API Gateway

Visão geral de serviço

Edição 01

Data 2024-04-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Cloud Computing Technologies Co., Ltd.

Marcas registadas e permissões

e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

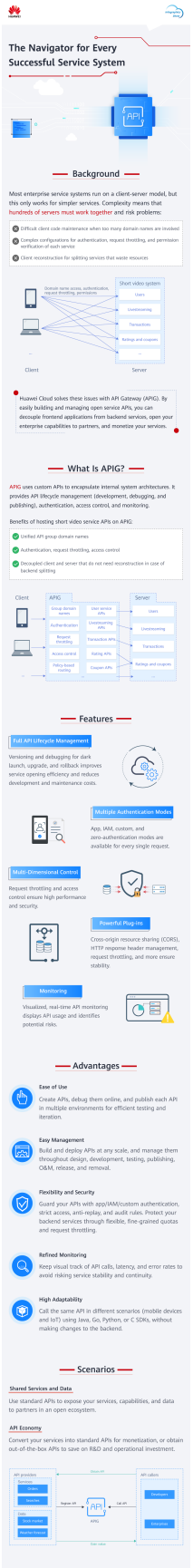
Índice

1 Infográficos do APIG....1
2 O que é o API Gateway?....3
3 Vantagens do produto....5
4 Cenários de aplicação....7
5 Especificações....9
6 Segurança....13
6.1 Responsabilidades compartilhadas....13
6.2 Identificação e gerenciamento de ativos....14
6.3 Autenticação de identidade e controle de acesso....14
6.4 Proteção de dados....14
6.5 Auditoria e logs....15
6.6 Monitoramento de riscos de segurança....16
6.7 Certificados....16
7 Observações e restrições....18
8 Gerenciamento de permissões....22
9 Conceitos básicos....25
10 Cobrança....27

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Infográficos do APIG

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



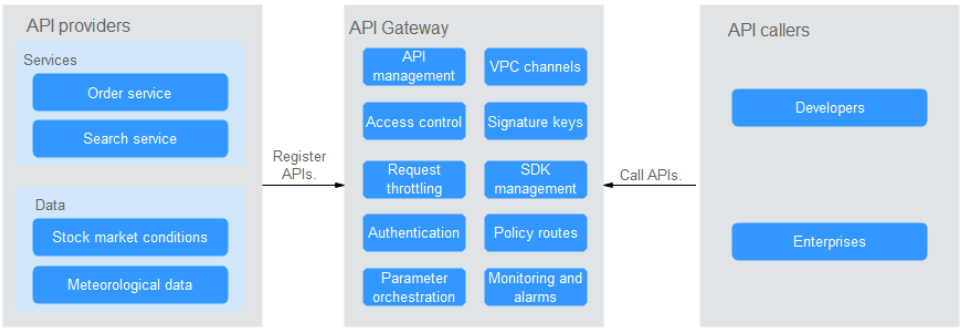
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 O que é o API Gateway?

O API Gateway é um serviço de hospedagem de API de alto desempenho, alta disponibilidade e alta segurança que ajuda você a criar, gerenciar e implementar Interfaces de Programação de Aplicações (APIs) em qualquer escala. Com apenas alguns cliques, você pode integrar sistemas internos, monetizar recursos de serviço e expor recursos seletivamente com custos e riscos mínimos. O API Gateway ajuda você a monetizar os recursos de serviços e reduzir o investimento em pesquisa e desenvolvimento, além de permitir que você se concentre nos principais serviços corporativos para melhorar a eficiência operacional.

- Para monetizar seus serviços e recursos de dados, você pode abri-los criando APIs no API Gateway. Em seguida, você pode fornecer as APIs para chamadores de API usando canais off-line.
- Você também pode obter APIs abertas do API Gateway para reduzir o tempo e os custos de desenvolvimento.

Figura 2-1 Arquitetura do API Gateway



Funções do produto

- **Gerenciamento do ciclo de vida da API**

  O ciclo de vida de uma API envolve a criação, publicação, remoção e exclusão da API. O gerenciamento do ciclo de vida da API permite que você exponha os recursos do serviço de forma rápida e eficiente.

- **Ferramenta de depuração incorporada**

  Com a ferramenta de depuração interna, você pode depurar APIs usando diferentes cabeçalhos HTTP e corpos de solicitação. Esta ferramenta simplifica o processo de desenvolvimento da API e reduz os custos de desenvolvimento e manutenção da API.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- **Gerenciamento de versões**

  Uma API pode ser publicada em diferentes ambientes. Publicar uma API novamente no mesmo ambiente substituirá a versão anterior da API. O API Gateway exibe o histórico de publicações (incluindo a versão, a descrição, a data, a hora e o ambiente) de cada API. Você pode reverter uma API para qualquer versão histórica para atender aos requisitos de lançamento escuro e atualização de versão.

- **Variáveis de ambiente**

  As variáveis de ambiente são gerenciáveis e específicas para ambientes. As variáveis de uma API serão substituídas pelos valores das variáveis no ambiente onde a API será publicada. Você pode criar variáveis em ambientes diferentes para chamar diferentes serviços de back-end usando a mesma API.

- **Limitação de solicitação**
  - Para diferentes serviços e usuários, você pode controlar a frequência de solicitação na qual uma API pode ser chamada por um usuário, uma credencial e um endereço IP. Isso garante que os serviços de back-end possam ser executados de forma estável.
  - A limitação pode ser precisa para o segundo, minuto, hora ou dia.
  - Aplicações e locatários excluídos podem ser configurados para limitar o número de chamadas de API de aplicações e locatários específicos, respectivamente.

- **Monitoramento e alarmes**

  O API Gateway fornece monitoramento de API visualizado e em tempo real e exibe várias métricas, incluindo número de solicitações, latência de invocação e número de erros. As métricas ajudam a entender o uso da API, permitindo identificar possíveis riscos de serviço.

- **Controle de acesso**

  As políticas de controle de acesso são uma das medidas de segurança fornecidas pelo API Gateway. Eles permitem ou negam acesso à API de endereços IP ou contas específicas.

- **Canais de VPC**

  Os canais de VPC podem ser criados para acessar recursos em Virtual Private Clouds (VPCs) e expor recursos de serviços de back-end implementados em VPCs. Um canal de VPC encaminha solicitações de API para servidores diferentes para balanceamento de carga.

- **Chaves de assinatura**

  Uma chave de assinatura consiste em uma chave e um segredo e entra em vigor somente após ser vinculada a APIs. As chaves de assinatura são usadas pelos serviços de back-end para verificar a identidade do API Gateway e garantir o acesso seguro.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Vantagens do produto

Disponível fora da caixa

Você pode criar APIs rapidamente definindo as configurações necessárias no console do API Gateway. O API Gateway fornece uma ferramenta de depuração embutida para simplificar o desenvolvimento da API e permite que você publique uma API em vários ambientes para testes fáceis e iteração rápida.

Gerenciamento conveniente do ciclo de vida da API

O API Gateway fornece gerenciamento de API de ciclo de vida completo, incluindo design, desenvolvimento, teste, publicação e O&M, para ajudá-lo a criar, gerenciar e implementar rapidamente as APIs em qualquer escala.

Limitação de solicitação refinada

O API Gateway combina controle de tráfego síncrono e assíncrono e vários algoritmos para limitar as solicitações no segundo nível. Você pode definir com flexibilidade as políticas de limitação de solicitações para garantir a estabilidade e a continuidade dos serviços de API.

Invocação de função

O **FunctionGraph** funciona perfeitamente com o API Gateway, permitindo expor seletivamente funções do FunctionGraph na forma de APIs.

Monitoramento de API visualizada

O API Gateway monitora o número de chamadas de API, a latência de dados e o número de erros, ajudando você a identificar possíveis riscos de serviço.

Proteção de segurança abrangente

O API Gateway oferece várias medidas para proteger a chamada de API, como transferência Secure Sockets Layer (SSL), controle de acesso estrito, lista negra/lista branca de endereços IP, autenticação, anti-replay, anti-ataque e várias regras de auditoria. Além disso, o API Gateway implementa gerenciamento de cotas flexível e refinado e limitação de solicitações para ajudá-lo a abrir seus serviços de back-end de forma flexível e segura.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Rotas de política flexível

Você pode configurar back-ends para uma API para encaminhar solicitações de acordo com várias políticas. Isso facilita o lançamento escuro e o gerenciamento do ambiente.

Os SDKs de diferentes linguagens de programação

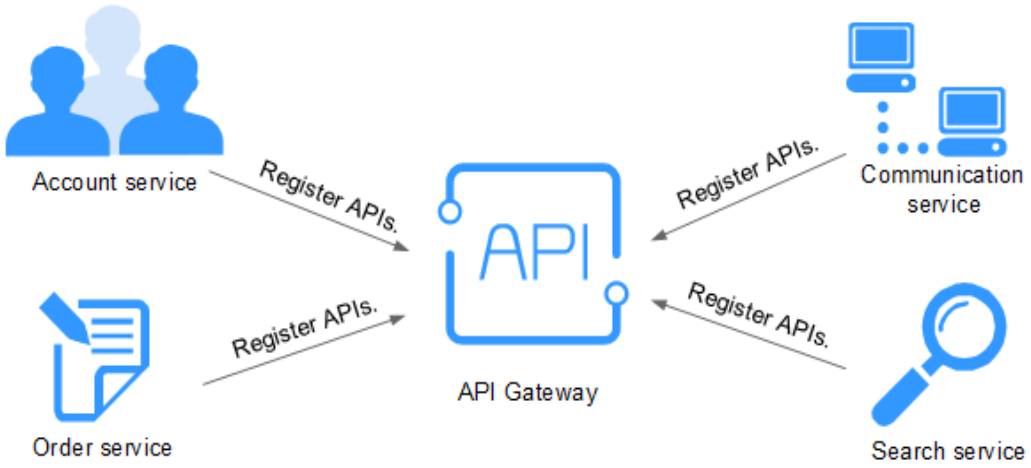
Os SDKs de diferentes linguagens de programação (como Java, Go, Python e C) estão disponíveis para acesso dos clientes. Como os back-ends não precisam ser modificados, apenas um sistema é necessário para se adaptar a diferentes cenários de serviço (como dispositivos móveis e IoT).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Cenários de aplicação

Desacoplamento interno do sistema

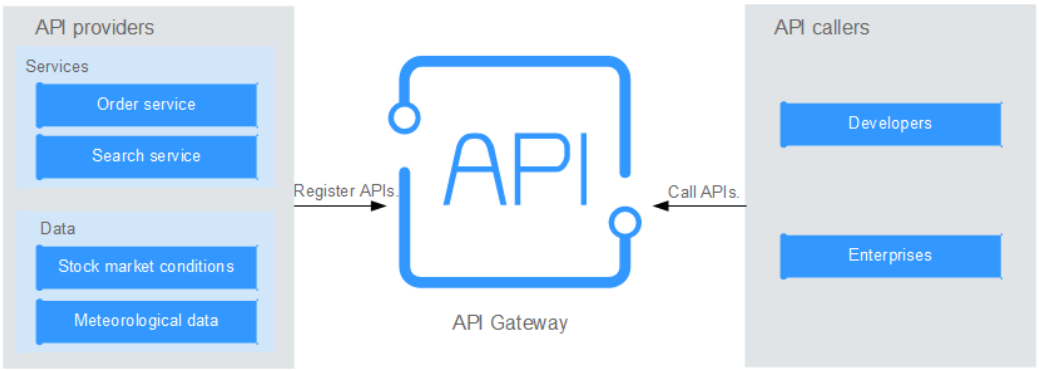
À medida que as empresas se desenvolvem rapidamente com mudanças rápidas nos negócios, os sistemas internos das empresas precisam acompanhar o ritmo do desenvolvimento. No entanto, é difícil garantir a universalidade e a estabilidade do sistema porque os sistemas internos dependem uns dos outros. O APIG usa APIs RESTful padrão para simplificar a arquitetura do serviço, desacoplar sistemas internos e separar o front-end do back-end. As capacidades existentes podem ser reutilizadas para evitar o desenvolvimento repetitivo.



Abertura de recursos empresariais

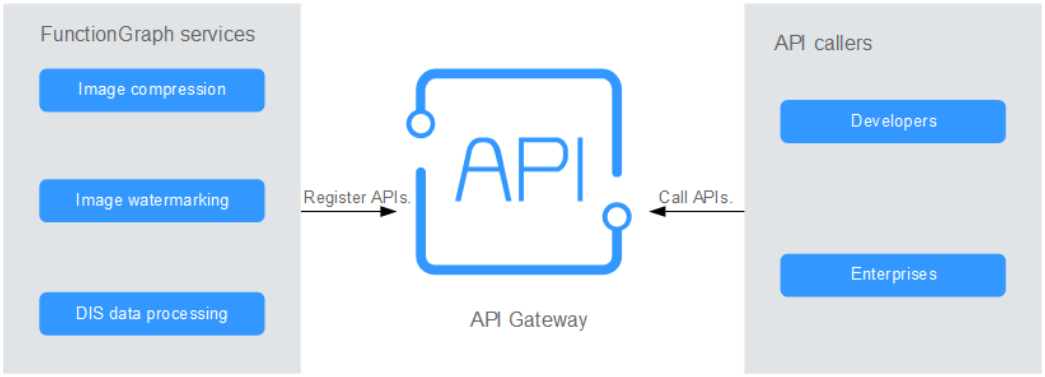
Uma empresa não pode se desenvolver sem os recursos dos parceiros, como uma plataforma de pagamento de terceiros e logon de conta de parceiro. O APIG permite que você exponha seletivamente os recursos aos parceiros usando APIs padrão e compartilhe serviços e dados com parceiros para criar um novo ecossistema.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



Abertura dos serviços de FunctionGraph

O APIG também pode ajudá-lo a expor seletivamente serviços sem servidor (serviços de FunctionGraph) a parceiros. Os serviços de FunctionGraph são mais fáceis de desenvolver, implementar e manter do que os serviços tradicionais. Você pode usar o FunctionGraph para criar rapidamente a lógica de serviço de back-end e usar o APIG para expor funções de lógica de serviço para expansão de simultaneidade linear.



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Especificações

Especificações do gateway compartilhado

O gateway compartilhado não fornece nenhuma configuração de especificação. Veja as cotas para criar e usar APIs em **Observações e restrições**.

NOTA

O recurso de gateway compartilhado foi removido. Em vez disso, use gateways dedicados.

Especificações do gateway dedicado

Tabela 5-1 lista as especificações de gateways de API dedicados.

Tabela 5-1 Especificações de gateways dedicados

Edição	Número máximo de solicitações por segundo
Básica	2000
Profissional	4000
Empresarial	6000
Platina	10.000

Tabela 5-2 Especificações dos gateways dedicados da nova edição

Edição	Número máximo de solicitações por segundo
Básica	2000
Profissional	4000
Empresarial	6000
Platina	10.000
Platina 2	20.000

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Edição	Número máximo de solicitações por segundo
Platina 3	30.000
Platina 4	40.000
Platina 5	50.000
Platina 6	60.000
Platina 7	70.000
Platina 8	80.000

NOTA

- Alguns novos recursos (como modificação de especificação de gateway e política de disjuntores) estão disponíveis apenas em novos gateways. Se o gateway não oferecer suporte a esses recursos, entre em contato com o suporte técnico para atualizá-lo.
- As cotas **padrão** relacionadas à API de gateways dedicados são as mesmas do gateway compartilhado.
- Para gateways dedicados, você pode ajustar o número máximo de solicitações por segundo para cada API.
- Para obter detalhes sobre como modificar as especificações de um gateway dedicado, consulte **Modificação de especificações**.
- Atualmente, a edição platinum 2 e posterior estão disponíveis nas versões **CN-Hong Kong**.
- As especificações de gateway dedicado são obtidas por testes nas seguintes condições:
  - Protocolo: HTTPS
  - Tipo de conexão: conexão longa
  - Solicitações simultâneas: 100
  - Modo de autenticação: nenhum
  - Tamanho dos dados retornados: 1 KB
  - Largura de banda 10 MB/s

Diferenças entre gateways dedicados e compartilhados

O APIG fornece um gateway compartilhado e gateways dedicados. Você pode usar o gateway compartilhado imediatamente ou comprar gateways dedicados para gerenciar APIs.

Gateways dedicados facilitam o desacoplamento de sistemas internos dentro de uma empresa. Os serviços implementados em VPCs se comunicam entre si por meio de APIs RESTful com alta segurança de rede. Gateways dedicados suportam a implantação de serviços de front-end ou back-end em redes públicas, e esses serviços podem ser acessados usando IPs elásticos (EIPs).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Tabela 5-3 Diferenças básicas entre os gateways de API compartilhados e dedicados

Item	Gateway compartilhado	Gateway dedicado
Cobrança	Baseado em chamadas de API.	Com base nas especificações do gateway e na duração do uso.
Acesso à rede	As APIs são acessadas através de redes públicas.	Gateways executados em VPCs. As APIs em uma VPC são chamadas usando o endereço de sub-rede da VPC. Você pode habilitar o acesso a recursos de API em um gateway em redes públicas ou acessar recursos em redes públicas por meio de APIs em um gateway.
Usuários-alvo	Pequenas empresas que têm baixos requisitos de isolamento físico e querem expor seletivamente os recursos da API.	Grandes e médias empresas que querem expor seletivamente e chamar APIs internas. Os gateways dedicados são implantados em clusters fisicamente isolados com diferentes larguras de banda para acesso de entrada e saída.

A tabela a seguir mostra as **diferenças funcionais** entre os gateways de API compartilhados e dedicados.

Tabela 5-4 Diferenças funcionais entre os gateways de API compartilhados e dedicados

Categoria	Características	Gateway compartilhado	Gateway dedicado
Funções básicas	Refinamento de limitação de solicitação	√	√
	Controle de acesso por endereço IP e conta	√	√
	Autenticação de segurança	√	√
	Gerenciamento do ciclo de vida da API	√	√
	Nomes de domínio personalizados	√	√
	Importação e exportação da API Swagger	√	√
	Canais de VPC	√	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Categoria	Características	Gateway compartilhado	Gateway dedicado
	Orquestração de parâmetros da API	√	√
	Gerenciamento de variáveis de grupo da API	√	√
Funções avançadas	Autenticação personalizada	√	√
	Roteamento baseado em políticas	√	√
	Monitoramento de API	√	√
	Balanceamento de carga de back-end	×	√
	Gerenciamento de API interna	×	√
	Acesso a serviços de back-end em nuvens privadas	×	√
	Acesso ao serviço através do Direct Connect	×	√
	Plug-ins	×	√
	Análise de logs	×	√
Indicadores de desempenho	Clusters fisicamente isolados	×	√
	Diferentes larguras de banda para acesso de entrada e saída	×	√
	TPS	200	4000~10.000TPS

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Segurança

6.1 Responsabilidades compartilhadas

Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

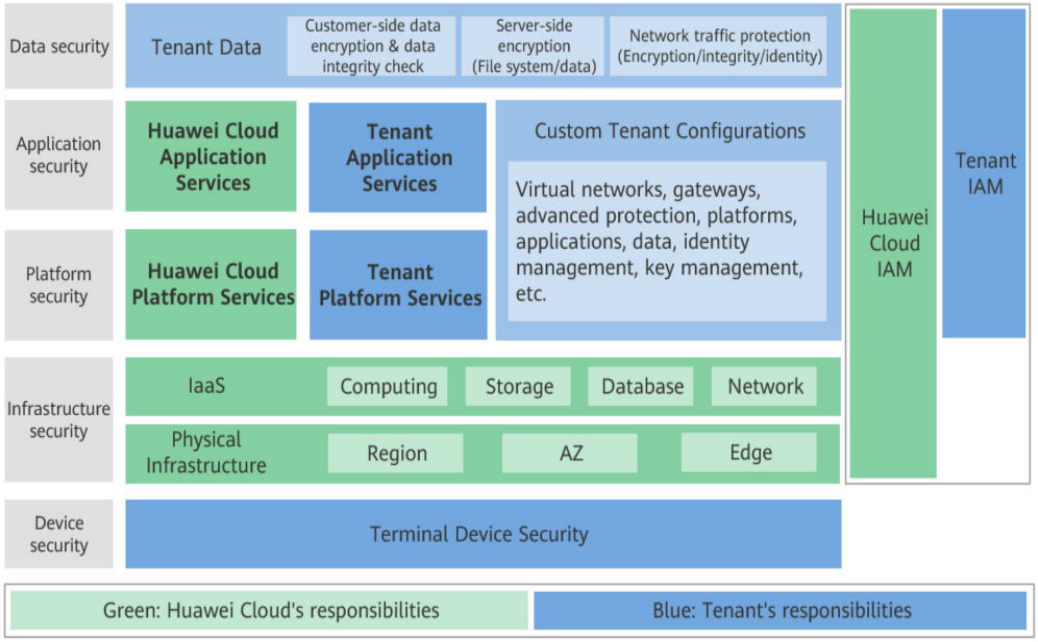
Figura 6-1 ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

O livro branco de segurança da Huawei Cloud elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figura 6-1 Modelo de responsabilidade de segurança compartilhada da Huawei Cloud



6.2 Identificação e gerenciamento de ativos

Gerenciamento de API por grupo durante todo o ciclo de vida, abrangendo criação, depuração, autorização, publicação e colocação off-line

6.3 Autenticação de identidade e controle de acesso

Autenticação da identidade

AK/SK e **autenticação** de token

Autenticação personalizada

Verificação do certificado de serviço de back-end

Autenticação de identidade com chaves de assinatura

Controle de acesso

Limitação de solicitação de API por credencial, API ou endereço IP

Lista negra/lista branca de IP no nível do sistema e da API

Balanceamento de carga e **disjuntor automático**

6.4 Proteção de dados

Transmissão de rede segura através de HTTPS; acesso ao serviço de back-end através de canais seguros

Anti-reprodução e anti-adulteração com algoritmos internos

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

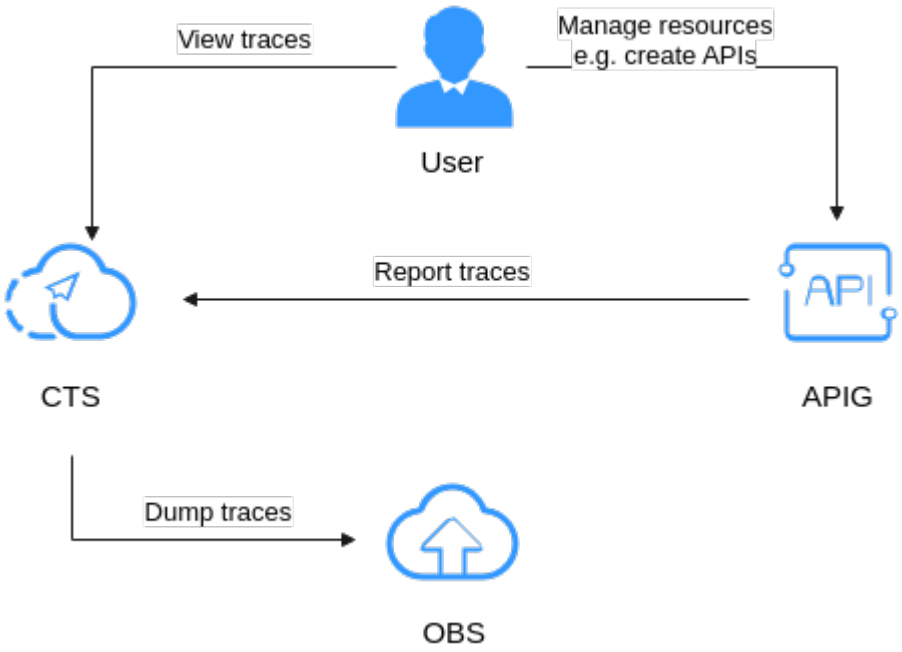
6.5 Auditoria e logs

Auditoria

Cloud Trace Service (CTS) registra as operações nos recursos em nuvem em sua conta. Você pode usar os logs gerados pelo CTS para realizar análises de segurança, rastrear alterações de recursos, auditar a conformidade e localizar falhas.

Depois de ativar o CTS, ele inicia a gravação de operações em recursos de APIG e armazena os registros de operação dos últimos sete dias. Para obter detalhes sobre as operações de APIG que podem ser registradas pelo CTS, consulte **Operações de APIG registradas pelo CTS**.

Figura 6-2 CTS



Para obter detalhes sobre como habilitar e configurar o CTS, consulte **Habilitação do CTS**.

Para obter detalhes sobre como exibir logs de CTS, consulte **Consulta de logs de auditoria**.

Logs

O APIG oferece suporte a modelos de análise de log personalizados, que você pode usar para coletar e gerenciar logs e rastrear e analisar exceções de solicitação de API.

Para obter detalhes sobre como configurar a coleta de logs de APIG, consulte **Análise de log**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6.6 Monitoramento de riscos de segurança

O Cloud Eye fornece monitoramento multidimensional para seus recursos na nuvem. Ele permite que você visualize o uso de recursos e o status de execução do serviço e responda a exceções em tempo hábil para garantir o bom funcionamento dos serviços.

O APIG monitora recursos e operações com base no Cloud Eye, permitindo que você saiba sobre o status de execução do serviço visualizando diferentes métricas no console.

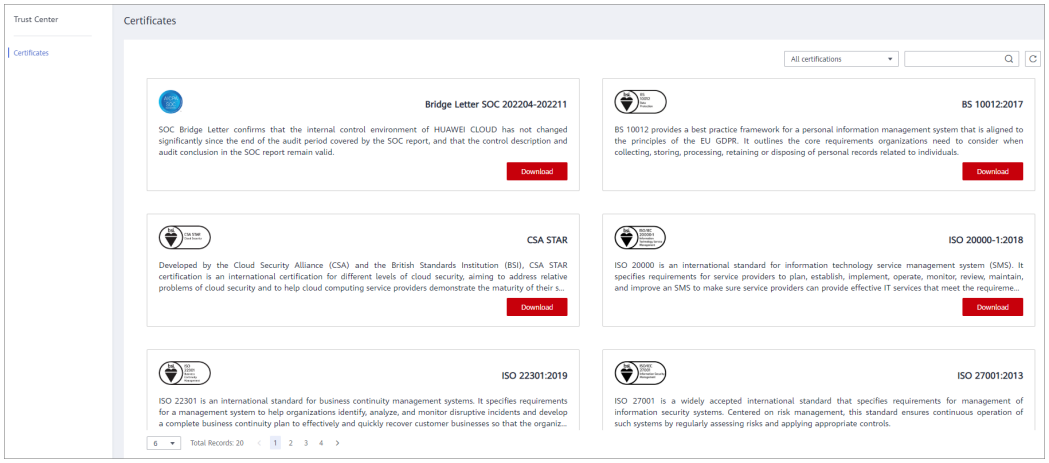
Para obter detalhes sobre as métricas de APIG e como criar regras de alarme, consulte **Monitoramento da API**.

6.7 Certificados

Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO). Você pode **baixá-los** do console.

Figura 6-3 Download de certificados de conformidade

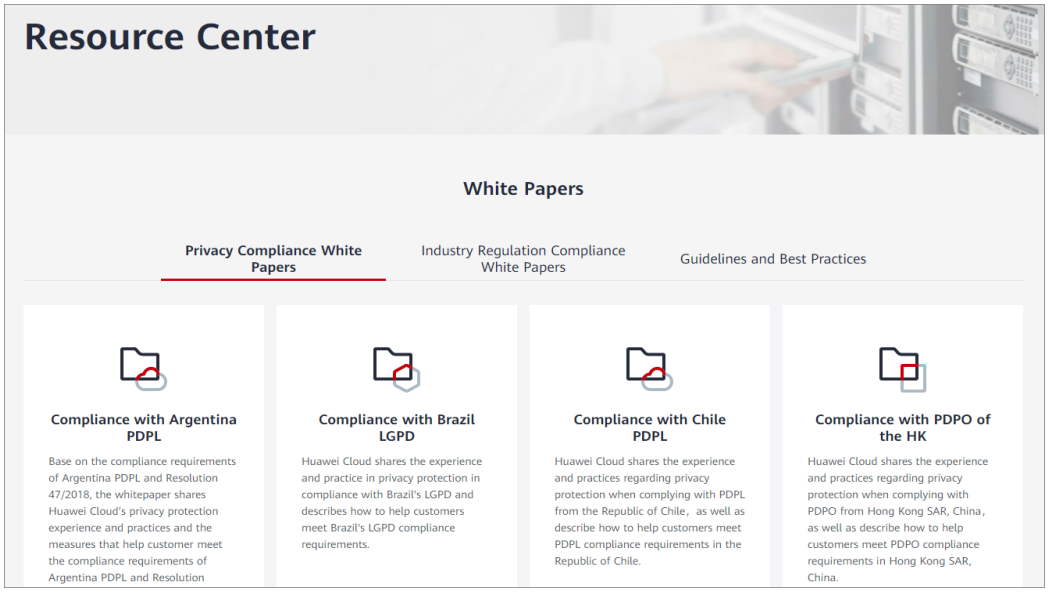


Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figura 6-4 Central de recursos



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7 Observações e restrições

Para alterar as restrições padrão, **aumente a cota**. Para obter detalhes sobre a configuração de parâmetros de um gateway dedicado, consulte **Modificação de parâmetros de configuração**.

Tabela 7-1 Cotas de gateway API compartilhado

Item	Restrição padrão	Modificabilidade
Grupos de API	50	√
APIs	200	√
Políticas de back-end	5	√
Aplicações	50. A cota de aplicações inclui aplicações criadas e aplicações geradas quando as APIs são compradas no KooGallery.	√
Solicitar políticas de limitação	● Você pode criar no máximo 30 políticas de limitação de solicitações. ● O limite de chamadas para um único usuário não pode exceder o limite para a API de destino. ● O limite de chamadas para uma única aplicação não pode exceder o limite para um único usuário. ● O limite de chamadas para um único endereço IP não pode exceder o limite para a API de destino.	√
Ambientes	10	√
Chaves de assinatura	30	√
Políticas de controle de acesso	100	√
Canais de VPC	30	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Item	Restrição padrão	Modificabilidade
Variáveis	Você pode criar no máximo 50 variáveis para um grupo de API em cada ambiente.	√
Nomes de domínio independentes	Um máximo de cinco nomes de domínio independentes podem ser vinculados a um grupo de API.	√
Servidores em nuvem	Um máximo de 200 servidores em nuvem podem ser adicionados a um canal VPC.	√
Parâmetros	Um máximo de 50 parâmetros podem ser criados para uma API.	√
Registros de publicação da API	Um máximo de 10 registros de publicação de uma API podem ser mantidos para cada ambiente.	√
Taxa de acesso à API	Até 200 vezes por segundo	√
Aplicações excluídas	Um máximo de 30 aplicações excluídas pode ser adicionado a uma política de limitação de solicitações.	√
Locatários excluídos	Um máximo de 30 locatários excluídos pode ser adicionado a uma política de limitação de pedidos.	√
Acesso a um nome de subdomínio	Um nome de subdomínio pode ser acessado até 1000 vezes por dia.	x
Tamanho máximo de um pacote de solicitação de API	12 MB	x
Protocolo TLS	TLS 1.1 e TLS 1.2 são suportados. O TLS 1.2 é recomendado.	x
Autorizadores personalizados	20	√

Tabela 7-2 Cotas de gateway API dedicado

Item	Restrição padrão	Modificabilidade
Gateways	5	√
Grupos de API	1500	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Item	Restrição padrão	Modificabilidade
APIs	Número de APIs para cada edição do gateway: ● Básico: 250 ● Profissional: 800 ● Empresarial: 2000 ● Platina: 8000	√
Políticas de back-end	5	√
Credenciais	50 para cada gateway. A cota de credencial inclui as credenciais que você criou.	√
Solicitar políticas de limitação	● Você pode criar um máximo de 300 políticas de limitação de solicitações para cada gateway. ● O limite de chamadas para um único usuário não pode exceder o limite para a API de destino. ● O limite de chamadas para uma única credencial não pode exceder o limite para um único usuário. ● O limite de chamadas para um único endereço IP não pode exceder o limite para a API de destino.	√
Ambientes	10	√
Chaves de assinatura	200	√
Políticas de controle de acesso	100	√
Canais de VPC	200	√
Variáveis	Você pode criar no máximo 50 variáveis para um grupo de API em cada ambiente.	√
Nomes de domínio independentes	Um máximo de cinco nomes de domínio independentes podem ser vinculados a um grupo de API.	√
Servidores em nuvem	Um máximo de 10 servidores em nuvem podem ser adicionados a um canal VPC.	√
Parâmetros	Um máximo de 50 parâmetros podem ser criados para uma API.	√
Registros de publicação da API	Um máximo de 10 registros de publicação de uma API podem ser mantidos para cada ambiente.	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Item	Restrição padrão	Modificabilidade
Taxa de acesso à API	Até 6000 vezes por segundo	√
Aplicações excluídas	Um máximo de 30 aplicações excluídas pode ser adicionado a uma política de limitação de solicitações.	√
Locatários excluídos	Um máximo de 30 locatários excluídos pode ser adicionado a uma política de limitação de pedidos.	√
Acesso a um nome de subdomínio	Um nome de subdomínio pode ser acessado até 1000 vezes por dia.	x
Tamanho máximo de um pacote de solicitação de API	12 MB	√
Protocolo TLS	TLS 1.1 e TLS 1.2 são suportados. O TLS 1.2 é recomendado.	√
Autorizadores personalizados	50	x
Plug-ins	500	√

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

8 Gerenciamento de permissões

Se você precisar atribuir permissões diferentes aos funcionários de sua empresa para acessar seus recursos de APIG, o Identity and Access Management (IAM) é uma boa opção para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos da Huawei Cloud.

Com o IAM, você pode usar sua conta da Huawei Cloud para criar usuários do IAM para seus funcionários e atribuir permissões aos funcionários para controlar seu acesso a recursos específicos.

Se sua conta da Huawei Cloud não exigir usuários individuais do IAM para gerenciamento de permissões, pule este capítulo.

O IAM é gratuito. Você paga apenas pelos recursos em sua conta. Para obter mais informações sobre o IAM, consulte **Visão geral de serviço do IAM**.

Permissões de APIG

Por padrão, os novos usuários do IAM não têm nenhuma permissão atribuída. Você precisa adicionar um usuário a um ou mais grupos e anexar políticas ou funções a esses grupos. Em seguida, o usuário herda permissões dos grupos aos quais pertence e pode executar operações especificadas em serviços de nuvem com base nas permissões.

O APIG é um serviço de nível de projeto implementado e acessado em regiões físicas específicas. Para atribuir permissões APIG a um grupo de usuários, você precisa especificar projetos específicos da região (por exemplo, **ap-southeast-1** para **CN-Hong Kong**) para os quais as permissões entrarão em vigor. Se você selecionar **All projects**, as permissões serão concedidas para o projeto de serviço global e para todos os projetos específicos da região. Ao acessar o APIG, os usuários precisam mudar para uma região onde foram autorizados a usar este serviço.

Você pode conceder permissões usando funções e políticas.

- Funções: um tipo de mecanismo de autorização de granulação grosseira que define permissões relacionadas às responsabilidades do usuário. Esse mecanismo fornece apenas um número limitado de funções de nível de serviço para autorização. Ao usar funções para conceder permissões, você também precisa atribuir outras funções dependentes para que as permissões entrem em vigor. No entanto, as funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em políticas mais flexível e atende aos requisitos de controle de acesso seguro. Por exemplo, você pode conceder aos usuários do APIG apenas as permissões para executar operações específicas. A maioria das políticas define permissões com base em APIs. Para as ações de API suportadas pelo APIG, consulte **Políticas de permissões e ações suportadas**.

Tabela 8-1 lista todas as funções e políticas definidas pelo sistema suportadas pelo APIG.

Tabela 8-1 Funções e políticas definidas pelo sistema suportadas pelo APIG

Nome da função/ política	Descrição	Tipo	Dependência
APIG Administrator	Permissões de administrador para APIG. Os usuários com essas permissões podem usar todas as funções dos gateways **compartilhados** e **dedicados**.	Função definida pelo sistema	Nenhuma
APIG FullAccess	Permissões completas para APIG. Os usuários concedidos a essas permissões podem usar todas as funções de gateways **dedicados**.	Política definida pelo sistema	Nenhuma
APIG ReadOnlyAccess	Permissões somente leitura para APIG. Os usuários com essas permissões só podem exibir gateways **dedicados**.	Política definida pelo sistema	Nenhuma

Você pode visualizar o conteúdo dos papéis e políticas anteriores no console do IAM. Por exemplo, o conteúdo da política de **APIG FullAccess** é o seguinte:

```
{
    "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"
        }
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    ]
}
```

Links úteis

- **Visão geral de serviço do IAM**
- **Criação de um usuário e concessão de permissões de APIG**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

9 Conceitos básicos

API

Um conjunto de funções predefinidas que encapsula as capacidades da aplicação. Você pode criar APIs e torná-las acessíveis aos usuários.

Ao criar uma API, você precisa configurar as informações básicas e os caminhos de solicitação, parâmetros e protocolos de front-end e back-end.

Grupo de API

Uma coleção de APIs usadas para o mesmo serviço. Os grupos de API facilitam o gerenciamento da API.

Ambiente

Um estágio no ciclo de vida de uma API. Um ambiente, como teste de API ou ambiente de desenvolvimento, especifica o escopo de uso das APIs, facilitando o gerenciamento do ciclo de vida da API. A mesma API pode ser publicada em diferentes ambientes.

Para chamar uma API em diferentes ambientes, você precisa adicionar o parâmetro de cabeçalho **x-stage** à solicitação enviada para chamar a API. O valor deste parâmetro é um nome de ambiente.

Variável de ambiente

Uma variável que é gerenciável e específica para um ambiente. Você pode criar variáveis em ambientes diferentes para chamar diferentes serviços de back-end usando a mesma API.

Limitação de solicitação

Controla o número de vezes que as APIs podem ser chamadas por um usuário, uma credencial ou um endereço IP durante um período específico para proteger os serviços de back-end.

A limitação de solicitação pode ser precisa ao minuto e ao segundo.

Controle de acesso

As políticas de controle de acesso são uma das medidas de segurança fornecidas pelo API Gateway. Eles permitem ou negam acesso à API de endereços IP ou contas específicas.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Credencial

Uma entidade que solicita APIs. Uma credencial pode ser autorizada a acessar várias APIs e várias credenciais podem ser autorizadas a acessar a mesma API.

Chave de assinatura

Consiste em uma chave e um segredo, que são usados pelos serviços de back-end para verificar a identidade do API Gateway e garantir o acesso seguro.

Quando uma API vinculada a uma chave de assinatura é chamada, o API Gateway adiciona informações de assinatura às solicitações da API. O serviço de back-end da API assina as solicitações da mesma maneira e verifica a identidade do API Gateway, verificando se a assinatura é consistente com a do cabeçalho **Authorization** enviado pelo API Gateway.

Canal de balanceamento de carga

Um método usado para acessar serviços implementados em VPCs. Você pode expor seletivamente serviços de back-end implementados em VPCs a usuários de terceiros.

Autenticação personalizada

Um mecanismo definido com regras personalizadas para o API Gateway verificar a validade e a integridade das solicitações iniciadas pelos chamadores da API. O mecanismo também é usado para serviços de back-end para verificar as solicitações encaminhadas pelo API Gateway.

Os dois tipos de autenticação personalizada a seguir são fornecidos:

- Autenticação personalizada do front-end: um autorizador personalizado é configurado com uma função para autenticar solicitações de uma API.
- Autenticação personalizada de back-end: um autorizador personalizado pode ser configurado para autenticar solicitações para diferentes serviços de back-end, eliminando a necessidade de personalizar APIs para diferentes sistemas de autenticação e simplificando o desenvolvimento de APIs. Você só precisa criar um autorizador personalizado baseado em função no API Gateway para se conectar ao sistema de autenticação de back-end.

Autenticação simples

A autenticação simples facilita a resposta rápida para solicitações de API adicionando o parâmetro **X-Apig-AppCode** (cujo valor é um AppCode) ao cabeçalho da solicitação HTTP. O API Gateway verifica apenas o AppCode e não verifica a assinatura da solicitação.

Resposta do gateway

As respostas do gateway são retornadas se o API Gateway falhar ao processar solicitações de API. O API Gateway fornece respostas padrão para vários cenários e permite personalizar códigos de status e conteúdo de resposta. Você pode adicionar uma resposta de gateway no formato JSON na página **API Groups**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

10 Cobrança

Para o gateway compartilhado, você será cobrado com base no número de chamadas de API e na quantidade de dados transferidos para fora. Para gateways dedicados, você será cobrado com base na edição de gateway e na duração de uso da largura de banda de acesso de saída.

Para saber mais sobre o preço do APIG e calcular os preços para usar esse serviço, acesse a página **Detalhes de preço do produto**.

Gateway compartilhado

O gateway compartilhado é cobrado com base no **número de chamadas de API recebidas** e na **quantidade de dados transferidos para fora**. As regras de cobrança diferem entre essas duas categorias. Quando uma API é chamada, tanto o número de chamadas quanto o tráfego gerado **serão cobrados**.

Cobrança para chamadas de API

- Item de cobrança: número de chamadas de API que você recebeu
- Modo de cobrança: pagamento por uso
- Ciclo de cobrança: dia
- Tempo de cobrança: as contas geralmente são emitidas dentro de 1 a 3 horas após o término do ciclo de cobrança atual.

Cobrança para transferência de dados

- Item de cobrança: quantidade de dados transferidos para fora
- Preço: taxa padrão para transferência de dados
- Modo de cobrança: pagamento por uso
- Unidade: GB
- Ciclo de cobrança: dia
- Se você usar o APIG em conjunto com serviços de back-end que estão em diferentes regiões ou oferecidos por outros provedores de serviços de nuvem, custos adicionais podem ser incorridos pela transferência de dados do APIG para os serviços de back-end.

Gateway dedicado

Gateways dedicados são faturados com base na **edição de gateway** e na **largura de banda**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Cobrança para a edição de gateway

Gateways dedicados estão disponíveis em quatro edições: básica, profissional, empresarial e platina. Você precisa pagar os preços correspondentes ao comprar essas edições.

O APIG oferece dois modos de cobrança: pagamento por uso e anual/mensal. O modo de pagamento por uso é recomendado se você não puder prever com precisão suas necessidades futuras de serviço e quiser evitar pagar por recursos não utilizados. No entanto, se você puder prever com precisão suas necessidades futuras de serviço, o modo anual/mensal será mais econômico.

- Anual/mensal: oferece um desconto maior do que o modo de pagamento por uso e é recomendado para usuários de longo prazo.
- Pagamento por uso (por hora): você pode iniciar e parar gateways dedicados conforme necessário. Você será cobrado com base na duração pela qual você usa os gateways. A cobrança começa quando um gateway dedicado é comprado e termina quando o gateway é parado devido a atrasos ou é eliminado. A unidade mínima de tempo é um segundo.
- Alteração do modo de cobrança: você pode alterar o modo de cobrança de gateways dedicados de anual/mensal para pagamento por uso ou de pagamento por uso para anual/mensal.

Cobrança para largura de banda

Se o serviço de back-end da API for implementado na rede pública, você será cobrado pela largura de banda para encaminhar solicitações de API para a rede pública. Os preços são calculados com base na **largura de banda** e na **duração** pela qual você usa o gateway.

NOTA

- Se o serviço de back-end for implementado na mesma VPC que o gateway dedicado, o serviço de back-end poderá ser acessado usando um endereço IP privado e você não precisará comprar largura de banda para o gateway.
- Se o gateway dedicado contiver APIs que serão chamadas de redes públicas, você precisará comprar um EIP e vinculá-lo ao gateway.
- Se as APIs em seu gateway dedicado forem chamadas dentro da VPC, você não precisará comprar ou vincular um EIP ao gateway.

Expiração e pagamento em atraso

Se a sua conta estiver em atraso, pode ver os detalhes dos pagamentos em atraso na Central de cobrança. Para evitar que os recursos relacionados sejam interrompidos ou liberados, recarregue sua conta o mais cedo possível. Para obter detalhes, consulte **Recarga e reembolso**.

Cancelamento da assinatura

Para parar de usar gateways dedicados anuais/mensais, cancele a assinatura deles na página **Cancelamentos de assinatura de serviços em nuvem** da Central de cobrança ou na lista de gateways do console de APIG.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.