API Gateway

# Descripción general del servicio

| | |
|---|---|
| **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.

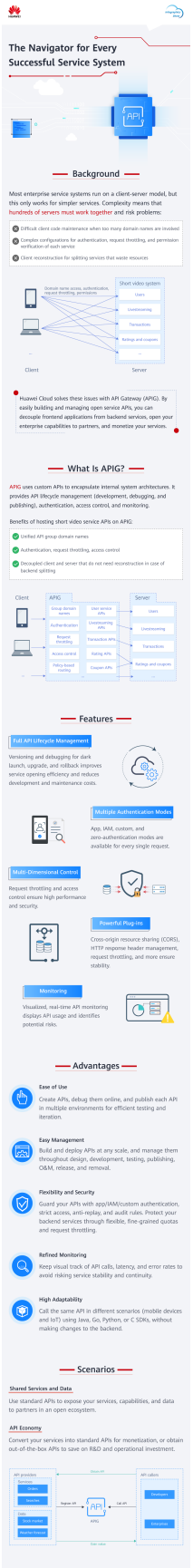
# Índice



# 1 Infografía de APIG



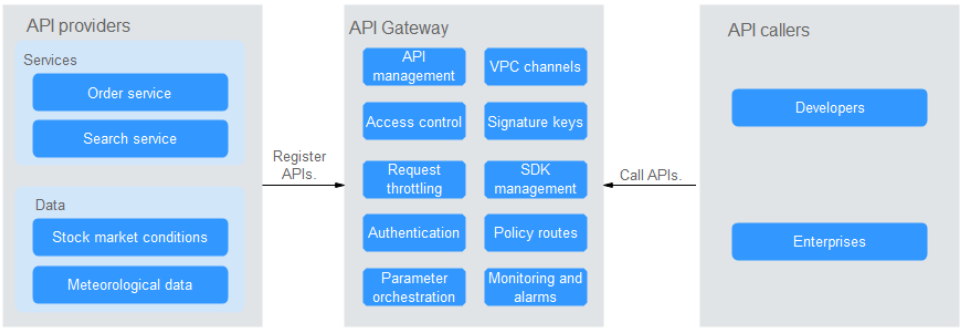

  

# 2 ¿Qué es API Gateway?

API Gateway es un servicio de alojamiento de API de alto rendimiento, alta disponibilidad y alta seguridad que le ayuda a crear, gestionar e implementar interfaces de programación de aplicaciones (API) a cualquier escala. . Con solo unos pocos clics, puede integrar sistemas internos, monetizar las capacidades del servicio, y exponer selectivamente las capacidades con costos y riesgos mínimos. API Gateway le ayuda a monetizar las capacidades del servicio y reducir la inversión en I+D, y le permite centrarse en los servicios empresariales principales para mejorar la eficiencia operativa.

- Para monetizar sus capacidades de servicio y datos, puede abrirlas creando APIs en API Gateway. A continuación, puede proporcionar las API para los que llaman a la API mediante canales sin conexión.
- También puede obtener API abiertas de API Gateway para reducir el tiempo y los costos de desarrollo.

**Figura 2-1** Arquitectura de API Gateway




## Funciones del producto

- **Gestión del ciclo de vida de la API**

  El ciclo de vida de una API implica crear, publicar, quitar y eliminar la API. La gestión del ciclo de vida de la API le permite exponer las capacidades de servicio de forma rápida y eficiente.

- **Herramienta de depuración integrada**

  Con la herramienta de depuración integrada, puede depurar APIs utilizando diferentes encabezados HTTP y cuerpos de solicitud. Esta herramienta simplifica el proceso de desarrollo de API y reduce los costos de desarrollo y mantenimiento de API.

- **Gestión de versiones**

  Una API se puede publicar en diferentes entornos. Publicar una API nuevamente en el mismo entorno anulará la versión anterior de la API. API Gateway muestra el historial de publicaciones (incluida la versión, la descripción, la fecha y la hora y el entorno) de cada API. Puede revertir una API a cualquier versión histórica para cumplir con los requisitos de lanzamiento oscuro y actualización de versión.

- **Variables de entorno**

  Las variables de entorno son manejables y específicas para entornos. Las variables de una API serán reemplazadas por los valores de las variables en el entorno donde se publicará la API. Puede crear variables en diferentes entornos para llamar a diferentes servicios de backend utilizando la misma API.

- **limitación de solicitudes**
  - Para diferentes servicios y usuarios, puede controlar la frecuencia de solicitud a la que un usuario, una aplicación y una dirección IP pueden llamar a una API. Esto garantiza que los servicios de backend puedan ejecutarse de manera estable.
  - El estrangulamiento puede ser preciso al segundo, minuto, hora o día.
  - Las apps y los inquilinos excluidos se pueden configurar para limitar el número de llamadas a la API de apps e inquilinos específicos, respectivamente.

- **Monitoreo y alarma**

  API Gateway proporciona monitorización de API en tiempo real y muestra varias métricas, incluyendo el número de solicitudes, latencia de invocación y el número de errores. Las métricas le ayudan a comprender el uso de la API, lo que te permite identificar posibles riesgos de servicio.

- **Control de acceso**

  Las políticas de control de acceso son una de las medidas de seguridad proporcionadas por API Gateway. Permiten o niegan el acceso a la API desde direcciones IP o cuentas específicas.

- **Canales de VPC**

  Los canales de VPC se pueden crear para acceder a recursos en Virtual Private Clouds (VPCs) y exponer las capacidades de los servicios de backend implementados en las VPC. Un canal de VPC reenvía las solicitudes de API a diferentes servidores para equilibrar la carga.

- **Claves de firma**

  Una clave de firma consiste en una clave y un secreto, y solo tiene efecto después de estar vinculada a las API. Los servicios de backend utilizan las claves de firma para verificar la identidad de API Gateway y garantizar un acceso seguro.

# 3 Ventajas del producto

## Listo para usar

Puede crear API rápidamente configurando la configuración requerida en la consola API Gateway. API Gateway proporciona una herramienta de depuración en línea para simplificar el desarrollo de API y le permite publicar una API en múltiples entornos para realizar pruebas sencillas e iteraciones rápidas.

## Gestión conveniente del ciclo de vida de la API

API Gateway proporciona una gestión de API de ciclo de vida completo, que incluye diseño, desarrollo, prueba, publicación y O&M, para ayudarlo a crear, gestionar e implementar API rápidamente a cualquier escala.

## Limitación de Solicitudes Refinadas

API Gateway combina el control de tráfico síncrono y asíncrono y múltiples algoritmos para limitar las solicitudes en el segundo nivel. Puede definir de manera flexible las políticas de limitación de solicitudes para garantizar la estabilidad y la continuidad de los servicios API.

## Invocación de función

API Gateway funciona sin problemas con **FunctionGraph** lo que le permite exponer selectivamente funciones de FunctionGraph en forma de API.

## Monitoreo de API visualizado

API Gateway supervisa el número de llamadas a la API, la latencia de datos y el número de errores, lo que le ayuda a identificar los riesgos potenciales del servicio.

## Protección de seguridad integral

API Gateway proporciona múltiples medidas para proteger las llamadas a la API, como transferencia de Secure Sockets Layer (SSL), control de acceso estricto, lista negra/lista blanca de direcciones IP, autenticación, anti-reproducción, anti-ataque y reglas de auditoría múltiples. Además, API Gateway implementa una gestión flexible y refinada de cuotas y limitación de solicitudes para ayudarle a abrir sus servicios de backend de manera flexible y segura.

## Rutas de políticas flexibles

Puede configurar backends para que una API reenvíe solicitudes de acuerdo con varias políticas. Esto facilita el lanzamiento oscuro y la gestión del entorno.

## SDK de diferentes lenguajes de programación

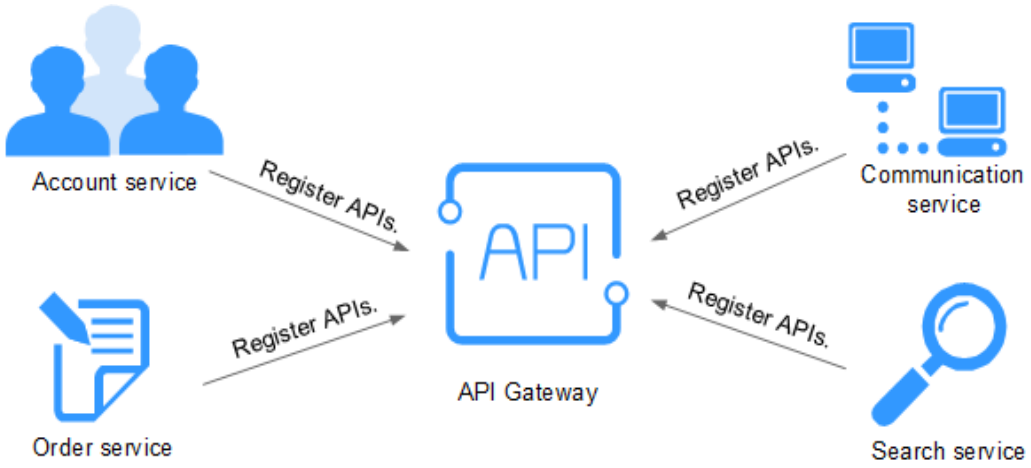
Los SDK de diferentes lenguajes de programación (como Java, Go, Python y C) están disponibles para el acceso desde los clientes. Debido a que los backends no necesitan ser modificados, solo se requiere un sistema para adaptarse a diferentes escenarios de servicio (como dispositivos móviles e IoT).

# 4 Escenarios de aplicación

## Desacoplamiento del sistema interno

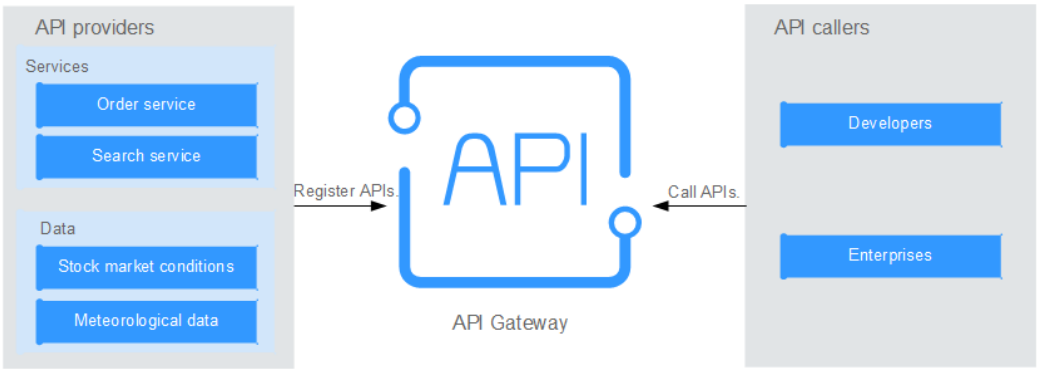
A medida que las empresas se desarrollan rápidamente con cambios de negocio rápidos, los sistemas internos de las empresas deben mantenerse al ritmo del desarrollo. Sin embargo, es difícil asegurar la universalidad y estabilidad del sistema porque los sistemas internos dependen unos de otros. APIG utiliza RESTful APIs estándar para simplificar la arquitectura del servicio, desacopla los sistemas internos y separa el frontend del backend. Las capacidades existentes se pueden reutilizar para evitar el desarrollo repetitivo.




## Apertura de capacidades empresariales

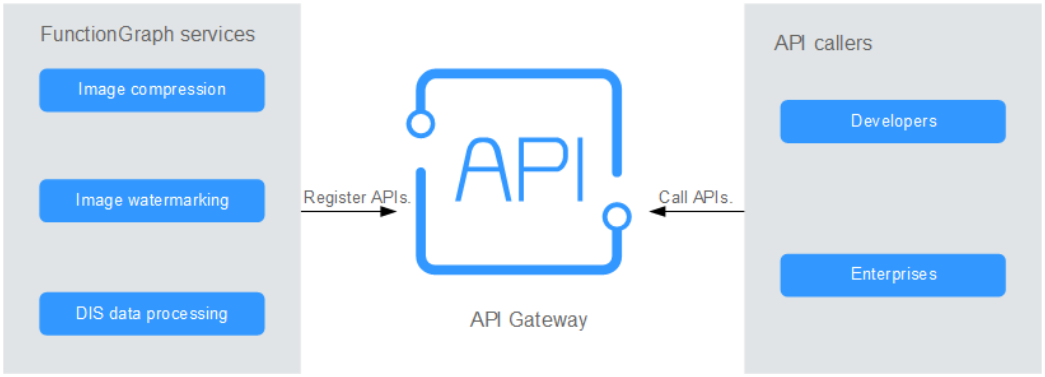
Una empresa no puede desarrollarse sin las capacidades de los socios, como una plataforma de pago de terceros y el inicio de sesión en la cuenta de socios. APIG le permite exponer selectivamente las capacidades a los socios mediante el uso de API estándar y compartir servicios y datos con los socios para crear un nuevo ecosistema.




## Apertura de servicios de FunctionGraph

APIG también puede ayudarle a exponer selectivamente los servicios sin servidor (servicios de FunctionGraph) a los socios. Los servicios de FunctionGraph son más fáciles de desarrollar, implementar y mantener que los servicios tradicionales. Puede usar FunctionGraph para crear rápidamente lógica de servicio de backend y usar APIG para exponer funciones de lógica de servicio para la expansión de simultaneidad lineal.



# 5 Especificaciones

## Especificaciones de la puerta de enlace compartida

La puerta de enlace compartida no proporciona ninguna configuración de especificación. Ver las cuotas para crear y usar APIs en **Notas y restricciones**.

NOTA

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

## Especificaciones de la puerta de enlace dedicada

**Tabla 5-1** enumera las especificaciones de las puertas de enlace de API dedicadas.

**Tabla 5-1** Especificaciones de puertas de enlace dedicadas

| Edición | Número máximo de solicitudes por segundo |
|---|---|
| Basic | 2000 |
| Professional | 4000 |
| Enterprise | 6000 |
| Platinum | 10,000 |

NOTA

- Las cuotas **default** relacionadas con la API de las puertas de enlace dedicadas son las mismas que las de la puerta de enlace compartida.
- Para las puertas de enlace dedicadas, puede ajustar el número máximo de solicitudes por segundo para cada API.
- Las especificaciones de la puerta de enlace dedicada se obtienen mediante pruebas en las siguientes condiciones:
  - Protocolo: HTTPS
  - Tipo de conexión: long connection
  - Solicitudes simultáneas: 100
  - Modo de autenticación: ninguno
  - Tamaño de los datos devueltos: 1 KB
  - Ancho de banda: 10 MB/s

## Diferencias entre puertas de enlace dedicadas y compartidas

APIG proporciona una puerta de enlace compartida y puertas de enlace dedicadas. Puede usar la puerta de enlace compartida de inmediato o comprar puertas de enlace dedicadas para gestionar las API.

Las puertas de enlace dedicadas facilitan el desacoplamiento de los sistemas internos dentro de una empresa. Los servicios implementados en las VPC se comunican entre sí a través de RESTful APIs con alta seguridad de red. Las puertas de enlace dedicadas admiten el despliegue de servicios front-end o back-end en redes públicas, y se puede acceder a estos servicios mediante IP elásticas (EIP).

**Tabla 5-2** Diferencias básicas entre las puertas de enlace de API compartidas y dedicadas

| Elemento | Puerta de enlace compartida | Puerta de enlace dedicada |
| --- | --- | --- |
| Facturación | Basado en llamadas API. | Basado en las especificaciones de la puerta de enlace y la duración del uso. |
| Acceso a la red | Se accede a las API a través de redes públicas. | Las puertas de enlace se ejecutan en las VPC. Las API en una VPC se llaman usando la dirección de subred de la VPC.<br>Puede habilitar el acceso a recursos de API en una puerta de enlace a través de redes públicas o el acceso a recursos en redes públicas a través de API en una puerta de enlace. |
| Usuarios objetivo | Las pequeñas empresas que tienen bajos requisitos de aislamiento físico y desean exponer selectivamente las capacidades de API. | Empresas grandes y medianas que desean exponer y llamar selectivamente a las API internas. Las puertas de enlace dedicadas se implementan en clústeres aislados físicamente con diferentes anchos de banda para el acceso entrante y saliente. |

La siguiente tabla muestra las **diferencias funcionales** entre las puertas de enlace de API compartidas y dedicadas.

**Tabla 5-3** Diferencias funcionales entre las puertas de enlace de API compartidas y dedicadas

| Categoría | Características | Puerta de enlace compartida | Puerta de enlace dedicada |
|---|---|---|---|
| Funciones básicas | Limitación de solicitud refinada | √ | √ |
| | Control de acceso por dirección IP y cuenta | √ | √ |
| | Autenticación de la Seguridad | √ | √ |
| | Gestión del ciclo de vida de la API. | √ | √ |
| | Nombres de dominio personalizados | √ | √ |
| | Importación y exportación de Swagger API | √ | √ |
| | Canales de VPC | √ | √ |
| | Orquestación de parámetros de API | √ | √ |
| | Gestión de variables de grupo API | √ | √ |
| Funciones avanzadas | Autenticación personalizada | √ | √ |
| | Enrutamiento basado en políticas | √ | √ |
| | Monitoreo de API | √ | √ |
| | **Equilibrio de carga de backend** | × | √ |
| | **Gestión interna de API** | × | √ |
| | **Acceso a servicios de backend en nubes privadas** | × | √ |
| | **Acceso al servicio a través de Direct Connect** | × | √ |
| | Plug-ins | × | √ |

| Categoría | Características | Puerta de enlace compartida | Puerta de enlace dedicada |
| --- | --- | --- | --- |
| | Análisis de log | × | √ |
| Indicadores de rendimiento | **Clústeres aislados físicamente** | × | √ |
| | **Diferentes anchos de banda para el acceso entrante y saliente** | × | √ |
| | **TPS** | 200 | 4000 – 10,000 |

# 6 Notas y restricciones

Para cambiar las restricciones predeterminadas, **aumente la cuota**. Para obtener más información sobre la configuración de parámetros de una puerta de enlace dedicada, consulte **Modificación de parámetros de configuración**.

**Tabla 6-1** Cuotas de API gateway compartida

| Elemento | Restricción predeterminada | Modificable |
| --- | --- | --- |
| Grupos de API | 50 | √ |
| APIs | 200 | √ |
| Políticas de backend | 5 | √ |
| Apps | 50. La cuota de aplicaciones incluye aplicaciones creadas y aplicaciones generadas cuando se compran API en KooGallery. | √ |
| Políticas de limitación de solicitudes | ● Puede crear un máximo de 30 políticas de limitación de solicitudes.<br>● El límite de llamadas para un solo usuario no puede exceder el de la API de destino.<br>● El límite de llamadas para una sola aplicación no puede exceder el de un solo usuario.<br>● El límite de llamadas para una sola dirección IP no puede exceder el de la API de destino. | √ |
| Entornos | 10 | √ |
| Claves de firma | 30 | √ |
| Políticas de control de acceso | 100 | √ |
| Canales de VPC | 30 | √ |

| Elemento | Restricción predeterminada | Modificable |
| --- | --- | --- |
| Variables | Puede crear un máximo de 50 variables para un grupo de API en cada entorno. | √ |
| Nombres de dominio independientes | Un máximo de cinco nombres de dominio independientes pueden estar enlazados a un grupo de API. | √ |
| Servidores en la nube | Se puede agregar un máximo de 200 servidores en la nube a un canal de VPC. | √ |
| Parámetros | Se puede crear un máximo de 50 parámetros para una API. | √ |
| Registros de publicación de API | Se puede conservar un máximo de 10 registros de publicación de una API para cada entorno. | √ |
| Tasa de acceso a la API | Hasta 200 veces por segundo | √ |
| Aplicaciones excluidas | Se puede agregar un máximo de 30 aplicaciones excluidas a una política de limitación de solicitudes. | √ |
| Inquilinos excluidos | Se puede agregar un máximo de 30 inquilinos excluidos a una política de limitación de solicitudes. | √ |
| Acceso a un nombre de subdominio | Se puede acceder a un nombre de subdominio hasta 1000 veces al día. | x |
| Tamaño máximo de un paquete de solicitud de API | 12 MB | x |
| Protocolo TLS | Se admiten TLS 1.1 y TLS 1.2. Se recomienda TLS 1.2. | x |
| Autorizadores personalizados | 20 | √ |

**Tabla 6-2** Cuotas de API gateway dedicadas

| Elemento | Restricción predeterminada | Modificable |
| --- | --- | --- |
| Gateways | 5 | √ |
| Grupos de API | 1500 | √ |

| Elemento | Restricción predeterminada | Modificable |
| --- | --- | --- |
| APIs | Número de API para cada edición de gateway:<br>● Básico: 250<br>● Profesional: 800<br>● Empresa: 2000<br>● Platino: 8000 | √ |
| Políticas de backend | 5 | √ |
| Apps | 50. La cuota de aplicaciones incluye las aplicaciones que ha creado. | √ |
| Políticas de limitación de solicitudes | ● Puede crear un máximo de 300 políticas de limitación de solicitudes para cada puerta de enlace.<br>● El límite de llamadas para un solo usuario no puede exceder el de la API de destino.<br>● El límite de llamadas para una sola aplicación no puede exceder el de un solo usuario.<br>● El límite de llamadas para una sola dirección IP no puede exceder el de la API de destino. | √ |
| Entornos | 10 | √ |
| Claves de firma | 200 | √ |
| Políticas de control de acceso | 100 | √ |
| Canales de VPC | 200 | √ |
| Variables | Puede crear un máximo de 50 variables para un grupo de API en cada entorno. | √ |
| Nombres de dominio independientes | Un máximo de cinco nombres de dominio independientes pueden estar enlazados a un grupo de API. | √ |
| Servidores en la nube | Se puede agregar un máximo de 10 servidores en la nube a un canal de VPC. | √ |
| Parámetros | Se puede crear un máximo de 50 parámetros para una API. | √ |
| Registros de publicación de API | Se puede conservar un máximo de 10 registros de publicación de una API para cada entorno. | √ |

| Elemento | Restricción predeterminada | Modificable |
| --- | --- | --- |
| Tasa de acceso a la API | Hasta 6000 veces por segundo | √ |
| Aplicaciones excluidas | Se puede agregar un máximo de 30 aplicaciones excluidas a una política de limitación de solicitudes. | √ |
| Inquilinos excluidos | Se puede agregar un máximo de 30 inquilinos excluidos a una política de limitación de solicitudes. | √ |
| Acceso a un nombre de subdominio | Se puede acceder a un nombre de subdominio hasta 1000 veces al día. | x |
| Tamaño máximo de un paquete de solicitud de API | 12 MB | √ |
| Protocolo TLS | Se admiten TLS 1.1 y TLS 1.2. Se recomienda TLS 1.2. | √ |
| Autorizadores personalizados | 50 | x |
| Plug-ins | 500 | √ |

# 7 Gestión de permisos

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de APIG, Identity and Access Management (IAM) es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud .

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM para sus empleados y asignar permisos a los empleados para controlar su acceso a recursos específicos.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM para la gestión de permisos, omita este capítulo.

IAM es gratuito. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **Descripción general de IAM**.

## Permisos APIG

De forma predeterminada, los nuevos usuarios de IAM no tienen ningún permiso asignado. Debe agregar un usuario a uno o más grupos y adjuntar directivas o roles a estos grupos. A continuación, el usuario hereda los permisos de los grupos a los que pertenece el usuario y puede realizar operaciones específicas en servicios en la nube basadas en los permisos.

APIG es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos APIG a un grupo de usuarios, debe especificar proyectos específicos de región (por ejemplo, **ap-southeast-1** for **CN-Hong Kong**) para los que los permisos tendrán efecto. Si selecciona **All projects**, los permisos se otorgarán tanto para el proyecto de servicio global como para todos los proyectos específicos de la región. Al acceder a APIG, los usuarios deben cambiar a una región en la que han sido autorizados para usar este servicio.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Este mecanismo proporciona solo un número limitado de roles de nivel de servicio para la autorización. Al usar roles para conceder permisos, también debe asignar otros roles dependientes para que los permisos surtan efecto. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas

condiciones. Este mecanismo permite una autorización basada en políticas más flexible y cumple con los requisitos de control de acceso seguro. Por ejemplo, puede conceder a los usuarios de APIG solo los permisos para realizar operaciones específicas. La mayoría de las políticas definen permisos basados en API. Para ver las acciones de API admitidas por APIG, consulte **Políticas de permisos y acciones admitidas**.

**Tabla 7-1** enumera todas las funciones y políticas definidas por el sistema compatibles con APIG.

**Tabla 7-1** 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 |
| 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 |

Puede ver el contenido de las funciones y políticas anteriores en la consola de IAM. Por ejemplo, el contenido de la política de **APIG FullAccess** es el siguiente:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "apig:*:*",
                "vpc:*:get*",
                "vpc:*:list*",
                "vpc:ports:create",
                "vpc:ports:update",
                "vpc:ports:delete",
                "vpc:publicIps:update",
                "FunctionGraph:function:listVersion",
                "FunctionGraph:function:list",
                "FunctionGraph:function:getConfig",
                "ecs:servers:list",
                "lts:groups:list",
                "lts:logs:list",
                "lts:topics:list"
            ],
            "Effect": "Allow"
```

```
            }
        ]
}
```

## Enlaces útiles

- **Descripción general del servicio IAM**
- **Creación de un usuario y concesión de permisos de API Gateway**

# 8 Conceptos Básicos

## API

Un conjunto de funciones predefinidas que encapsulan las capacidades de la aplicación. Puede crear APIs y hacerlas accesibles para los usuarios.

Al crear una API, debe configurar la información básica y las rutas, parámetros y protocolos de solicitud de frontend y backend.

## Grupo de API

Una colección de APIs usadas para el mismo servicio. Los grupos de API facilitan la gestión de API.

## Entorno

Una etapa en el ciclo de vida de una API. Un entorno, como el entorno de pruebas o desarrollo de API, especifica el alcance de uso de las API, lo que facilita la gestión del ciclo de vida de las API. La misma API se puede publicar en diferentes entornos.

Para llamar a una API en diferentes entornos, necesitas agregar el parámetro de encabezado **x-stage** a la solicitud enviada para llamar a la API. El valor de este parámetro es un nombre de entorno.

## Variable de entorno

Una variable que es manejable y especial para un entorno. Puede crear variables en diferentes entornos para llamar a diferentes servicios de backend utilizando la misma API.

## Limitación de solicitudes

Controla el número de veces que un usuario, una aplicación o una dirección IP pueden llamar a las API durante un período específico para proteger los servicios de backend.

Limitación de solicitud puede ser preciso al minuto y al segundo.

## Control de acceso

Las políticas de control de acceso son una de las medidas de seguridad proporcionadas por API Gateway. Permiten o niegan el acceso a la API desde direcciones IP o cuentas específicas.

## App

Una entidad que solicita APIs. Una app puede estar autorizada para acceder a varias API, y varias apps pueden estar autorizadas para acceder a la misma API.

## Clave de firma

Consiste en una clave y un secreto, que son utilizados por los servicios de backend para verificar la identidad de API Gateway y garantizar un acceso seguro.

Cuando se llama a una API vinculada con una clave de firma, API Gateway agrega información de firma a las solicitudes de API. El servicio backend de la API firma las solicitudes 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.

## Canal de VPC

Método para acceder a los recursos de VPC desde API Gateway, que le permite exponer selectivamente los servicios de backend implementados en las VPC a usuarios de terceros.

## Autenticación personalizada

Un mecanismo definido con reglas personalizadas para API Gateway para verificar la validez e integridad de las solicitudes iniciadas por los llamantes de API. El mecanismo también se utiliza para que los servicios de backend verifiquen las solicitudes reenviadas por API Gateway.

Se proporcionan los siguientes dos tipos de autenticación personalizada:

- Autenticación personalizada Frontend: Un autorizador personalizado está configurado con una función para autenticar las solicitudes de una API.
- Autenticación personalizada de backend: Se puede configurar 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.

## Autenticación sencilla

La autenticación simple facilita la respuesta rápida a las solicitudes de API agregando el parámetro **X-Apig-AppCode** (cuyo valor es un AppCode) al encabezado de solicitud HTTP. API Gateway verifica solo el AppCode y no verifica la firma de la solicitud.

## Respuesta de Gateway

Las respuestas de puerta de enlace se devuelven si API Gateway no procesa las solicitudes de API. API Gateway proporciona respuestas predeterminadas para múltiples escenarios y le

permite personalizar los códigos de estado de respuesta y el contenido. Puede agregar una respuesta de puerta de enlace en formato JSON en la página **API Groups**.

# 9 Facturación

Para la puerta de enlace compartida, se le facturará en función del número de llamadas a la API y la cantidad de datos transferidos. Para las puertas de enlace dedicadas, se le facturará en función de la edición de la puerta de enlace y la duración del uso del ancho de banda de acceso saliente.

Para obtener más información sobre los precios de APIG y calcular los precios para usar este servicio, vaya a la página **Detalles de precio de producto**.

## Puerta de enlace compartida

La puerta de enlace compartida se factura en función de **número de llamadas API que ha recibido** and the **cantidad de datos transferidos**. Las reglas de facturación difieren entre estas dos categorías. Cuando se llama a una API, **se facturará** tanto el número de llamadas como el tráfico generado.

**Facturación para llamadas API**

- Artículo de facturación: número de llamadas API que ha recibido
- Modo de facturación: pago por uso
- Ciclo de facturación: día
- Tiempo de facturación: Las facturas generalmente se emiten dentro de 1 a 3 horas después de que finalice el ciclo de facturación actual.

**Facturación por transferencia de datos**

- Elemento de facturación: cantidad de datos transferidos
- Precio: tarifa estándar para la transferencia de datos
- Modo de facturación: pago por uso
- Unidad: GB
- Ciclo de facturación: día
- Si utiliza APIG junto con servicios de backend que se encuentran en diferentes regiones u ofrecidos por otros proveedores de servicios en la nube, se pueden incurrir en cargos adicionales por la transferencia de datos de APIG a los servicios de backend.

## Puerta de enlace dedicada

Las puertas de enlace dedicadas se facturan en función de la **edición de gateway** y **ancho de banda**.

**Facturación para la edición Gateway**

Las puertas de enlace dedicadas están disponibles en cuatro ediciones: básica, profesional, empresarial y platino. Debe pagar los precios correspondientes al comprar estas ediciones.

APIG ofrece dos modos de facturación: pago por uso y anual/mensual. Se recomienda el modo de pago por uso si no puede predecir con precisión sus necesidades futuras de servicio y desea evitar pagar por los recursos no utilizados. Sin embargo, si puede predecir con precisión sus necesidades futuras de servicio, el modo anual/mensual es más rentable.

- Anual/Mensual: Proporciona un descuento mayor que el modo de pago por uso y se recomienda para usuarios a largo plazo.
- Pago por uso (por hora): puede iniciar y detener puertas de enlace dedicadas según sea necesario. Se le facturará en función de la duración durante la que utilice las puertas de enlace. La facturación comienza cuando se compra una puerta de enlace dedicada y finaliza cuando la puerta de enlace se detiene debido a atrasos o se elimina. La unidad de tiempo mínima es de un segundo.
- Cambio del modo de facturación: puede cambiar el modo de facturación de las puertas de enlace dedicadas de anual/mensual a pago por uso o de pago por uso a anual/mensual.

**Facturación por ancho de banda**

Si el servicio de backend de API se implementa en la red pública, se le cobrará el ancho de banda por reenviar las solicitudes de API a la red pública. Los precios se calculan en función del **ancho de banda** y la **duration** durante la que se utiliza la puerta de enlace.

NOTA

- Si su servicio de backend se implementa en la misma VPC que su puerta de enlace dedicada, se puede acceder al servicio de backend mediante una dirección IP privada y no es necesario adquirir ancho de banda para la puerta de enlace.
- Si su puerta de enlace dedicada contiene API que se llamarán desde redes públicas, debe comprar un EIP y vincularlo a la puerta de enlace.
- Si las API de su puerta de enlace dedicada se llamarán dentro de la VPC, no necesita comprar o vincular un EIP a la puerta de enlace.

## Vencimiento y pago atrasado

Si su cuenta está en mora, puede ver los detalles de los atrasos en el Centro de facturación. Para evitar que los recursos relacionados se detengan o se liberen, recargue su cuenta lo antes posible. Para obtener más información, consulte **Recarga y pago**.

## Cancelación de suscripción

Para dejar de usar puertas de enlace dedicadas anuales/mensuales, anule su suscripción en la página **Cloud Service Unsubscriptions** del Centro de facturación o en la lista de puertas de enlace de la consola APIG.