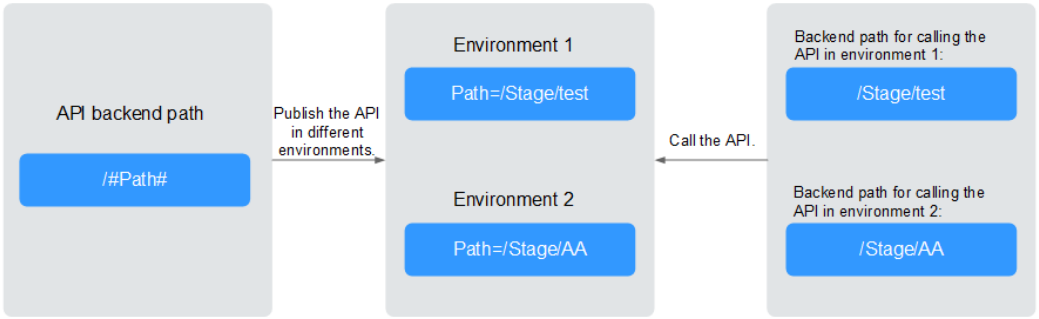
Escenario

Una API se puede llamar en diferentes entornos, como entornos de producción, pruebas y desarrollo. RELEASE es el entorno predeterminado proporcionado por API Gateway. Puede definir variables de entorno para permitir que se llame a una API en diferentes entornos.

Las variables de entorno son manejables y específicas para entornos. Puede crear variables en diferentes entornos para llamar a diferentes servicios de backend utilizando la misma API.

Para las variables que defina durante la creación de la API, debe crear las variables y los valores correspondientes. Por ejemplo, la variable **Path** se define para una API, y dos variables con el mismo nombre se crean y asignan los valores **//Stage/test** y **/Stage/AA** en los entornos 1 y 2, respectivamente. Si la API se publica y se llama en el entorno 1, se utiliza la ruta **/Stage/test**. Si la API se publica y se llama en el entorno 2, se utiliza la ruta **/Stage/AA**.

Figura 3-24 Uso de variables de entorno



NOTA

Puede crear un máximo de 50 variables para un grupo de API en cada entorno.

Prerrequisitos

Ha **creado un grupo de API**.

Creación de un entorno

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Environments**.

Paso 6 Haga clic en **Create Environment**, y defina los parámetros enumerados en **Tabla 3-21**.

Figura 3-25 Creación de un entorno

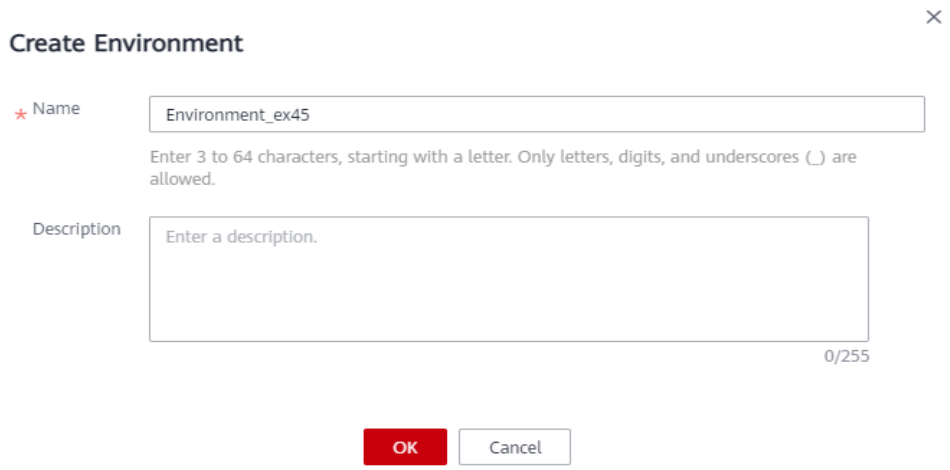


Tabla 3-21 Información del entorno

Parámetro	Descripción
Name	Nombre del entorno.
Description	Descripción del entorno.

Paso 7 Haga clic en **OK**.

Después de crear el entorno, se muestra en la lista de entornos.

----Fin

Acceso a un entorno

Puedes llamar a una API en el entorno RELEASE usando una RESTful API. Para acceder a la API en otros entornos, agregue el encabezado **X-Stage** a la solicitud para especificar un nombre de entorno. Por ejemplo, agregue **X-Stage:DEVELOP** al encabezado de solicitud para acceder a una API en el entorno **DEVELOP**.

NOTA

API Gateway no admite la depuración de API mediante variables de entorno.

Creación de una variable de entorno

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **API Groups**.

Paso 6 Cree una variable. Puede utilizar uno de los métodos siguientes:

- Haga clic en el nombre del grupo de API de destino y haga clic en la pestaña **Variables** de la página de detalles del grupo de API que se muestra.
- En la columna **Operation** del grupo API de destino, elija **More** > **Manage Variable**.

Paso 7 Seleccione un entorno en la lista desplegable **Environment** y haga clic en **Create Variable**.

Paso 8 Establezca los parámetros enumerados en **Tabla 3-22**.

Figura 3-26 Creación de una variable de entorno

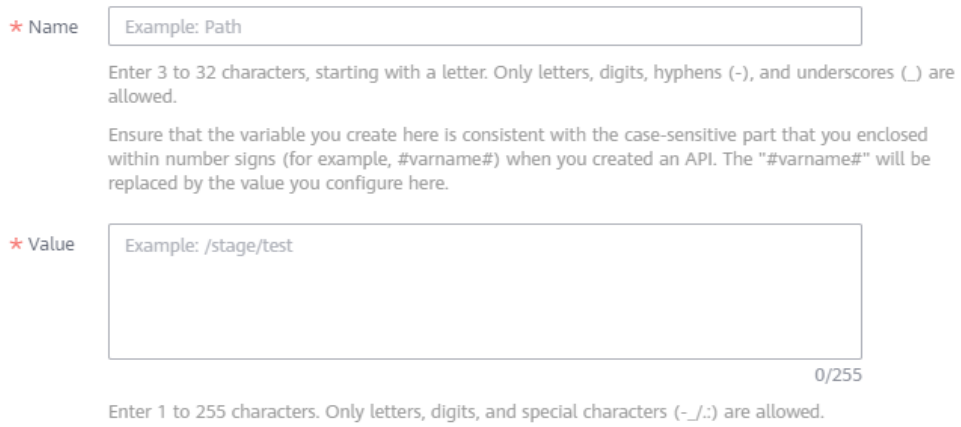


Tabla 3-22 Parámetros para crear una variable de entorno

Parámetro	Descripción
Name	Nombre de la variable que desea crear. Asegúrese de que el nombre es el mismo que el nombre de la variable definida para la API.
Value	La ruta de acceso que se va a utilizar en el entorno seleccionado.

Paso 9 Haga clic en **OK**.

NOTA

Si no se necesita una variable, haga clic en **Delete** en la fila que contiene la variable para eliminarla.

Los nombres y valores de las variables de entorno se mostrarán en texto sin formato en las solicitudes de API. No incluya información confidencial en los nombres y valores de las variables.

----Fin

Operaciones de seguimiento

Después de crear un entorno y una variable, **publique las API** en el entorno para que puedan ser llamadas por los llamantes de la API.

Creación de una variable de entorno y entorno mediante llamada a una API

También puede crear un entorno y una variable de entorno llamando a una API proporcionada por API Gateway. Para obtener más información, consulte las siguientes referencias:

Creación de un entorno

Creación de una variable de entorno

Preguntas frecuentes sobre las variables de entorno

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

3.5.2 Eliminación de un entorno

Escenario

Puede eliminar los entornos que ya no necesite.

Prerrequisitos

Usted ha creado un entorno.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **Environments**.

Paso 6 En la columna **Operation** del entorno que desea eliminar, haga clic en **Delete**.

NOTA

Puede eliminar un entorno solo si no se han publicado APIs en el entorno.

Paso 7 Haga clic en **Yes**.

----Fin

Eliminación de un entorno mediante llamada a una API

También puede eliminar un entorno llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Eliminación de un entorno**.

3.6 Gestión de clave de firma

3.6.1 Creación y uso de una clave de firma

Escenario

Los servicios de backend utilizan las claves de firma para verificar la identidad de API Gateway.

Una clave de firma consiste en una clave y un secreto, y solo se puede usar después de estar vinculada a una API. Cuando se llama a una API vinculada con una clave de firma, API Gateway agrega detalles de firma a la solicitud de API. El servicio backend de la API firma la solicitud de la misma manera y verifica la identidad de API Gateway comprobando si la firma es consistente con la del encabezado de **Authorization** enviado por API Gateway.

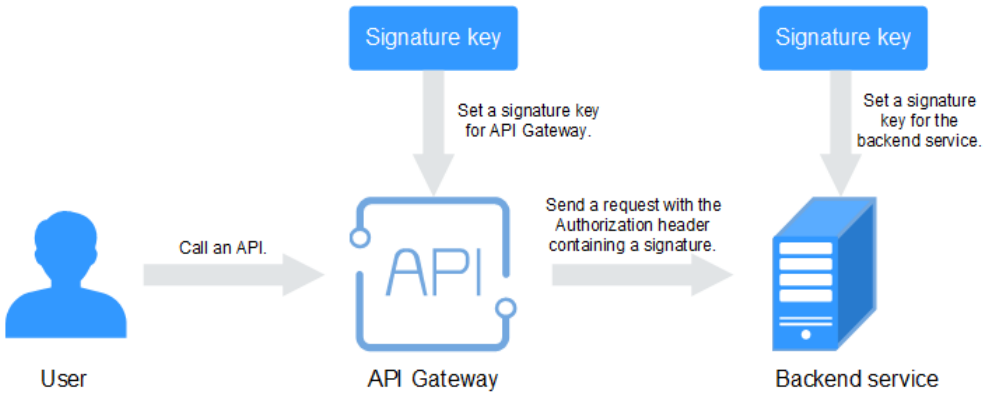
NOTA

Cada API solo se puede vincular con una clave de firma en un entorno determinado, pero cada clave de firma se puede vincular a varias API.

Procedimiento

1. Cree una clave de firma en la consola API Gateway.
2. Enlace la clave de firma a una API.
3. API Gateway envía solicitudes firmadas que contienen una firma en el encabezado **Authorization** al servicio de backend. El servicio backend puede utilizar diferentes lenguajes de programación (como Java, Go, Python, JavaScript, C#, PHP, C++, C, y Android) para firmar cada solicitud y comprobar si las dos firmas son consistentes.

Figura 3-27 Flujo de proceso de clave de firma



Creación de una clave de firma

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, seleccione **API Publishing** > **Signature Keys**.

Paso 6 Haga clic en **Create Signature Key**.

Paso 7 En el cuadro de diálogo **Create Signature Key**, establezca los parámetros enumerados en **Tabla 3-23**.

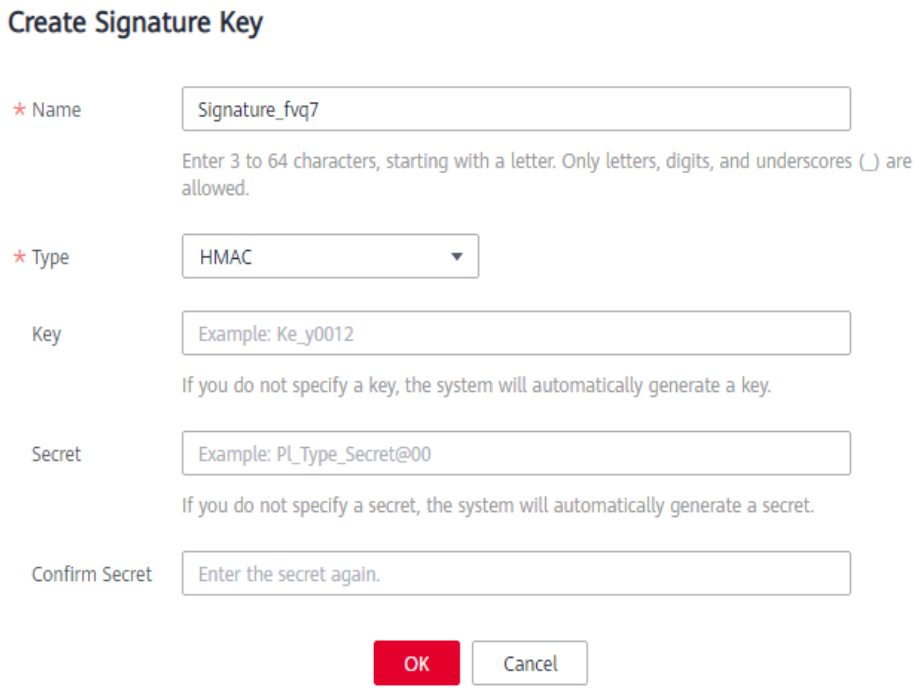


Tabla 3-23 Parámetros para crear una clave de firma

Parámetro	Descripción
Name	Nombre de clave de firma.
Type	Tipo de la clave de firma. Seleccione **HMAC** o **Basic**. Este parámetro solo está disponible para puertas de enlace dedicadas.

Parámetro	Descripción
Key	Combinado con **Secret** para formar un par de claves de firma. ● Si establece **Type** en **HMAC**, ingrese la clave del par de claves utilizado para la autenticación de código de autenticación de mensaje basado en hash (HMAC). ● Si establece **Type** en **Basic**, introduzca el nombre de usuario utilizado para la autenticación básica.
Secret	Combinado con **Key** para formar un par de claves de firma. ● Si establece **Type** en **HMAC**, introduzca el secreto del par de claves utilizado para la autenticación HMAC. ● Si establece **Type** en **Basic**, introduzca la contraseña utilizada para la autenticación básica.
Confirm Secret	Introduce el secreto de nuevo.

Paso 8 Haga clic en **OK**.

----Fin

Vinculación de una clave de firma a una API

Paso 1 En el panel de navegación, seleccione **API Publishing** > **Signature Keys**.

Paso 2 Enlace una clave de firma a una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la clave de firma que se vinculará a una API, haga clic en **Bind to API**.
- Haga clic en el nombre de la clave de firma de destino.

Paso 3 Haz clic en **Select API**.

Paso 4 Especifique un grupo de API, un entorno y una palabra clave de nombre de API para buscar la API deseada.

Paso 5 Seleccione la API y haga clic en **OK**.

NOTA

Si ya no se necesita una clave de firma para una API, desvíela de la API.

----Fin

Verificación del resultado de la firma

Firme cada solicitud de backend siguiendo las instrucciones en **Algoritmo de firma**, y compruebe si la firma de backend es coherente con la firma en el encabezado **Authorization** de la solicitud de API.

Creación de una clave de firma mediante llamada a una API

También puede crear una clave de firma mediante llamada a una API proporcionada por API Gateway. Para obtener más información, consulte **Creación de una clave de firma**.

3.6.2 Eliminación de una clave de firma

Escenario

Puede eliminar las claves de firma que ya no necesite.

Prerrequisitos

Ha creado una clave de firma.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, seleccione **API Publishing** > **Signature Keys**.

Paso 6 Eliminar una clave de firma. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la clave de firma que desea eliminar, haga clic en **Delete**.
- Haga clic en el nombre de la clave de firma de destino y haga clic en **Delete** en la esquina superior derecha de la página de detalles de la clave de firma mostrada.

NOTA

Si la clave de firma se ha enlazado a alguna API, desvíela y, a continuación, elimínela.

Paso 7 Haga clic en **Yes**.

----Fin

Eliminación de una clave de firma mediante llamada a una API

También puede eliminar una clave de firma llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Eliminación de una clave de firma**.

3.7 Gestión de canales de VPC

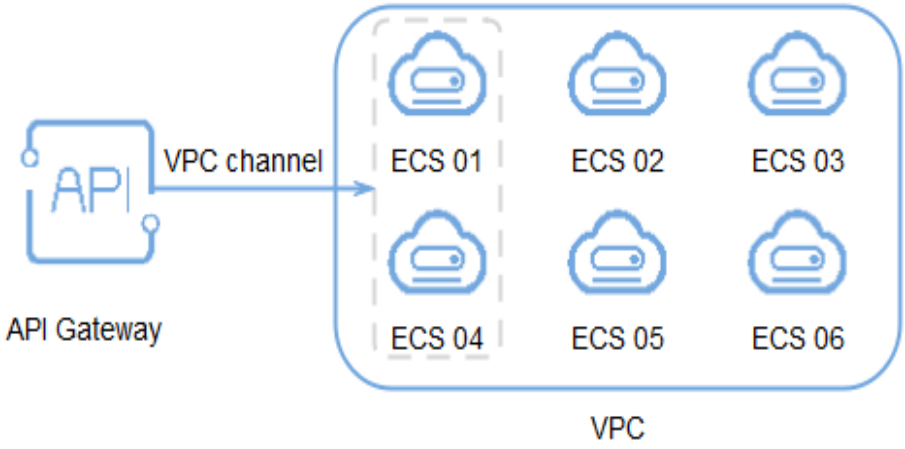
3.7.1 Creación de un canal de VPC

Escenario

Los canales de VPC permiten acceder a los servicios implementados en las VPC a través de sus subredes, lo que reduce la latencia y equilibra las cargas de los servicios de backend.

Después de crear un canal de VPC, puede configurarlo para una API con un servicio de backend HTTP/HTTPS. Por ejemplo, se han desplegado seis ECS en una VPC, y se ha creado un canal de VPC para alcanzar ECS 01 y ECS 04. API Gateway puede acceder a estos dos ECS a través del canal VPC.

Figura 3-28 Acceso a ECS en un canal de VPC a través de API Gateway



NOTA

Las puertas de enlace dedicadas admiten balanceadores de carga de red privada como canales VPC, mientras que la puerta de enlace compartida no.

Prerrequisitos

- Ha creado un servidor en la nube.
- Tiene el permiso de **VPC Administrator**.

Creación de un canal rápido

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **VPC Channels**.

Paso 6 Haga clic en **Create VPC Channel**, y establezca los parámetros enumerados en **Tabla 3-24**.

Figura 3-29 Creación de un canal de VPC

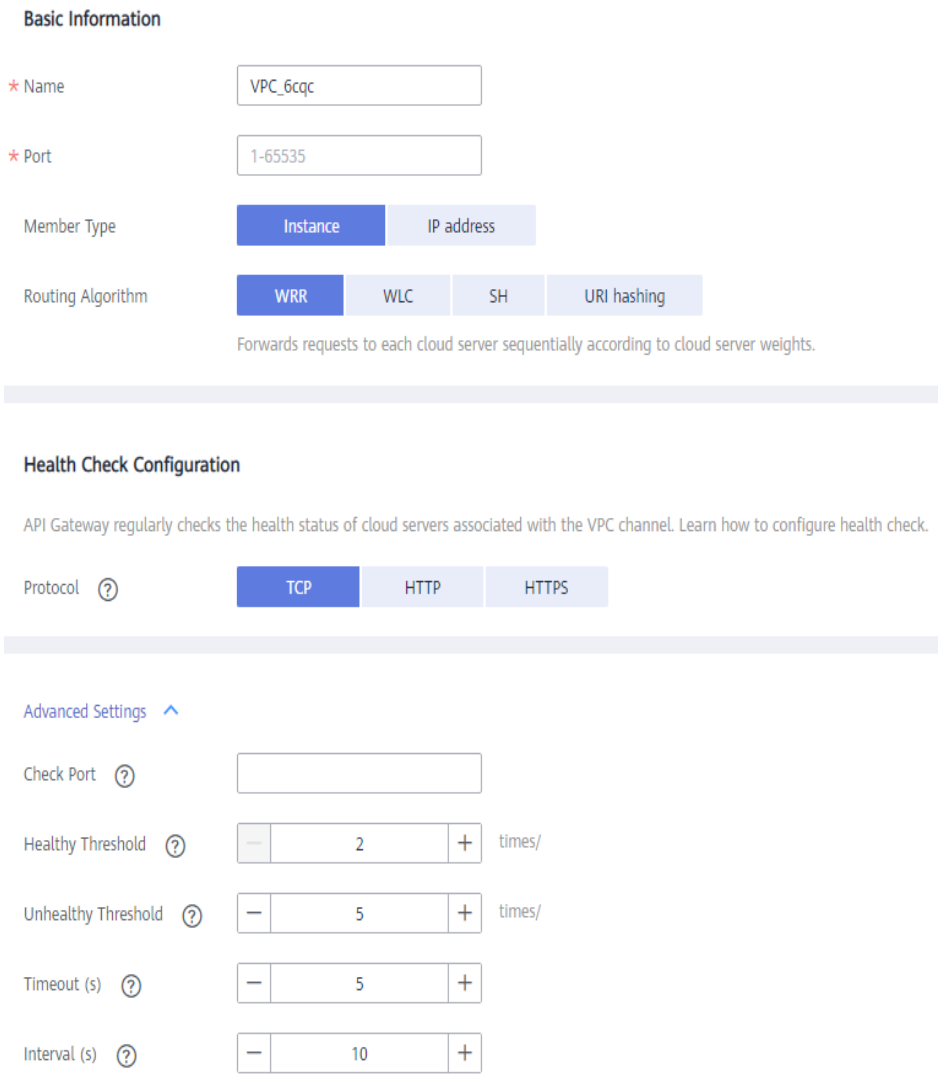


Tabla 3-24 Parámetros para crear un canal de VPC

Parámetro	Descripción
Name	Nombre del canal de VPC.
Port	El puerto host del canal VPC, es decir, el puerto del servicio backend. Rango: 1–65535.

Parámetro	Descripción
Member Type	Seleccione un método que desee utilizar para especificar servidores para el canal de VPC. El tipo de miembro es una configuración única y no se puede cambiar después de crear el canal de VPC. ● **Instance**: Seleccione servidores en la nube. ● **IP address**: Especifique las direcciones IP del servidor en la nube. Este parámetro solo está disponible para puertas de enlace dedicadas.
Routing Algorithm	El algoritmo que se utilizará para reenviar solicitudes a los servidores en la nube que seleccione. Los siguientes algoritmos de enrutamiento están disponibles: ● **WRR**: weighted round robin ● **WLC**: weighted least connection ● **SH**: source hashing ● **URI hashing**
Protocol	Protocolo utilizado para realizar comprobaciones de estado en servidores en la nube asociados con el canal VPC. Opciones: ● TCP ● HTTP ● HTTPS Valor predeterminado: **TCP**.
Path	La ruta de destino para las comprobaciones de estado. Establezca este parámetro solo cuando **Protocol** no se establezca en **TCP**.
Check Port	Puerto de destino para las comprobaciones de estado. De forma predeterminada, se utilizará el puerto del canal VPC.
Healthy Threshold	El número de comprobaciones exitosas consecutivas requeridas para que un servidor en la nube se considere saludable. Rango: 2–10. Valor predeterminado: **2**.
Unhealthy Threshold	El número de comprobaciones consecutivas fallidas requeridas para que un servidor en la nube se considere insalubre. Rango: 2–10. Valor predeterminado: **5**.
Timeout (s)	Tiempo de espera utilizado para determinar si una comprobación de estado ha fallado. Unidad: s. Rango: 2–30. Valor predeterminado: **5**.
Interval (s)	Intervalo entre comprobaciones consecutivas. Unidad: s. Rango: 5–300. Valor predeterminado: **10**.

Parámetro	Descripción
Response Codes	Los códigos HTTP utilizados para comprobar si hay una respuesta correcta de un destino. Establezca este parámetro solo cuando **Protocol** no se establezca en **TCP**.

Paso 7 Haga clic en **Next**.

Paso 8 Haga clic en **Select Cloud Server**.

Paso 9 Seleccione los servidores en la nube que desea agregar y haga clic en **OK**.

NOTA

Para garantizar una comprobación del estado y la disponibilidad del servicio con éxito, configure los grupos de seguridad de los servidores en la nube para permitir el acceso desde 100.125.0.0/16.

Paso 10 Haga clic en **Finish**.

----Fin

Creación de un canal de VPC mediante llamada a una API

También puede crear un canal de VPC llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Creación de un canal de VPC**.

Operaciones de seguimiento

Crear una API para los servicios de backend implementados en una VPC para equilibrar las cargas.

3.7.2 Eliminación de un canal de VPC

Escenario

Puede eliminar los canales de VPC que ya no necesite.

NOTA

Los canales de VPC que están actualmente en uso por las API publicadas no se pueden eliminar.

Prerrequisitos

Ha creado un canal de VPC.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **VPC Channels**.

Paso 6 Eliminar un canal de VPC. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** del canal de VPC que desea eliminar, haga clic en **Delete**.
- Haga clic en el nombre del canal de VPC de destino y haga clic en **Delete** en la esquina superior derecha de la página de detalles del canal de VPC que se muestra.

Paso 7 Haga clic en **Yes**.

----Fin

Eliminación de un canal de VPC mediante llamada a una API

También puede eliminar un canal de VPC mediante llamada a una API proporcionada por API Gateway. Para obtener más información, consulte **Elimiación de un canal de VPC**.

3.7.3 Edición de configuraciones de comprobación de estado

Escenario

Puede modificar las configuraciones de comprobación de estado de un canal de VPC para cumplir con los requisitos de servicio.

Prerrequisitos

Ha creado un canal de VPC.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **VPC Channels**.

Paso 6 Haga clic en el nombre del canal de VPC de destino,

Paso 7 Haga clic en la pestaña **Health Check**.

Paso 8 Haga clic en **Edit Health Check**.

Paso 9 En el cuadro de diálogo **Edit Health Check Configuration**, modifique los parámetros enumerados en **Tabla 3-25**.

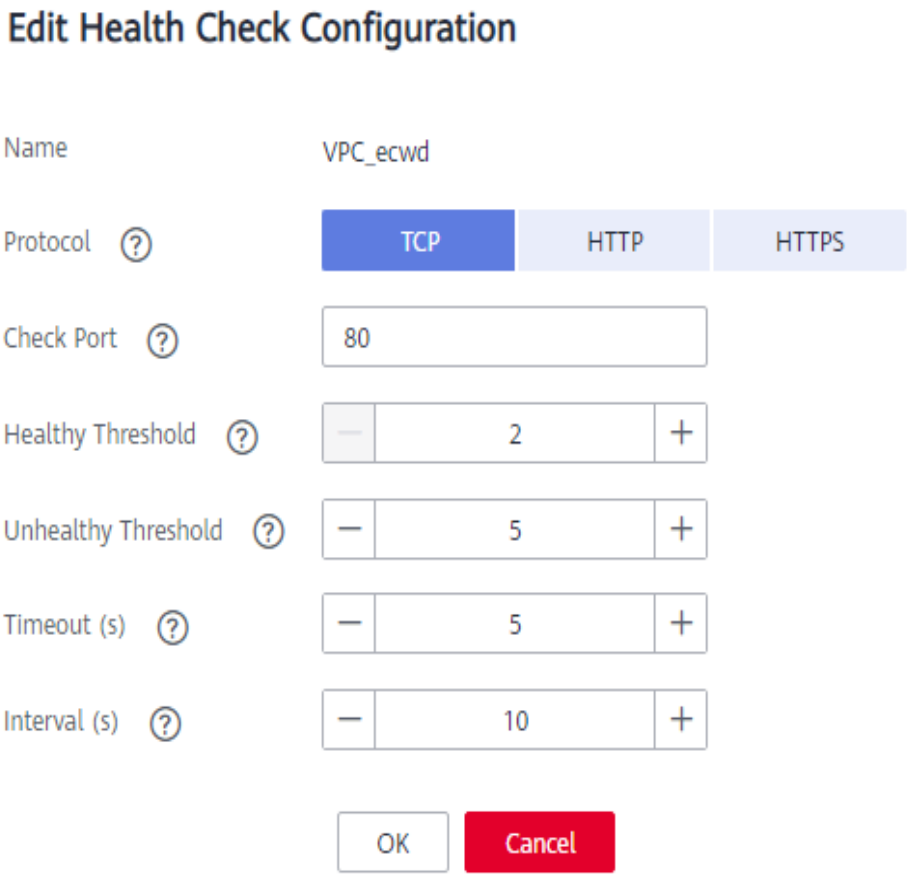


Tabla 3-25 Configuraciones de comprobación de estado

Parámetro	Descripción
Protocol	Protocolo utilizado para realizar comprobaciones de estado en servidores en la nube asociados con el canal VPC. Opciones: ● TCP ● HTTP ● HTTPS Valor predeterminado: **TCP**.
Path	La ruta de destino para las comprobaciones de estado. Establezca este parámetro solo cuando **Protocol** no se establezca en **TCP**.

Parámetro	Descripción
Check Port	Puerto de destino para las comprobaciones de estado. De forma predeterminada, se utilizará el puerto del canal VPC.
Healthy Threshold	El número de comprobaciones exitosas consecutivas requeridas para que un servidor en la nube se considere saludable. Rango: 2–10. Valor predeterminado: **2**.
Unhealthy Threshold	El número de comprobaciones consecutivas fallidas requeridas para que un servidor en la nube se considere insalubre. Rango: 2–10. Valor predeterminado: **5**.
Timeout (s)	Tiempo de espera utilizado para determinar si una comprobación de estado ha fallado. Unidad: s. Rango: 2–30. Valor predeterminado: **5**.
Interval (s)	Intervalo entre comprobaciones consecutivas. Unidad: s. Rango: 5–300. Valor predeterminado: **10**.
Response Codes	Los códigos HTTP utilizados para comprobar si hay una respuesta correcta de un destino. Establezca este parámetro solo cuando **Protocol** no se establezca en **TCP**.

Paso 10 Haga clic en **OK**.

----Fin

3.7.4 Edición de configuraciones de servidor en la nube de un canal de VPC

Escenario

Puede agregar o eliminar servidores en la nube y editar los pesos de los servidores en la nube para que los canales de VPC cumplan con los requisitos de servicio.

Prerrequisitos

Ha creado un canal de VPC.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **VPC Channels**.

Paso 6 Haga clic en el nombre del canal de VPC de destino.

Paso 7 Haga clic en la pestaña **Cloud Servers**.

Paso 8 Agregue o elimine servidores en la nube y edite los pesos de los servidores en la nube.

- Adición de servidores en la nube
  a. Haga clic en **Select Cloud Server**.
  b. Seleccione los servidores en la nube que desea agregar, establezca los pesos del servidor en la nube y haga clic en **OK**.

  NOTA

  Para garantizar una comprobación del estado y la disponibilidad del servicio con éxito, configure los grupos de seguridad de los servidores en la nube de backend para permitir el acceso desde 100.125.0.0/16.
- Eliminación de servidores en la nube
  a. En la columna **Operation** de los servidores en la nube que desea eliminar, haga clic en **Remove**.
  b. Haga clic en **Yes**.
- Edición del peso de un servidor en la nube
  a. En la columna **Weight** del servidor en la nube de destino, haga clic en  .
  b. Cambie el peso y haga clic en .
- Edición de los pesos de varios servidores en la nube
  a. Seleccione los servidores en la nube que se van a editar y haga clic en **Edit Weight**.
  b. Cambie los pesos de los servidores en la nube seleccionados y haga clic en **OK**.

----Fin

Edición de configuraciones de servidor en la nube de un canal de VPC mediante una llamada a una API

También puede editar las configuraciones del servidor en la nube de un canal de VPC llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Adición de instancias de backend (servidores en la nube)**.

3.8 Autorizadores personalizados

3.8.1 Creación de un autorizador personalizado

Escenario

API Gateway admite la autenticación personalizada de solicitudes tanto de front-end como de back-end.

- Autenticación personalizada de Frontend: Si ya tiene un sistema de autenticación, puede configurarlo en una función y luego crear un autorizador personalizado mediante la función para autenticar solicitudes de API.
- Autenticación personalizada de backend: Puede crear un autorizador personalizado para autenticar solicitudes para diferentes servicios de backend, eliminando la necesidad de personalizar APIs para diferentes sistemas de autenticación y simplificando el desarrollo de API. Solo necesita crear un autorizador personalizado basado en funciones en API Gateway para conectarse al sistema de autenticación backend.

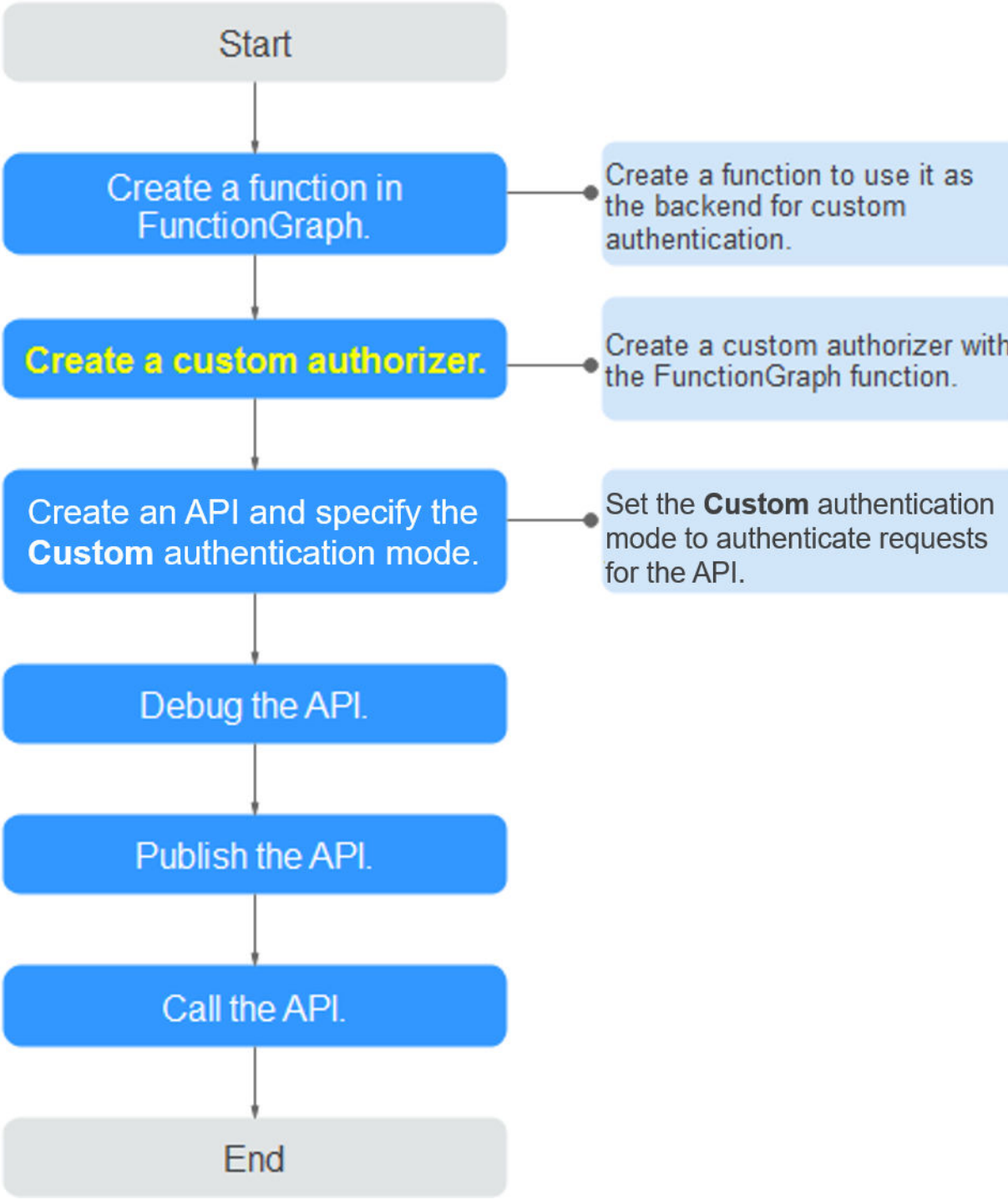
NOTA

La autenticación personalizada se implementa con FunctionGraph y no se admite si FunctionGraph no está disponible en la región seleccionada.

Para obtener más información sobre la autenticación personalizada, consulte *Guía del desarrollador*.

La siguiente figura muestra el proceso de llamar a las API a través de la autenticación personalizada.

Figura 3-30 Llamar a las API mediante autenticación personalizada



Prerrequisitos

- Ha creado una función de FunctionGraph.
- Tiene el permiso de **FunctionGraph Administrator**.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 Elija **API Publishing** > **Custom Authorizers**, and click **Create Custom Authorizer**.

Paso 6 Establezca los parámetros enumerados en **Tabla 3-26**.

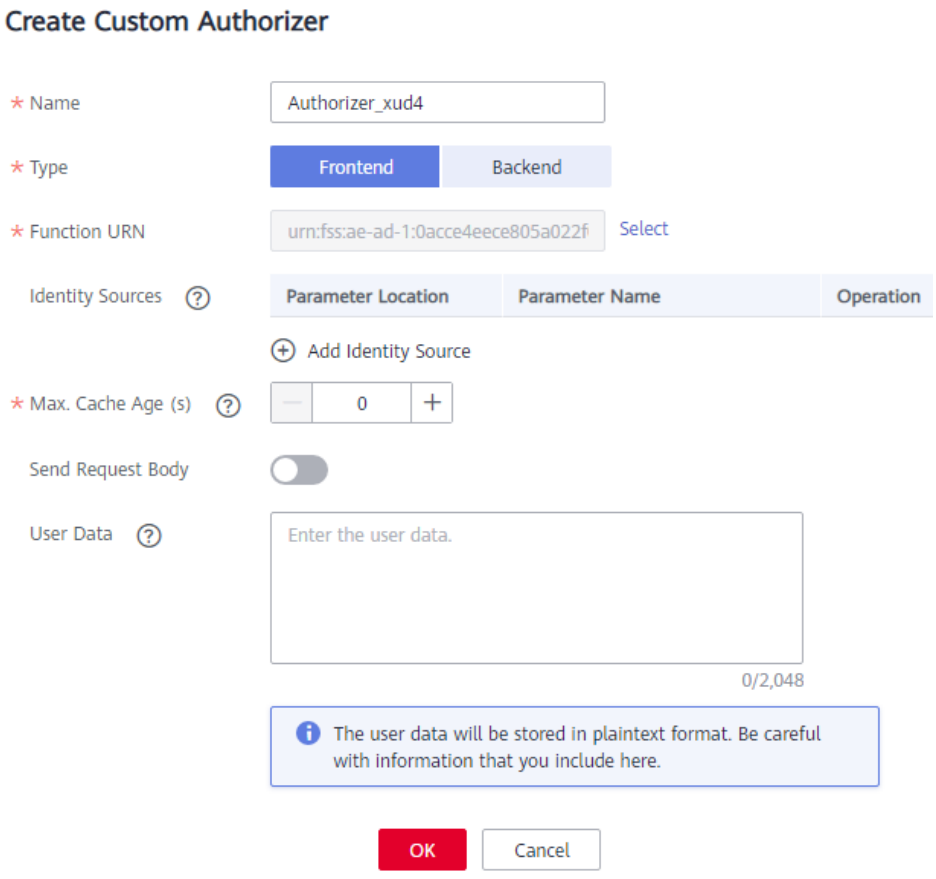


Tabla 3-26 Parámetros para crear un autorizador personalizado

Parámetro	Descripción
Name	Nombre del autor.

Parámetro	Descripción
Type	● **Frontend**: Autentica el acceso a las API. ● **Backend**: Autentica el acceso a los servicios backend.
Function URN	Seleccione una función de FunctionGraph.
Identity Sources	Solicite parámetros para la autenticación. Puede agregar encabezados y cadenas de consulta. Los nombres de encabezado no distinguen entre mayúsculas y minúsculas. Este parámetro solo es obligatorio si establece **Type** en **Frontend** y **Max.** Edad (es) de la caché es mayor que **0**. Cuando se utiliza la caché, este parámetro se utiliza como criterio de búsqueda para consultar resultados de autenticación.
Max. Cache Age (s)	El tiempo para almacenar los resultados de autenticación en caché. El valor **0** significa que los resultados de la autenticación no se almacenarán en caché. El valor máximo es **3600**.
Send Request Body	Determine si desea enviar el cuerpo de cada solicitud de API a la función de autenticación. Si habilita esta opción, el cuerpo de la solicitud se enviará a la función de autenticación del mismo modo que los encabezados y las cadenas de consulta. **NOTA** Esta opción solo está disponible para API gateways dedicados.
User Data	Parámetros de solicitud personalizados que se utilizarán junto con **Identity Sources** cuando API Gateway invoca una función.

Paso 7 Haga clic en **OK**.

----Fin

3.8.2 Eliminación de un autorizador personalizado

Escenario

Puede eliminar los autorizados personalizados que ya no necesite.

NOTA

- La autenticación personalizada se implementa con FunctionGraph y no se admite si FunctionGraph no está disponible en la región seleccionada.
- Los autorizadores personalizados que se han configurado para las API no se pueden eliminar.

Prerrequisitos

Ha **creado un autorizador personalizado**.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 Elija **API Publishing** > **Custom Authorizers**, y haga clic en **Delete** en la fila que contiene el autorizador personalizado que desea eliminar.

Paso 6 Haga clic en **Yes**.

----Fin

3.9 Plug-ins

3.9.1 Creación de un plug-in

API Gateway proporciona capacidades de extensión flexibles para API a través de plug-in.

Pautas para el uso de plug-ins

- Una API puede estar vinculada con un solo plug-in del mismo tipo.
- Los plug-ins son independientes de las API. Un plug-in tiene efecto para una API solo después de que se unen entre sí. Al vincular un plug-in a una API, debe especificar un entorno en el que se haya publicado la API. El plug-in solo tiene efecto para la API en el entorno especificado.
- Después de vincular un plug-in a una API, desvincular el plug-in de la API o actualizar el plug-in, no es necesario que vuelva a publicar la API.
- Tomar una API sin conexión no afecta a los plug-ins vinculados a ella. Los plug-ins siguen enlazados a la API si la API se publica de nuevo.
- Los plug-ins que se han enlazado a las API no se pueden eliminar.

Creación de un plug-in

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**. A continuación, haga clic en **Access Console** en la esquina superior derecha de una puerta de enlace dedicada.

Paso 5 En el panel de navegación, elija **API Publishing** > **Plug-ins**.

Paso 6 Haga clic en **Create Plug-in**.

En el cuadro de diálogo **Create Plug-in**, configure la información del plug-in.

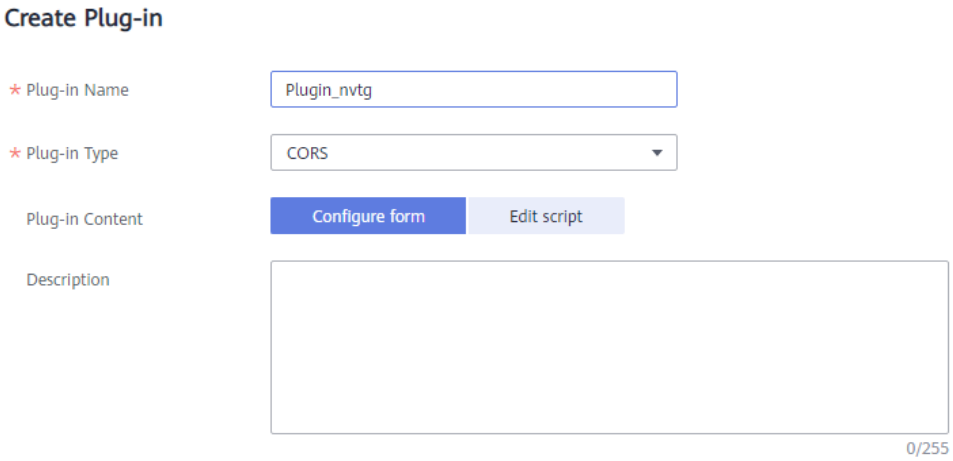


Tabla 3-27 Configuración de plug-in

Parámetro	Descripción
Plug-in Name	Nombre del plug-in que desea crear. Se recomienda que introduzca un nombre basado en ciertas reglas de nomenclatura para facilitar la identificación y la búsqueda.
Plug-in Type	Tipo del plug-in, que determina las capacidades de extensión del plug-in. ● **CORS**: especifica los encabezados de solicitud de comprobación previa y los encabezados de respuesta y crea automáticamente API de solicitud de comprobación previa para el acceso a la API de origen cruzado. ● **HTTP Response Headers**: le permite personalizar los encabezados de respuesta HTTP que se mostrarán en una respuesta de API. ● **Request throttling**: limita el número de veces que se puede llamar a una API dentro de un período de tiempo específico. Se admite la limitación basada en parámetros, básica y excluida.
Plug-in Content	Contenido del plug-in, que se puede configurar en un formulario o mediante un script. El contenido del plug-in varía según el tipo de plug-in: ● **CORS Plug-in** ● **Plugin de gestión de encabezados de respuesta HTTP** ● **Solicitud de plug-in de limitación**
Description	Descripción del plug-in.

Paso 7 Haga clic en **OK**.

Después de crear el plug-in, **enlácelo a la API** para la que el plug-in tendrá efecto.

----Fin

Vinculación de un plug-in a una API

Paso 1 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 2 Haz clic en el nombre de la API de destino para ir a la página de detalles de la API.

Paso 3 En la página de la pestaña **Plug-ins**, haga clic en **Bind**.

Paso 4 En el cuadro de diálogo **Bind Plug-in**, seleccione un entorno y un tipo de plug-in y seleccione el plug-in que desea vincular.

Paso 5 Haga clic en **OK**.

----Fin

3.9.2 CORS Plug-in

Por motivos de seguridad, el navegador restringe las solicitudes entre dominios para que no se inicien desde un script de página. En este caso, la página solo puede acceder a los recursos del dominio actual. CORS permite al navegador enviar XMLHttpRequest al servidor en un dominio diferente. Para obtener más información, consulte **CORS**.

El CORS plug-in proporciona las capacidades de especificar encabezados de solicitud de comprobación previa y encabezados de respuesta y crear automáticamente API de solicitud de comprobación previa para el acceso a la API de origen cruzado.

NOTA

Solo las puertas de enlace dedicadas creadas a partir del 10 de febrero de 2021 admiten el plug-in CORS. Para utilizar el CORS plug-in para puertas de enlace dedicadas creadas antes del 10 de febrero de 2021, comuníquese con el servicio de atención al cliente.

Directrices de uso

- Usted ha entendido las **Directrices para el uso de Plug-ins**.
- Las API con la misma ruta de solicitud en un grupo de API solo pueden vincularse con el mismo CORS plug-in.
- Si ha habilitado CORS para una API y también ha vinculado el plug-in CORS a la API, se utilizará el CORS plug-in.
- No puede vincular el CORS plug-in a API con la misma ruta de solicitud que otra API que utiliza el método OPTIONS.
- Cuando **enlaza un plug-in a una API**, asegúrese de que el método de solicitud de la API esté incluido en **allow_methods**.

Parámetros de configuración

Tabla 3-28 Parámetros de configuración

Parámetro	Descripción
allowed origins	Encabezado de respuesta **Access-Control-Allow-Origin**, que especifica un único origen, que indica a los navegadores que permitan que ese origen acceda a una API; o bien, para solicitudes sin credenciales, el comodín "*", para indicar a los navegadores que permitan que cualquier origen acceda a la API. Separe varios URI mediante comas.
allowed methods	Encabezado de respuesta **Access-Control-Allow-Methods**, que especifica los métodos HTTP permitidos al acceder a la API. Separe varios métodos usando comas.
allowed headers	Encabezado de respuesta **Access-Control-Allow-Headers**, que especifica los encabezados de solicitud que se pueden usar al crear un XMLHttpRequest. Separe varios encabezados usando comas. De forma predeterminada, los encabezados de solicitud simples **Accept**, **Accept-Language**, **Content-Language**, y **Content-Type** (solo si el valor es **application/x-www-form-urlencoded**, **multipart/form-data**, o **text/plain**) se llevan en las solicitudes. No es necesario configurar estos encabezados en este parámetro.
exposed headers	Encabezado de respuesta de **Access-Control-Expose-Headers**, que especifica qué encabezados de respuesta pueden estar contenidos en la respuesta de XMLHttpRequest. Separe varios encabezados usando comas. De forma predeterminada, los encabezados de respuesta básicos **Cache-Control**, **Content-Language**, **Content-Type**, **Expires**, **Last-Modified**, y **Pragma** pueden estar contenidos en la respuesta. No es necesario configurar estos encabezados en este parámetro.
maximum age	Encabezado de respuesta **Access-Control-Max-Age**, que especifica durante cuántos segundos se pueden almacenar en caché los resultados de una solicitud de comprobación previa. No se enviarán más solicitudes de comprobación previa dentro del período especificado.
allowed credentials	Encabezado de respuesta **Access-Control-Allow-Credentials**, que especifica si las solicitudes XMLHttpRequest pueden llevar a cookies.

Script de ejemplo

```
{
  "allow_origin": "*",
  "allow_methods": "GET,POST,PUT",
  "allow_headers": "Content-Type,Accept,Accept-Ranges,Cache-Control",
```



```
  "expose_headers": "X-Request-Id,X-Apig-Latency",
  "max_age": 172800,
  "allow_credentials": true
}
```

3.9.3 Plug-in de gestión de encabezados de respuesta HTTP

Los encabezados de respuesta HTTP son parte de la respuesta devuelta por API Gateway a un cliente que llama a una API. Puede personalizar los encabezados de respuesta HTTP que se incluirán en una respuesta de API.

NOTA

Solo las puertas de enlace dedicadas creadas a partir del 1 de junio de 2021 admiten el complemento de gestión de encabezados de respuesta HTTP. Para utilizar este complemento para puertas de enlace dedicadas creadas antes del 1 de junio de 2021, póngase en contacto con el servicio de atención al cliente.

Directrices de uso

No puede modificar los encabezados de respuesta, como **x-apig-*** y **x-request-id**, agregados por API Gateway, o los encabezados configurados para CORS.

Parámetros de configuración

Tabla 3-29 Parámetros de configuración

Parámetro	Descripción
Name	Nombre del encabezado de la respuesta, que no distingue entre mayúsculas y minúsculas y debe ser único dentro de un plug-in. Puede agregar un máximo de 10 encabezados de respuesta.
Value	Valor del encabezado de respuesta. Este parámetro no tiene efecto y puede dejarse en blanco si establece **Action** en **Delete**.

Parámetro	Descripción
Action	Operación del encabezado de respuesta. Puede anular, anexar, eliminar, omitir o agregar el encabezado especificado. **Override** ● El valor de este encabezado de respuesta anulará el del mismo encabezado que existe en una respuesta de API. ● Si una respuesta de API contiene varios encabezados con el mismo nombre que el que ha establecido aquí, solo se devolverá el valor del encabezado especificado. ● Si una respuesta de API no contiene el encabezado especificado, se devolverá el valor que establezca aquí. **Append** ● Si una respuesta de API contiene el encabezado especificado, se agregará el valor que establezcas aquí, siguiendo el valor existente. Los dos valores se separarán con comas (,). ● Si una respuesta de API contiene varios encabezados con el mismo nombre que el que estableces aquí, los valores de estos encabezados se separarán con comas (,) y seguidos por el valor del encabezado especificado. ● Si una respuesta de API no contiene el encabezado especificado, se devolverá el valor que establezca aquí. **Delete** ● Si una respuesta de API contiene el encabezado especificado, el encabezado se eliminará. ● Si una respuesta de API contiene varios encabezados con el mismo nombre que el que configuraste aquí, todos estos encabezados se eliminarán. **Skip** ● Si una respuesta de API contiene el encabezado especificado, el encabezado se omitirá. ● Si una respuesta de API contiene varios encabezados con el mismo nombre que el que ha establecido aquí, los valores de todos estos encabezados se devolverán sin modificación. ● Si una respuesta de API no contiene el encabezado especificado, se devolverá el valor que establezca aquí. **Add** El valor del encabezado especificado se devolverá incluso si el encabezado no existe en una respuesta de API.

Script de ejemplo

```
{
    "response_headers": [
        {
            "name": "test",
```



```
            "value": "test",
            "action": "append"
        },
        {
            "name": "test1",
            "value": "test1",
            "action": "override"
        }
    ]
}
```

3.9.4 Solicitud de plug-in de limitación

El plug-in de limitación de solicitudes limita el número de veces que se puede llamar a una API dentro de un período de tiempo específico. Soporta la limitación basada en parámetros, básica y excluida.

NOTA

Solo las puertas de enlace dedicadas creadas a partir del 4 de diciembre de 2021 admiten el plug-in de limitación de solicitudes. Para utilizar este plug-in para puertas de enlace dedicadas creadas antes del 4 de diciembre de 2021, póngase en contacto con el servicio de atención al cliente.

- Limitación básica

  Limita las solicitudes por API, usuario, aplicación o dirección IP de origen. Esta función es equivalente a una **política de limitación de solicitudes** pero es incompatible con ella.
- Limitación basada en parámetros

  Limitar las solicitudes basadas en encabezados, parámetros de ruta, métodos, cadenas de consulta o variables del sistema.
- Limitación excluida

  Limitar las solicitudes basadas en aplicaciones o inquilinos específicos.

Restricciones

- Una política de limitación de solicitudes no es válida si un plug-in de limitación de solicitudes está enlazado a la misma API que la política.
- Puede definir un máximo de 100 reglas de parámetros.
- El contenido del plug-in no puede exceder los caracteres 65,535.

Parámetros de configuración

Tabla 3-30 Parámetros de configuración

Parámetro	Descripción
Policy Type	● API-specific Supervise y controle las solicitudes de una única API. ● API-sharing Supervise y controle el total de solicitudes de todas las API vinculadas con el plug-in.

Parámetro	Descripción
Period	Durante cuánto tiempo desea limitar el número de solicitudes de API. ● **Max. API Requests**: Limite el número máximo de veces que se puede llamar a una API dentro de un período de tiempo específico. ● **Max. User Requests**: Limite el número máximo de veces que un usuario puede llamar a una API dentro de un período de tiempo específico. ● **Max. App Requests**: Limite el número máximo de veces que una aplicación puede llamar a una API dentro de un período de tiempo específico. ● **Max. IP Address Requests**: Limita el número máximo de veces que una dirección IP puede llamar a una API dentro de un período de tiempo específico.
Max. API Requests	El número máximo de veces que se puede llamar a cada API enlazada dentro del período especificado. Este parámetro debe usarse junto con **Period**.
Max. User Requests	El número máximo de veces que un usuario puede llamar a cada API enlazada dentro del período especificado. Para las API con autenticación IAM, la limitación se basa en un ID de proyecto; para las API con autenticación de aplicación, la limitación se basa en un ID de cuenta. Para obtener más información sobre los ID de cuenta y los ID de proyecto, consulte la descripción sobre **Excluded Tenants** en esta tabla. ● El valor de este parámetro no puede exceder el de **Max. API Requests**. ● Este parámetro debe usarse junto con **Period**. ● Si hay muchos usuarios bajo su cuenta que acceden a una API, los límites de limitación de solicitudes de la API se aplicarán a todos estos usuarios.
Max. App Requests	Número máximo de veces que una aplicación puede llamar a cada API enlazada dentro del período especificado. Este límite solo se aplica a las API a las que se accede a través de la autenticación de aplicaciones. ● El valor de este parámetro no puede exceder el de **Max. User Requests**. ● Este parámetro debe usarse junto con **Period**.
Max. IP Address Requests	El número máximo de veces que cada API enlazada puede ser llamada por una dirección IP dentro del período especificado. ● El valor de este parámetro no puede exceder el de **Max. API Requests**. ● Este parámetro debe usarse junto con **Period**.

Parámetro	Descripción
Parameter-based Throttling	Habilitar o deshabilitar la limitación basada en parámetros. Después de activar esta función, las solicitudes de API se reducen en función de los parámetros especificados.
Parameters	Defina los parámetros para las reglas de limitación. ● **Parameter Location**: la ubicación de un parámetro que se va a utilizar en una regla. – **path**: URI de solicitud de API. Este parámetro está configurado de forma predeterminada. – **method**: método de solicitud de API. Este parámetro está configurado de forma predeterminada. – **Header**: el valor del primer encabezado HTTP con el nombre del parámetro que ha establecido. – **Query**: el valor de la primera cadena de consulta con el nombre del parámetro establecido. – **System**: un parámetro de sistema. ● **Parameter Name**: el nombre de un parámetro para que coincida con el valor especificado en una regla.

Parámetro	Descripción
Rules	Definir reglas de limitación. Una regla consiste en condiciones, un límite de limitación de solicitudes de API y un período. Para agregar más reglas, haga clic en **Add Rule**. ● Condiciones Haga clic en  para establecer expresiones de condición. Para establecer una expresión, seleccione un parámetro y un operador e introduzca un valor. – =: igual a – **!=**: no es igual a – **pattern**: expresión regular – **enum**: valores enumerados. Separar varios valores con comas (,). ● Max. API Requests Número máximo de veces que se puede llamar a una API dentro de un período de tiempo específico. ● Period Un período de tiempo que se aplicará con el límite de limitación que establezca. Si no se especifica, se utilizará el período establecido en el área **Police Details**. Por ejemplo, configure el estrangulamiento basado en parámetros de la siguiente manera: agregue el parámetro **Host** y especifique la ubicación como **Header**; agregue la condición **Host = www.abc.com**, y establezca el límite de estrangulamiento en **10** y el período en 60s. Para las API cuyo parámetro **Host** en el encabezado de solicitud es igual a **www.abc.com**, no se pueden llamar de nuevo una vez que se les llama 10 veces en 60s.
Excluded Throttling	Habilitar o deshabilitar la limitación excluida. Después de habilitar esta función, los límites de limitación para los inquilinos y las aplicaciones excluidos anulan el valor **Max. User Requests** y **Max. App Requests** en la área **Basic Throttling**.
Excluded Tenants	**Tenant ID**: ID de cuenta o ID de proyecto. ● Especifique un ID de proyecto para una API con autenticación de aplicación. Para obtener más información, consulte **Obtención de un ID de proyecto**. ● Especifique un ID de cuenta (no un ID de usuario de IAM) para una API con autenticación de IAM. Para obtener más información, consulte **Obtención de un nombre de cuenta y ID de cuenta**. **Threshold**: el número máximo de veces que un inquilino específico puede acceder a una API dentro del período especificado. El umbral no puede exceder el valor de **Max.** . **API Requests** en el área **Basic Throttling**.

Parámetro	Descripción
Excluded Apps	Seleccione una aplicación y especifica el número máximo de veces que la aplicación puede acceder a una API dentro del período especificado. El umbral no puede exceder el valor de **Max.** . **API Requests** en el área **Basic Throttling**.

Script de ejemplo

```
{
  "scope": "basic",
  "default_interval": 60,
  "default_time_unit": "second",
  "api_limit": 100,
  "app_limit": 50,
  "user_limit": 50,
  "ip_limit": 20,
  "specials": [
    {
      "type": "app",
      "policies": [
        {
          "key": "2e421d76dc6c4c75941511ccf654e368",
          "limit": 10
        }
      ]
    },
    {
      "type": "user",
      "policies": [
        {
          "key": "878f1b87f71c40a7a15db0998f358bb9",
          "limit": 10
        }
      ]
    }
  ],
  "parameters": [
    {
      "type": "path",
      "name": "reqPath",
      "value": "reqPath"
    },
    {
      "type": "method",
      "name": "method",
      "value": "method"
    },
    {
      "type": "header",
      "name": "Host",
      "value": "Host"
    }
  ],
  "rules": [
    {
      "match_regex": "[\"Host\",\"==\",\"www.abc.com\"]",
      "rule_name": "rule-jlce",
      "time_unit": "second",
      "interval": 0,
      "limit": 5
    }
  ]
}
```


3.9.5 Eliminación de un plug-in

Escenario

Puede eliminar plug-ins que ya no necesite. Para eliminar un plug-in que se ha enlazado a las API, desvincule el plug-in de las API y, a continuación, elimínelo.

Prerrequisitos

Ha creado un plug-in.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**. A continuación, haga clic en **Access Console** en la esquina superior derecha de una puerta de enlace dedicada.

Paso 5 En el panel de navegación, elija **API Publishing** > **Plug-ins**.

Paso 6 Haga clic en el nombre del plug-in de destino para ir a la página de detalles del plug-in.

- Si el plug-in no está enlazado a ninguna API, haz clic en **Delete** en la esquina superior derecha.
- Si el plug-in está enlazado a las API, desvincule el plug-in de las API en el área **Bound APIs** y, a continuación, haga clic en **Delete** en la esquina superior derecha.

Paso 7 Haga clic en **Yes**.

----Fin

3.10 Monitoreo

3.10.1 Métricas de API Gateway

Introducción

En esta sección se describen las métricas que API Gateway reporta al Cloud Eye service. Puede ver métricas y alarmas usando la consola de Cloud Eye.

Espacio de nombres

Puerta de enlace compartida: SYS.APIG

Puerta de enlace dedicada: SYS.APIC

Métricas

Tabla 3-31 Métricas de puerta de enlace compartida

ID	Nombre	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (minuto)
avg_latency	Average Latency	Latencia media de la API.	≥ 0 Unidad: ms	API	1
input_throughput	Incoming Traffic	Tráfico entrante de la API.	≥ 0 Unidad: Byte, KB, MB o GB	API	1
max_latency	Maximum Latency	Latencia máxima de la API.	≥ 0 Unidad: ms	API	1
output_throughput	Outgoing Traffic	Tráfico saliente de la API.	≥ 0 Unidad: Byte, KB, MB o GB	API	1
req_count	Requests	Número de veces que se ha llamado a la API.	≥ 0	API	1
req_count_2xx	2xx Responses	Número de veces que la API devuelve una respuesta 2xx.	≥ 0	API	1
req_count_4xx	4xx Errors	Número de veces que la API devuelve un error 4xx.	≥ 0	API	1
req_count_5xx	5xx Errors	Número de veces que la API devuelve un error 5xx.	≥ 0	API	1
req_count_error	Total Errors	Número total de errores devueltos por la API.	≥ 0	API	1

Tabla 3-32 Métricas de puerta de enlace dedicadas

ID	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (minuto)
requests	Requests	Número de veces que se ha llamado a todas las API de una puerta de enlace dedicada.	≥0	Dedicated gateway	1
error_4xx	4xx Errors	Número de veces que todas las API de la puerta de enlace dedicada devuelven un error 4xx.	≥0	Dedicated gateway	1
error_5xx	5xx Errors	Número de veces que todas las API de la puerta de enlace dedicada devuelven un error 5xx.	≥0	Dedicated gateway	1
throttled_calls	Throttled API Calls	Número de veces que se han limitado todas las API de la puerta de enlace dedicada.	≥0	Dedicated gateway	1
avg_latency	Average Latency	Latencia media de todas las API en la puerta de enlace.	≥0 Unidad: ms	Dedicated gateway	1
max_latency	Maximum Latency	Latencia máxima de todas las API en la puerta de enlace.	≥0 Unidad: ms	Dedicated gateway	1
req_count	Requests	Número de veces que se ha llamado a una API.	≥ 0	API	1
req_count_2xx	2xx Responses	Número de veces que la API devuelve una respuesta 2xx.	≥ 0	API	1

ID	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (minuto)
req_count_4xx	4xx Errors	Número de veces que la API devuelve un error 4xx.	≥ 0	API	1
req_count_5xx	5xx Errors	Número de veces que la API devuelve un error 5xx.	≥ 0	API	1
req_count_error	Total Errors	Número total de errores devueltos por la API.	≥ 0	API	1
avg_latency	Average Latency	Latencia media de la API.	≥ 0 Unidad: ms	API	1
max_latency	Maximum Latency	Latencia máxima de la API.	≥ 0 Unidad: ms	API	1
input_throughput	Incoming Traffic	Tráfico entrante de la API.	≥ 0 Unidad: Byte, KB, MB o GB	API	1
output_throughput	Outgoing Traffic	Tráfico saliente de la API.	≥ 0 Unidad: Byte, KB, MB o GB	API	1

Dimensión

Tabla 3-33 Dimensión de monitoreo de puerta de enlace compartida

Clave	Valor
api_id	API

Tabla 3-34 Dimensiones de monitoreo de puerta de enlace dedicado

Clave	Valor
instance_id	Dedicated gateway
api_id	API

3.10.2 Creación de reglas de alarma

Escenario

Puede crear reglas de alarma para monitorear el estado de sus API.

Una regla de alarma consiste en un nombre de regla, objetos supervisados, métricas, umbrales de alarma, intervalo de supervisión y notificación.

Prerrequisitos

Se ha llamado a una API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Haga clic en el nombre de la API de destino.

Paso 7 En la página de la pestaña **Dashboard**, haga clic en **View Metric** para acceder a la consola de Cloud Eye. A continuación, cree una regla de alarma. Para obtener más información, consulte **Creación de una regla de alarma**.

----Fin

3.10.3 Visualización de las métricas

Escenario

Cloud Eye supervisa el estado de tus API y te permite ver sus métricas.

Prerrequisitos

Ha creado un grupo de API y una API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Publishing** > **APIs**.

Paso 6 Haga clic en el nombre de la API de destino.

Las métricas de la API se muestran en la página de pestaña **Dashboard**.

Paso 7 Haga clic en **View Metric** para ver más métricas en la consola de Cloud Eye.

NOTA

Los datos de monitoreo se conservan durante dos días. Para conservar los datos durante un período más largo, guárdelos en un bucket OBS.

----Fin

4 Llamadas a API

4.1 Gestión de app

4.1.1 Creación de una aplicación y obtención de autorización

Escenario

Para una API que usa autenticación de aplicaciones, puede crear una aplicación y usar la aplicación y su ID y su par de claves (AppKey y AppSecret) para llamar a la API. Puede usar una aplicación para llamar a una API solo después de vincular la aplicación a la API. Cuando llame a la API, reemplaza el par de claves del SDK con su propio par de claves para que API Gateway pueda autenticar su identidad. Para obtener más información sobre la autenticación de aplicaciones, consulte **Guía para desarrolladores**.

NOTA

- Si el modo de autenticación de la API de destino se ha establecido en **None** o **IAM**, no es necesario crear aplicaciones para llamar a esta API.

Creación de una aplicación

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Haga clic en **Create App** y configure la información de la aplicación.

Tabla 4-1 Información de la aplicación

Parámetro	Descripción
Name	Nombre de la aplicación.
Description	Descripción de la aplicación.

NOTA

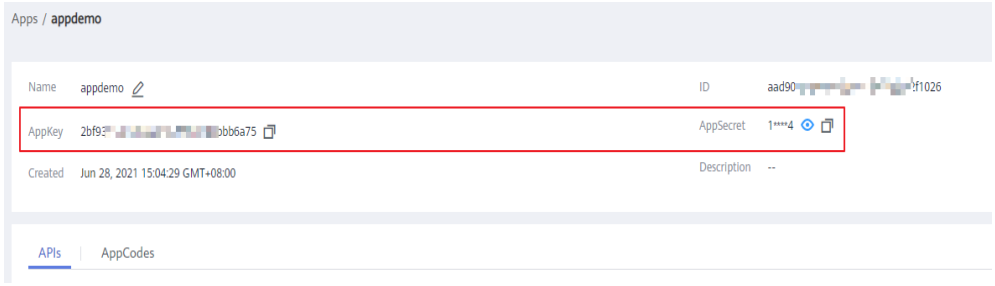
Puede personalizar AppKeys y AppSecrets en puertas de enlace dedicadas. Una AppKey es un identificador y debe ser globalmente único. Se genera automáticamente. No se recomienda personalizar uno a menos que sea necesario.

Paso 7 Haga clic en **OK**.

Después de crear la aplicación, su nombre y su ID se muestran en la lista de aplicaciones.

Paso 8 Haga clic en el nombre de la aplicación y vea AppKey y AppSecret en la página de detalles de la aplicación.

Figura 4-1 Detalles de la aplicación



----Fin

Vinculación de una aplicación a una API

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Enlace una aplicación a una API. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la aplicación, haz clic en **Bind to API**, y, a continuación, haz clic en **Select API**.
- Haz clic en el nombre de la aplicación de destino y haz clic en **Select API**.

Paso 7 Seleccione un entorno, seleccione una API y haga clic en **OK**.

Después de completar el enlace, puede ver la API en la página de detalles de la aplicación.

NOTA

- Solo las API que usan autenticación de aplicaciones pueden vincularse con las aplicaciones.
- Una aplicación puede estar vinculada a varias API que usan autenticación de aplicaciones, y cada una de estas API puede estar vinculada a varias aplicaciones.
- Para depurar una API a la que está vinculada la aplicación, haz clic en **Debug** en la fila que contiene la API.

----Fin

Creación de una aplicación mediante llamada a una API

También puede crear una aplicación mediante llamada a una API proporcionada por API Gateway. Para obtener más información, consulte la siguiente referencia:

Creación de una aplicación

Operaciones de seguimiento

Puede llamar a las API usando diferentes métodos de autenticación. Para más detalles, consulte **Llamadas a APIs**.

4.1.2 Eliminación de una App

Escenario

Puede eliminar aplicaciones que ya no necesite.

Prerrequisitos

Ha creado una aplicación.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en  en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en  en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.

- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Eliminar una aplicación. Puede utilizar uno de los métodos siguientes:

- En la columna **Operation** de la aplicación que desea eliminar, haga clic en **Delete**.
- Haz clic en el nombre de la aplicación de destino y haz clic en **Delete App** en la esquina superior derecha de la página de detalles de la aplicación mostrada.

NOTA

Si la aplicación está vinculada a alguna API, debes desvincularla y, a continuación, eliminarla.

Paso 7 Haga clic en **Yes**.

----Fin

Eliminación de una aplicación mediante llamada a una API

También puede eliminar una aplicación llamando a una API proporcionada por API Gateway. Para obtener más información, consulta **Eliminación de una App**.

4.1.3 Restablecimiento del AppSecret de una aplicación

Escenario

Puede restablecer el AppSecret de una aplicación. El AppKey es único y no se puede restablecer. Cuando restablece el AppSecret no es válido y no se puede llamar a las API vinculadas a la aplicación. Para volver a habilitar las llamadas a la API para esa aplicación, deberá actualizar el AppSecret de la aplicación que utilice.

Prerrequisitos

Ha creado una aplicación.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: Puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Haga clic en el nombre de la aplicación de destino.

Paso 7 En la esquina superior derecha de la página de detalles de la aplicación mostrada, haz clic en **Reset AppSecret**.

Paso 8 Haga clic en **Yes**.

----Fin

Restablecimiento de AppSecret llamando a una API

También puede restablecer el AppSecret de una aplicación llamando a una API proporcionada por API Gateway. Para obtener más información, consulte **Restablecimiento de AppSecret**.

4.1.4 Adición de un AppCode para una autenticación simple

Escenario

AppCodes son credenciales de identidad de una aplicación que se usa para llamar a las API en modo de autenticación simple. En este modo, el parámetro **X-Apig-AppCode** (cuyo valor es un AppCode en la página de detalles de la aplicación) se agrega al encabezado de solicitud HTTP para una respuesta rápida. API Gateway verifica solo el AppCode y el contenido de la solicitud no necesita estar firmado.

Cuando se llama a una API mediante autenticación de aplicación y se habilita la autenticación simple para la API, se pueden usar AppKey y AppSecret para firmar y verificar la solicitud de API. AppCode también se puede utilizar para la autenticación simple.

NOTA

- Por motivos de seguridad, la autenticación simple solo admite llamadas API a través de HTTPS.
- Puede crear un máximo de cinco AppCodes por cada aplicación.

Prerrequisitos

Ha creado una aplicación.

Generación de un AppCode

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

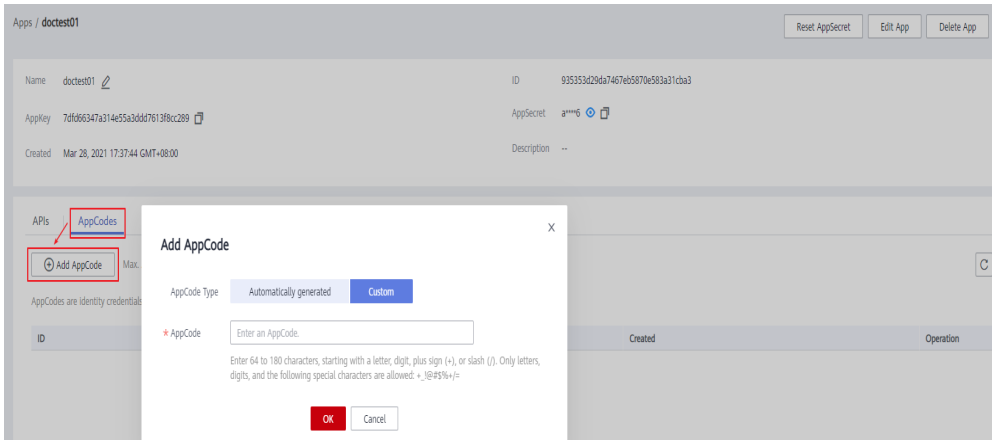
- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Haga clic en el nombre de la aplicación de destino.

Paso 7 Haga clic en la pestaña **AppCodes**.

Paso 8 Haga clic en **Add AppCode** para generar un archivo. Se puede generar o personalizar automáticamente.



----Fin

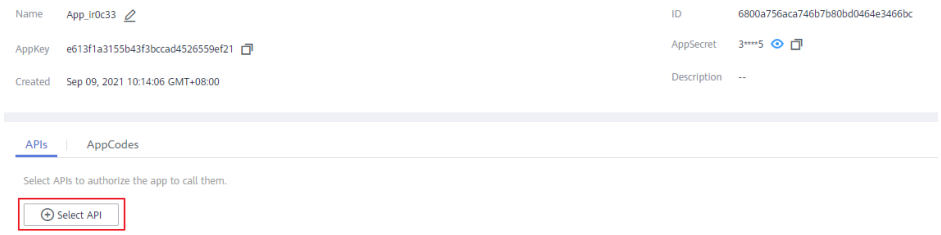
Uso de AppCode para la autenticación simple de solicitudes de API

Paso 1 Cuando cree una API, establezca **Security Authentication** en **App** y habilite **Simple Authentication**.

NOTA

Después de habilitar la autenticación simple para una API existente, debe publicar la API de nuevo para que la configuración surta efecto.

Paso 2 Enlace una aplicación a la API.



Paso 3 Cuando envíe una solicitud, agregue el parámetro **X-Apig-AppCode** al encabezado de la solicitud y omita la firma de la solicitud.

Por ejemplo, al usar curl, agregue el parámetro **X-Apig-AppCode** al encabezado de solicitud y establezca el valor del parámetro en el **AppCode generado**.

```
curl -X GET "https://api.exampledemo.com/testapi" -H "content-type: application/
json"  -H "host: api.exampledemo.com" -H "X-Apig-AppCode:
xhrJVJKABSOxc7d**********FZL4gSHEXkCMQC"
```

----Fin

4.1.5 Consulta de los detalles de la API

Escenario

Puede ver los detalles de una API a la que se ha enlazado una aplicación.

Prerrequisitos

- Ha creado una aplicación.
- La aplicación se ha vinculado a una API.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija un tipo de puerta de enlace en el panel de navegación.

- **Shared Gateway**: puede crear y gestionar API de inmediato. Se le facturará en función del número de llamadas API.
- **Dedicated Gateways**: puede crear y gestionar API después de comprar una puerta de enlace. Se le facturará en función de la duración del uso del gateway.

Paso 5 En el panel de navegación, elija **API Calling** > **Apps**.

Paso 6 Haga clic en el nombre de la aplicación de destino.

Paso 7 Haz clic en el nombre de la API de destino para ver sus detalles.

----Fin

4.2 Análisis de log

Escenario

Esta sección describe cómo obtener y analizar los registros de llamadas a la API de puertas de enlace dedicadas.

Prerrequisitos

Las APIs han sido llamadas.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en ☰ en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Dedicated Gateways**. A continuación, haga clic en **Access Console** en la esquina superior derecha de una puerta de enlace dedicada.

Paso 5 Elija **API Calling > Access Logs**, y haga clic en **Configure Log Collection**.

Paso 6 Habilitar la recopilación de registros ( ).

Paso 7 Especifique un grupo de registro y un flujo de registro y haga clic en **OK**. Para obtener más información acerca de los grupos de registros y las secuencias de registros, consulte **Gestión de log**.

Paso 8 Haga clic en **Log Fields** para ver la descripción de cada campo de registro. A continuación, vea y analice los registros haciendo referencia a las descripciones de los campos de registro.

Paso 9 Para exportar registros, consulte **Transferencia de Log**.

Los campos de los registros de acceso se separan mediante espacios. En la siguiente tabla se describe cada campo de registro.

Tabla 4-2 Descripción del campo de log

No.	Campo	Descripción
1	remote_addr	Dirección IP del cliente
2	request_id	ID de solicitud
3	api_id	ID de API
4	user_id	ID de proyecto proporcionado por un solicitante para la autenticación IAM
5	app_id	ID de la aplicación proporcionado por un solicitante para la autenticación basada en la aplicación
6	time_local	Hora en que se recibe una solicitud
7	request_time	Solicitar latencia
8	request_method	Método de solicitud HTTP
9	host	Nombre de dominio
10	router_uri	Solicitud de URI
11	server_protocol	Solicitud de protocolo
12	status	Código de estado de respuesta
13	bytes_sent	Tamaño de la respuesta en bytes, incluidos la línea de estado, el encabezado y el cuerpo.

No.	Campo	Descripción
14	request_length	Longitud de la solicitud en bytes, incluyendo la línea de inicio, el encabezado y el cuerpo.
15	http_user_agent	ID de agente de usuario
16	http_x_forwarded_for	Campo de encabezado X-Forwarded-For
17	upstream_addr	Dirección de backend
18	upstream_uri	URI de backend
19	upstream_status	Código de respuesta de backend
20	upstream_connect_time	Tiempo necesario para establecer una conexión con el backend
21	upstream_header_time	Duración desde el inicio del establecimiento de una conexión hasta la recepción del primer byte del backend
22	upstream_response_time	Duración desde el inicio del establecimiento de una conexión hasta la recepción del último byte del backend
23	region_id	ID de región

----Fin

4.3 SDKs

API Gateway admite la autenticación de API basada en IAM, aplicaciones y autorizadores personalizados. También puede optar por no autenticar las solicitudes de API. Para obtener más información sobre las diferencias entre los modos de autenticación, consulte **Cómo elegir un modo de autenticación**.

En esta sección se describe cómo descargar SDK y ver las instrucciones relacionadas.

Para obtener más información sobre la autenticación de IAM, consulte **Llamada a las API a través de la autenticación de IAM**.

Escenario

Los SDK se utilizan cuando se llama a las API a través de la autenticación de aplicaciones. Descargue los SDK y la documentación relacionada y, a continuación, llame a las API siguiendo las instrucciones de la documentación.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

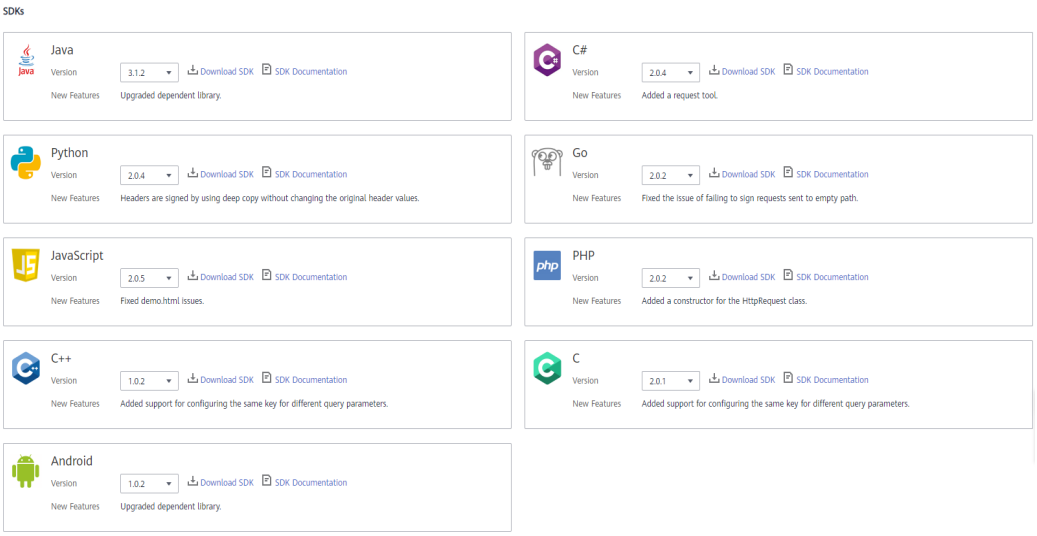
Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 Elija **Help Center** > **SDK Process Flow**.

Paso 5 Haga clic en **Download SDK** del idioma deseado.

Para ver la guía de soporte técnico, haga clic en **SDK Documentation**.



----Fin

4.4 APIs compradas

Escenario

En la puerta de enlace compartida, puede ver las API compradas y depurar las API para comprobar si se están ejecutando correctamente.

Las API compradas deben llamarse mediante autenticación de aplicaciones.

Prerrequisitos

Ha comprado APIs a través de KooGallery.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

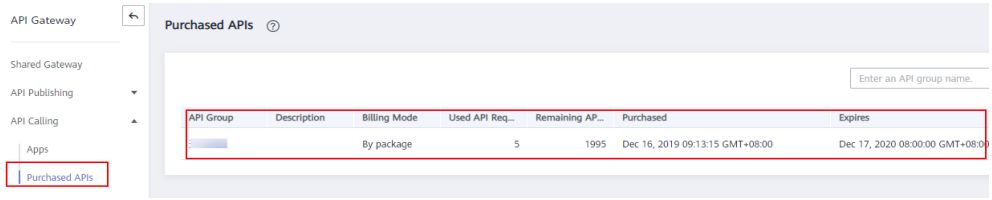
Paso 2 Haga clic en en la esquina superior izquierda y seleccione una región.

Paso 3 Haz clic en en la esquina superior izquierda y elige **API Gateway**.

Paso 4 En el panel de navegación, elija **Shared Gateway**.

Paso 5 En el panel de navegación, seleccione **API Calling** > **Purchased APIs**.

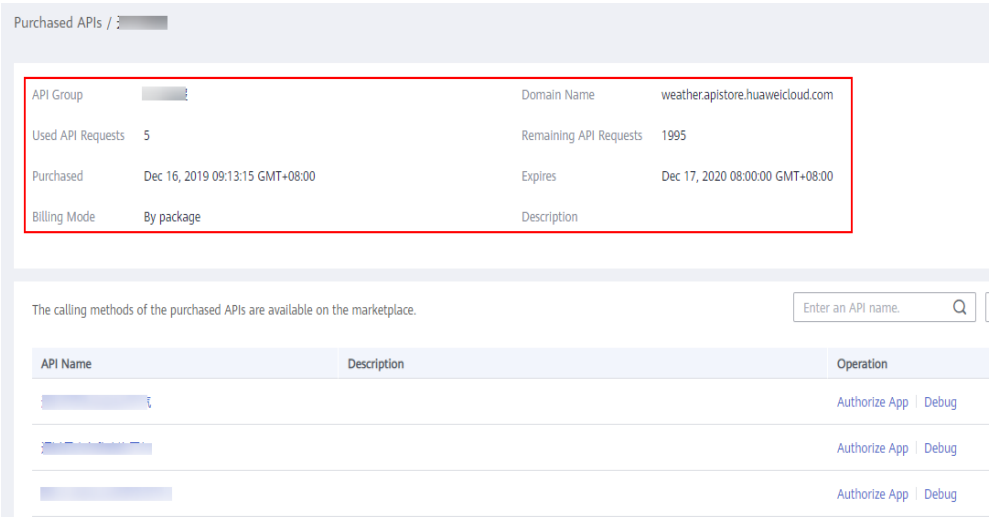
Figura 4-2 Grupo de API comprado



Paso 6 Haz clic en el nombre del grupo de API de destino.

Se muestran los detalles del grupo de API y las API compradas en el grupo.

Figura 4-3 Detalles del grupo API



Paso 7 En la columna **Operation** de la API deseada, haga clic en **Debug**.

Paso 8 En el lado izquierdo, establece los parámetros de solicitud de API enumerados en **Tabla 4-3**. En el lado derecho, consulta la información de solicitud y respuesta de la API después de hacer clic en **Send Request**.

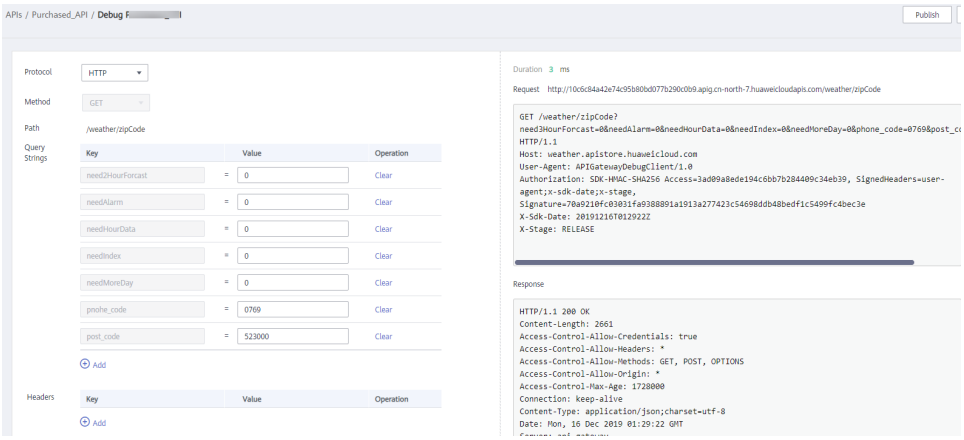
Tabla 4-3 Parámetros para la depuración de una API

Parámetro	Descripción
Protocol	Puede modificar este parámetro solo si ha establecido **Protocol** en **HTTP&HTTPS** para la API.
Method	Puede modificar este parámetro solo si ha establecido **Method** en **ANY** para la API.
Suffix	Puede modificar este parámetro solo si ha establecido **Matching** a **Prefix match** para la API.
Path Parameters	Puede modificar este parámetro sólo si el valor de **Path** contiene llaves ({}).

Parámetro	Descripción
Headers	Encabezados y valores HTTP.
Query Strings	Parámetros y valores de la cadena de consulta.
Body	Puede modificar este parámetro solo si ha establecido **Method** en **PATCH**, **POST** o **PUT** para la API.

Paso 9 Después de establecer los parámetros de solicitud, haga clic en **Send Request**.

La sección **Response** muestra la respuesta de la solicitud de API.



Paso 10 Puede enviar más solicitudes con diferentes parámetros y valores para verificar la API.

----Fin

4.5 Llamar a APIs publicadas

4.5.1 Llamadas a APIs

Obtención de APIs y documentación

Antes de llamar a las API, obtenga la información de solicitud del proveedor de API, incluidos el nombre de dominio de acceso, el protocolo, el método, la ruta de acceso y los parámetros de solicitud.

Obtenga APIs: de su empresa o de un socio

Obtenga la documentación relacionada:

- Para las API obtenidas de Huawei Cloud, obtenga la documentación del **Centro de ayuda**.

La información de autenticación a obtener varía con el modo de autenticación de API.

- Autenticación de aplicaciones:

  - Autenticación de firma: Obtén la clave y el secreto (o AppKey y AppSecret del cliente) de la aplicación autorizada para la API del proveedor de API, así como el SDK para llamar a la API.
  - Autenticación simple: obtenga el AppCode de la aplicación autorizada para la API del proveedor de API.
  - Otros modos de autenticación: Obtenga la clave y el secreto (o AppKey y AppSecret del cliente) de la aplicación autorizada para la API del proveedor de la API.
- Autenticación IAM: La credencial de cuenta (token o AK/SK obtenida con la cuenta y la contraseña) obtenida en la plataforma de servicio en la nube se utiliza para la autenticación. Si se utiliza AK/SK para la autenticación, también debe obtener el SDK del proveedor de API para llamar a la API.
- Autenticación personalizada: obtenga la información de autenticación personalizada que se incluirá en los parámetros de solicitud del proveedor de API.
- Ninguno: No se requiere información de autenticación.

Llamada a una API

NOTA

Esta sección describe solo la configuración de la ruta de acceso de solicitud y los parámetros de autenticación. Para otros parámetros, como el tiempo de espera y SSL, configúrelos según sea necesario. Para evitar pérdidas de servicio debido a parámetros incorrectos, configúrelos haciendo referencia a los estándares de la industria.

Paso 1 Establezca la ruta de la solicitud.

Escenario	Configuración de parámetros de solicitud
Llamar a una API con un nombre de dominio	Llama a la API mediante **el nombre de subdominio asignado al grupo de API o un nombre de dominio enlazado al grupo**. No se requiere ninguna configuración adicional.
Llamar a una API en el grupo DEFAULT con una dirección IP	En la puerta de enlace compartida, llame a una API del grupo DEFAULT con una dirección IP. No se requiere ninguna configuración adicional.

Escenario	Configuración de parámetros de solicitud
Llamar a una API en un grupo no-DEFAULT con una dirección IP	● Para llamar a las API mediante una dirección IP, asegúrese de que el parámetro **app_route** se ha establecido en **on** en la página de pestaña **Configuration Parameters** de la puerta de enlace dedicada. ● Para usar una dirección IP para llamar a una API que usa autenticación de aplicaciones en un grupo que no es DEFAULT, Agregue los parámetros de encabezado **X-HW-ID** y **X-HW-APPKEY** y establezca los valores de parámetro en la clave y el secreto de una aplicación autorizada para la API o un AppKey y AppSecret de cliente. ● Para usar una dirección IP para llamar a una API que no use autenticación de aplicación en un grupo que no sea DEFAULT, agregue el **host** de parámetros de encabezado.

Paso 2 Establezca los parámetros de autenticación.

Modo de autenticación	Configuración de parámetros de solicitud
App authentication (with a signature)	Use el SDK para firmar solicitudes de API. Para obtener más información, consulta la sección de **Llamar a las API a través de la autenticación de la aplicación**.
App authentication (through simple authentication)	Agregue el parámetro de encabezado **X-Apig-AppCode** y establezca el valor del parámetro en el AppCode obtenido en **Obtención de APIs y documentación**. Para obtener más información, consulte **Primeros pasos**.
App authentication (with app_api_key)	● Para habilitar la autenticación app_api_key, asegúrese de que el parámetro **app_api_key** se ha establecido en **on** en la página de pestaña **Configuration Parameters** de la puerta de enlace dedicada. ● Agregue el parámetro **apikey** del encabezado o cadena de consulta y establezca el valor del parámetro en la clave o AppKey obtenida en **Obtención de APIs y documentación**.

Modo de autenticación	Configuración de parámetros de solicitud
App authentication (with app_secret)	● En la página de pestaña **Configuration Parameters** de una puerta de enlace dedicada, el parámetro **app_secret** se ha establecido en **on** para habilitar la autenticación app_secret y **app_api_key** se ha establecido en **off** para deshabilitar la autenticación app_api_key. ● Agrega el parámetro de encabezado **X-HW-ID** y establece el valor del parámetro en la clave de la aplicación autorizada para la API o el AppKey cliente. ● Agregue el parámetro de encabezado **X-HW-AppKey** y establezca el valor del parámetro en el secreto o AppSecret obtenido en **Obtención de APIs y documentación**.
App authentication (with app_basic)	● Para habilitar la autenticación **app_basic**, asegúrese de que el parámetro app_basic se ha establecido en **on** en la página de pestaña **Configuration Parameters** de la puerta de enlace dedicada. ● Añada el parámetro de encabezado **Authorization** y ajuste el valor del parámetro a "Basic + base64 (*appkey* + : + *appsecret*)", en el que *appkey* y *appsecret* son la clave y el secreto (o AppKey y AppSecret que se obtiene en **Obtención de APIs y documentación**.
App authentication (with app_jwt)	● Para habilitar la autenticación app_jwt, asegúrese de que el parámetro **app_jwt** se ha establecido en **on** en la página de pestaña **Configuration Parameters** de la puerta de enlace dedicada. ● Agregue el parámetro de encabezado **Timestamp** y establezca el valor del parámetro en la marca de tiempo de Unix de la hora actual. ● Añada el parámetro de cabecera **Authorization** y ajuste el valor del parámetro a "sha256 (*appkey* + *appsecret* + *timestamp*) ", en el que *appkey* y *appsecret* son la clave y secreto (o AppKey y AppSecret) obtenidos en **Obtención de APIs y documentación** y *timestamp* es Unix timestamp de la hora actual.
IAM authentication (with a token)	Obtenga un token de la plataforma en la nube y lleve el token en las solicitudes de autenticación de la API. Para obtener más información, consulte la sección **Autenticación de token**.
IAM authentication (with AK/SK)	Use un SDK para firmar solicitudes de API. Para obtener más información, consulte **Autenticación de AK/SK**.

Modo de autenticación	Configuración de parámetros de solicitud
Custom authentication	Lleve información de autenticación en los parámetros de solicitud de API para la autenticación.
None	Llame a las API sin autenticación.

----Fin

4.5.2 Encabezado de respuesta

En la siguiente tabla se describen los encabezados de respuesta que API Gateway agrega a la respuesta devuelta cuando se llama a una API.

X-Apig-Mode: debug indica información de depuración de API.

Encabezado de respuesta	Descripción	Comentarios
X-Request-Id	ID de solicitud.	Se devuelve para todas las solicitudes válidas.
X-Apig-Latency	Duración desde el momento en que API Gateway recibe una solicitud hasta el momento en que el backend devuelve un encabezado de mensaje.	Se devuelve solo cuando el encabezado de la solicitud contiene **X-Apig-Mode: debug**.
X-Apig-Upstream-Latency	Duración desde el momento en que API Gateway envía una solicitud al backend hasta el momento en que el backend devuelve un encabezado de mensaje.	Se devuelve solo cuando el encabezado de la solicitud contiene **X-Apig-Mode: debug** y el tipo de backend no es Mock.
X-Apig-RateLimit-api	Información de límite de solicitud de API. Ejemplo: **remain:9,limit:10,time:10 second**.	Se devuelve solo cuando el encabezado de solicitud contiene **X-Apig-Mode: debug** y se ha configurado un límite para el número de veces que se puede llamar a la API.
X-Apig-RateLimit-user	Información de límite de solicitud de usuario. Ejemplo: **remain:9,limit:10,time:10 second**.	Se devuelve solo cuando el encabezado de solicitud contiene **X-Apig-Mode: debug** y se ha configurado un límite para el número de veces que un usuario puede llamar a la API.

Encabezado de respuesta	Descripción	Comentarios
X-Apig-RateLimit-app	Información de límite de solicitud de aplicación. Ejemplo: **remain:9,limit:10,time:10 second**.	Se devuelve solo cuando el encabezado de solicitud contiene **X-Apig-Mode: debug** y se ha configurado un límite para el número de veces que una aplicación puede llamar a la API.
X-Apig-RateLimit-ip	Información de límite de solicitud de dirección IP. Ejemplo: **remain:9,limit:10,time:10 second**.	Se devuelve solo cuando el encabezado de solicitud contiene **X-Apig-Mode: debug** y se ha configurado un límite para el número de veces que se puede llamar a la API mediante una dirección IP.
X-Apig-RateLimit-api-allenv	Información de límite de solicitud de API predeterminada. Ejemplo: **remain:199,limit:200,time:1 second**.	Se devuelve solo cuando el encabezado de la solicitud contiene **X-Apig-Mode: debug**.

4.5.3 Códigos de error

Tabla 4-4 enumera los códigos de error que puede encontrar al llamar a las API. Si se devuelve un código de error que comienza con **APIGW** después de llamar a una API, rectifique el error haciendo referencia a las instrucciones proporcionadas en **Códigos de error**.

NOTA

- Para obtener más información sobre los códigos de error que pueden producirse al gestionar las API, consulte **Códigos de error**.
- Si se produce un error al usar API Gateway, busque el mensaje de error y la descripción en la siguiente tabla de acuerdo con el código de error, por ejemplo, APIG.0101. Los mensajes de error están sujetos a cambios sin previo aviso.

Tabla 4-4 Códigos de error

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0101	The API does not exist or has not been published in the environment.	404	La API no existe o no se ha publicado en el entorno.	Compruebe si el nombre de dominio, el método y la ruta son consistentes con los de la API registrada. Compruebe si la API se ha publicado. Si se ha publicado en un entorno que no es de producción, compruebe si el encabezado X-Stage de la solicitud es el nombre del entorno. Compruebe si el nombre de dominio utilizado para llamar a la API está enlazado al grupo al que pertenece la API.
APIG.0101	The API does not exist.	404	El método de solicitud de API no existe.	Compruebe si el método de solicitud de API es el mismo que el método definido por la API.
APIG.0103	The backend does not exist.	500	No se encontró el servicio de backend.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0104	The plug-ins do not exist.	500	No se encontraron configuraciones de plug-in.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0105	The backend configurations do not exist.	500	No se encontraron configuraciones de backend.	Póngase en contacto con el servicio de asistencia técnica.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0106	Orchestration error.	400	Se ha producido un error de orquestación.	Comprueba si los parámetros frontend y backend de la API son correctos.
APIG.0201	API request error.	400	Parámetros de solicitud no válidos.	Establezca parámetros de solicitud válidos.
APIG.0201	Request entity too large.	413	El cuerpo de la solicitud supera los 12 MB.	Reduzca el tamaño del cuerpo de la solicitud.
APIG.0201	Request URI too large.	414	El URI de solicitud supera los 32 KB.	Reduzca el tamaño del URI de solicitud.
APIG.0201	Request headers too large.	494	Los encabezados de solicitud son demasiado grandes porque uno de ellos supera los 32 KB o la longitud total supera los 128 KB.	Reduzca el tamaño de los encabezados de solicitud.
APIG.0201	Backend unavailable.	502	El servicio de backend no está disponible.	Compruebe si la dirección de backend configurada para la API es accesible.
APIG.0201	Backend timeout.	504	El servicio de backend ha agotado el tiempo de espera.	Aumente la duración del tiempo de espera del servicio de backend o acorte el tiempo de procesamiento.
APIG.0201	An unexpected error occurred	500	Se ha producido un error interno.	Póngase en contacto con el servicio de asistencia técnica.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0202	Backend unavailable	502	El backend no está disponible.	Compruebe si el protocolo de solicitud de backend configurado para la API es el mismo que el protocolo de solicitud utilizado por el servicio de backend.
APIG.0203	Backend timeout.	504	El servicio de backend ha agotado el tiempo de espera.	Aumente el tiempo de espera del servicio backend o acorte su tiempo de procesamiento.
APIG.0204	SSL protocol is not supported: TLSv1.1	400	La versión del protocolo SSL no es compatible.	Utilice una versión de protocolo SSL compatible.
APIG.0301	Incorrect IAM authentication information.	401	Los detalles de autenticación de IAM son incorrectos.	Compruebe si el token es correcto.
APIG.0302	The IAM user is not authorized to access the API.	403	El usuario de IAM no tiene permitido acceder a la API.	Compruebe si el usuario está controlado por una lista de bloqueo o una lista de confianza.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0303	Incorrect app authentication information.	401	Los detalles de autenticación de la aplicación son incorrectos.	Compruebe si el método de solicitud, la ruta de acceso, las cadenas de consulta y el cuerpo de la solicitud son coherentes con los utilizados para la firma; compruebe si la fecha y la hora del cliente son correctas; y compruebe si el código de firma es correcto haciendo referencia a **Llamar a las API a través de la autenticación de la aplicación**.
APIG.0304	The app is not authorized to access the API.	403	La aplicación no tiene permitido acceder a la API.	Comprueba si la aplicación ha sido autorizada para acceder a la API.
APIG.0305	Incorrect authentication information.	401	La información de autenticación es incorrecta.	Compruebe si la información de autenticación es correcta.
APIG.0306	API access denied.	403	No se permite el acceso a la API.	Compruebe si tiene autorización para acceder a la API.
APIG.0307	The token must be updated.	401	El token necesita ser actualizado.	Obtenga un nuevo token de IAM.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0308	The throttling threshold has been reached.	429	Se ha alcanzado el umbral de estrangulamiento.	Inténtelo de nuevo después de que se reanude la regulación. Si se alcanza el número de solicitudes de subdominio por día, vincule un nombre de dominio independiente a la API.
APIG.0310	The project is unavailable.	403	El proyecto no está disponible en este momento.	Seleccione otro proyecto e inténtelo de nuevo.
APIG.0311	Incorrect debugging authentication information.	401	Los detalles de autenticación de depuración son incorrectos.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0401	Unknown client IP address.	403	No se puede identificar la dirección IP del cliente.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0402	The IP address is not authorized to access the API.	403	La dirección IP no está permitida para acceder a la API.	Compruebe si la dirección IP está controlada por una lista de bloqueo o una lista de confianza.
APIG.0404	Access to the backend IP address has been denied.	403	No se puede acceder a la dirección IP del servidor.	Compruebe si se puede acceder a la dirección IP del backend o a la dirección IP correspondiente al nombre de dominio del backend.
APIG.0501	The app quota has been used up.	405	Se ha alcanzado la cuota de aplicación.	Aumente la cuota de aplicaciones.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0502	The app has been frozen.	405	La aplicación ha sido congelada.	Compruebe si el saldo de su cuenta es suficiente.
APIG.0601	Internal server error.	500	Se ha producido un error interno.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0602	Bad request.	400	Solicitud no válida.	Compruebe si la solicitud es válida.
APIG.0605	Domain name resolution failed.	500	Error de resolución de nombre de dominio.	Compruebe si el nombre de dominio es correcto y está vinculado a una dirección de back-end correcta.
APIG.0606	Failed to load the API configurations.	500	No se pudieron cargar las configuraciones de API.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0607	The following protocol is supported: {xxx}	400	No se admite el protocolo. Solo se admite *xxx*. *xxx* está sujeto al valor real de la respuesta.	Use HTTP o HTTPS para acceder a la API.
APIG.0608	Failed to obtain the admin token.	500	Los detalles del inquilino no se pueden obtener.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0609	The VPC backend does not exist.	500	No se puede encontrar el servicio de backend de VPC.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0610	No backend available.	502	No hay servicios de backend disponibles.	Compruebe si todos los servicios de backend están disponibles. Por ejemplo, compruebe si la información de llamada a la API es consistente con la configuración real.

Código de error	Mensaje de error	Código de estado de HTTP	Descripción	Solución
APIG.0611	The backend port does not exist.	500	No se encontró el puerto de backend.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0612	An API cannot call itself.	500	Una API no puede llamarse a sí misma.	Modifique las configuraciones de backend y asegúrese de que la cantidad de capas a las que se llama recursivamente a la API no supere las 10.
APIG.0613	The IAM service is currently unavailable.	503	IAM no está disponible en este momento.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0705	Backend signature calculation failed.	500	Error en el cálculo de la firma de backend.	Póngase en contacto con el servicio de asistencia técnica.
APIG.0802	The IAM user is forbidden in the currently selected region	403	El usuario de IAM está deshabilitado en la región actual.	Póngase en contacto con el servicio de asistencia técnica.
APIG.1009	AppKey or AppSecret is invalid	400	El AppKey o AppSecret no es válido.	Compruebe si el AppKey o el AppSecret en la solicitud es correcto.

5 Gestión de permisos

5.1 Creación de un usuario y concesión de permisos de API Gateway

En este tema se describe cómo usar**Identity and Access Management** para implementar el control de permisos para los recursos de API Gateway. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tendrá sus propias credenciales de seguridad para acceder a los recursos de API Gateway.
- Conceda sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe una cuenta de Huawei Cloud o un servicio en la nube para realizar operaciones de operación en sus recursos de API Gateway.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita este capítulo.

En esta sección se describe el procedimiento para conceder permisos (consulte **Figura 5-1**).

Prerrequisitos

Obtenga más información sobre los permisos (consulte **Tabla 5-1**) compatible con API Gateway y elija políticas o roles según sus requisitos. Para obtener los permisos de otros servicios, consulte **Permisos de sistema**.

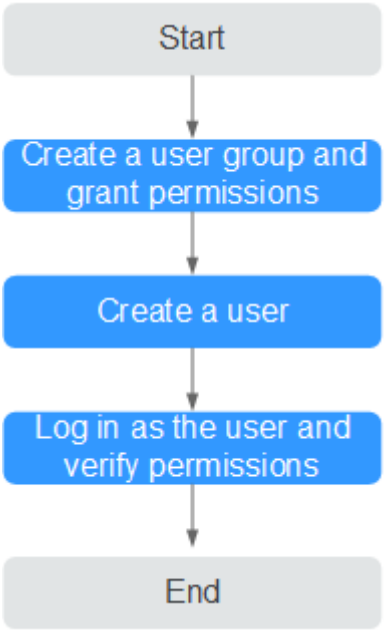
Tabla 5-1 Funciones y políticas definidas por el sistema compatibles con APIG

Nombre de rol/ política	Descripción	Tipo	Dependencia
APIG Administrator	Permisos de administrador para APIG. Los usuarios con estos permisos pueden utilizar todas las funciones de las puertas de enlace **compartida** y **dedicadas**.	System-defined role	None

Nombre de rol/ política	Descripción	Tipo	Dependencia
APIG FullAccess	Permisos completos para APIG. Los usuarios con estos permisos pueden utilizar todas las funciones de las puertas de enlace **dedicated**.	System-defined policy	None
APIG ReadOnlyAccess	Permisos de sólo lectura para APIG. Los usuarios a los que se han concedido estos permisos solo pueden ver puertas de enlace **dedicadas**.	System-defined policy	None

Flujo del proceso

Figura 5-1 Proceso para conceder permisos de API Gateway



1. **Crear un grupo de usuarios y asignar permisos**.

   Cree un grupo de usuarios en la consola de IAM y adjunte el rol **APIG Administrator** o la política **APIG FullAccess** al grupo.

2. **Crear un ususario de IAM**.

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.

3. **Iniciar la sesión** y verificar los permisos.

   Inicie sesión en la consola API Gateway como usuario creado y compruebe que el usuario tiene permisos de administrador para API Gateway.

5.2 Políticas personalizadas de API Gateway

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de API Gateway. Para ver las acciones que se pueden agregar a las directivas personalizadas, consulte **Políticas de permisos y acciones admitidas**.

Puede crear políticas personalizadas mediante uno de los métodos siguientes:

- Editor visual: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Editar las políticas JSON desde cero o basándose en una política existente.

Para obtener más información, consulte **Creación de una política personalizada**. La siguiente sección contiene ejemplos de políticas personalizadas comunes de API Gateway.

NOTA

Solo las puertas de enlace de API dedicadas admiten políticas definidas por el sistema y políticas personalizadas.

Ejemplo de políticas personalizadas

- Ejemplo 1: Permitir a los usuarios crear y depurar APIs

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                     apig:apis:create
                     apig:apis:debug
                 "
            ]
        }
    ]
}
```

- Ejemplo 2: Denegar la creación de un grupo API

  Una política con solo permisos "Deny" debe usarse junto con otras políticas para que surtan efecto. Si los permisos asignados a un usuario contienen tanto "Allow" y "Deny", los permisos "Deny" tienen prioridad sobre los permisos "Allow".

  El siguiente método se puede utilizar si necesita asignar permisos de la política **APIG FullAccess** a un usuario, pero desea evitar que el usuario cree grupos de API. Cree una política personalizada para denegar la creación de grupos de API y adjunte ambas políticas al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones en las puertas de enlace de API, excepto crear grupos de API. A continuación se muestra un ejemplo de una política de denegación:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [
                                "apig:groups:create"
                        ]
                }
```



```
            ]
}
```


6 Operaciones clave registradas por CTS

6.1 Operaciones de API Gateway que pueden ser registradas por CTS

Habilitación de CTS

Si desea recopilar, registrar o consultar registros de operaciones para API Gateway en escenarios comunes como análisis de seguridad, auditoría y localización de problemas, **habilitar Cloud Trace Service (CTS)**.

CTS proporciona las siguientes funciones:

- Registro de logs de auditoría
- Consulta de logs de auditoría
- Volcar logs de auditoría
- Encriptación de archivos de seguimiento
- Habilitación de notificaciones de operaciones clave

Consulta de operaciones clave

Con CTS, puede registrar las operaciones asociadas con API Gateway para futuras consultas, auditorías y seguimiento.

Tabla 6-1 Operaciones de API Gateway que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Creación de un grupo de API	ApiGroup	createApiGroup
Eliminación de un grupo de API	ApiGroup	deleteApiGroup
Actualización de un grupo de API	ApiGroup	updateApiGroup

Operación	Tipo de recurso	Nombre del rastro
Vinculación de un nombre de dominio	ApiGroup	createDomainBinding
Cambio de la versión mínima de TLS	ApiGroup	modifySecureTransmission
Desvinculación de un nombre de dominio	ApiGroup	relieveDomainBinding
Adición de un certificado de dominio	ApiGroup	addDomainCertificate
Eliminación de un certificado de dominio	ApiGroup	deleteDomainCertificate
Creación de una API	Api	createApi
Eliminación de una API	Api	deleteApi
Eliminación de varias APIs	Api	batchDeleteApi
Actualización de una API	Api	updateApi
Publicación de una API	Api	publishApi
Desconexión de una API	Api	offlineApi
Publicación de varias API o desconexión de una API	Api	batchPublishOrOfflineApi
Cambio de versiones de API	Api	switchApiVersion
Desconexión de una versión de API	Api	offlineApiByVersion
Depuración de una API	Api	debugApi
Creación de un entorno	Environment	createEnvironment
Eliminación de un entorno	Environment	deleteEnvironment
Actualización de un entorno	Environment	updateEnvironment
Creación de una variable de entorno	EnvVariable	createEnvVariable
Actualización de una variable de entorno	EnvVariable	updateEnvVariable
Eliminación de una variable de entorno	EnvVariable	deleteEnvVariable
Creación de una aplicación	App	createApp
Eliminación de una App	App	deleteApp

Operación	Tipo de recurso	Nombre del rastro
Actualización de una aplicación	App	updateApp
Restablecimiento de AppSecret	App	resetAppSecret
Vinculación de un cliente a una API	AppAuth	grantAuth
Desvinculación de un cliente de una API	AppAuth	relieveAuth
Creación de una clave de firma	Signature	createSignature
Eliminación de una clave de firma	Signature	deleteSignature
Actualización de una clave de firma	Signature	updateSignature
Vinculación de una clave de firma	SignatureBinding	createSignatureBinding
Desvinculación de una clave de firma	SignatureBinding	relieveSignatureBinding
Creación de una política de control de acceso	Acl	createAcl
Eliminación de una política de control de acceso	Acl	deleteAcl
Eliminación de políticas de control de acceso	Acl	batchDeleteAcl
Actualización de una política de control de acceso	Acl	updateAcl
Creación de una lista de bloqueo de control de acceso	Acl	addAclValue
Eliminación de una lista de bloqueo de control de acceso	Acl	deleteAclValue
Vinculación de una política de control de acceso a una API	AclBinding	createAclBinding
Desvinculación de una política de control de acceso de una API	AclBinding	relieveAclBinding

Operación	Tipo de recurso	Nombre del rastro
Desvinculación de varias políticas de control de acceso de las API	AclBinding	batchRelieveAclBinding
Creación de una política de limitación de solicitudes	Throttle	createThrottle
Eliminación de una política de limitación de solicitudes	Throttle	deleteThrottle
Eliminación de varias directivas de limitación de solicitudes	Throttle	batchDeleteThrottle
Actualización de una política de limitación que solicita	Throttle	updateThrottle
Vinculación de una política de limitación de solicitudes	ThrottleBinding	createThrottleBinding
Desvinculación de una política de limitación de solicitudes	ThrottleBinding	relieveThrottleBinding
Desvinculación de varias políticas de limitación de solicitudes	ThrottleBinding	batchRelieveThrottleBinding
Creación de una configuración de limitación de solicitudes excluidas	ThrottleSpecial	createSpecialThrottle
Eliminación de una configuración de limitación de solicitudes excluidas	ThrottleSpecial	deleteSpecialThrottle
Actualización de una configuración de limitación de solicitudes excluidas	ThrottleSpecial	updateSpecialThrottle
Creación de un canal de balance de carga	Vpc	createVpc
Supresión de un canal de equilibrio de carga	Vpc	deleteVpc
Actualización de un canal de balance de carga	Vpc	updateVpc
Adición de miembros a un canal de balance de carga	Vpc	addVpcMember

Operación	Tipo de recurso	Nombre del rastro
Eliminación de miembros de un canal de balanceo de carga	Vpc	deleteVpcMember
Exportación de una API	Swagger	swaggerExportApi
Exportación de varias APIs	Swagger	swaggerExportApiList
Exportación de todas las API de un grupo	Swagger	swaggerExportApiByGroup
Importación de APIs a un nuevo grupo	Swagger	swaggerImportApiTo-NewGroup
Importación de API a un grupo existente	Swagger	swaggerImportApiToEx-istGroup
Exportación de todos los backends personalizados	Swagger	SwaggerExportLdApi
Importación de backends personalizados	Swagger	SwaggerImportLdApi
Creación de un autorizador personalizado	Authorizer	createAuthorizer
Eliminación de un autorizador personalizado	Authorizer	deleteAuthorizer
Actualización de un autorizador personalizado	Authorizer	updateAuthorizer
Creación de un plug-in	Plugin	createPlugin
Actualización de un plug-in	Plugin	updatePlugin
Eliminación de un plug-in	Plugin	deletePlugin
Vinculación de un plug-in a una API	Plugin	pluginAttachApi
Desvinculación de una API de un plug-in	Plugin	pluginDetachApi
Binding a plug-in to an API	Plugin	apiAttachPlugin
Desvinculación de un plug-in de una API	Plugin	apiDetachPlugin

Deshabilitación de CTS

Deshabilite CTS siguiendo el procedimiento de **Eliminación de un rastreador**.

6.2 Consulta de logs de auditoría

Consulte logs de auditoría siguiendo el procedimiento en **Consulta de seguimientos en tiempo real**.

Figura 6-1 Visualización de logs