API Gateway

Perguntas frequentes

Edição	01
Data	2024-09-24

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.

Huawei Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 Perguntas frequentes comuns

Criação de API

- Como definir o endereço de back-end se não for usar um canal de VPC (ou um canal de balanceamento de carga)?
- Como configurar o endereço do serviço de back-end?
- Posso especificar um endereço de balanceador de carga de rede privada para o serviço de back-end?
- Posso especificar o endereço de back-end como um endereço IP de sub-rede?
- Posso vincular nomes de domínio privados para acesso à API?

Chamada de API

- Quais são as possíveis causas para uma falha de chamada de API?
- O que devo fazer se um código de erro for retornado durante a chamada da API?
- O que devo fazer se a mensagem "The API does not exist or has not been published in the environment." é exibida?
- Por que estou vendo a mensagem "No backend available"?
- Quais são as possíveis causas se a mensagem "Backend unavailable" ou "Backend timeout" for exibida?

Autenticação de API

- O APIG oferece suporte à autenticação bidirecional HTTPS?
- Como chamar uma API que não requer autenticação?

Políticas de controle da API

- Posso configurar o número máximo de solicitações simultâneas?
- O APIG tem limites de largura de banda?
- Como fornecer uma API aberta para usuários específicos?
- Como excluir um endereço IP específico para autenticação de identidade de uma API?

Importação e exportação de API

2 Criação de API

2.1 Por que não consigo criar APIs?

A criação de APIs é gratuita. Se você não puder criar APIs, sua conta deve estar em atraso.

2.2 Como definir códigos de resposta para uma API?

As respostas da API são definidas por serviços de back-end (provedores de API). O API Gateway (APIG) apenas transmite respostas de forma transparente aos chamadores da API.

2.3 Como especificar a porta do host para um canal de VPC (ou canal de balanceamento de carga)?

Use a porta do serviço de back-end da API.

2.4 Como definir o endereço de back-end se não for usar um canal de VPC (ou um canal de balanceamento de carga)?

Você pode especificar o endereço de back-end como um nome de domínio público ou um endereço IP público, como o Elastic IP (EIP) de um Elastic Cloud Server (ECS).

2.5 Como configurar o endereço do serviço de back-end?

Configure o endereço de serviço de back-end como um EIP de ECS ou o endereço IP público ou nome de domínio do seu próprio servidor.

2.6 Posso especificar um endereço de balanceador de carga de rede privada para o serviço de back-end?

- Não. O gateway compartilhado é compatível apenas com canais de VPC.
- Para gateways dedicados, você pode usar endereços de balanceador de carga de rede privada.
- Como alternativa, você pode usar o EIP vinculado a um balanceador de carga de rede pública.

2.7 Posso especificar o endereço de back-end como um endereço IP de sub-rede?

Se você usar um gateway dedicado, poderá especificar um endereço IP que pertença à mesma sub-rede em que o gateway está implementado ou o endereço privado de um data center local conectado ao gateway por meio da Direct Connect.

Segmentos de rede não suportados:

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

Se você usar o gateway compartilhado, não será possível especificar o endereço de back-end como um endereço IP de sub-rede. Para um serviço de back-end implementado em vários ECSs localizados na mesma região, mas não vinculados a EIPs, **crie um canal de Virtual Private Cloud (VPC)** e associe os ECSs a ele.

2.8 O APIG oferece suporte a vários pontos de extremidade de back-end?

Sim. O APIG oferece suporte à configuração de vários pontos de extremidade de back-end por meio de um canal de VPC (também chamado de "canal de balanceamento de carga"). Você pode adicionar vários servidores em nuvem a cada canal de VPC.

2.9 O que devo fazer depois de solicitar um nome de domínio independente?

Se você estiver usando o gateway compartilhado, adicione um registro CNAME que aponte o nome de domínio independente para o nome de subdomínio do grupo de API de destino. Se você estiver usando um gateway dedicado, adicione um registro A que aponte o nome de domínio independente para o endereço de acesso de entrada do gateway. Você pode vincular cinco nomes de domínio independentes a um grupo de APIs, mas pode vincular cada nome de domínio independente apenas a um grupo de APIs.

NOTA

Para usar um nome de domínio público, adicione um registro CNAME (gateway compartilhado) ou um registro A (gateway dedicado) no Domain Name Service (DNS).

Para usar um nome de domínio privado, adicione um registro CNAME (gateway compartilhado) ou um registro A (gateway dedicado) no serviço DNS e associe o nome de domínio ao VPC na qual seu serviço de back-end está localizado.

2.10 Posso vincular nomes de domínio privados para acesso à API?

No gateway compartilhado, o nome de domínio a ser vinculado deve ter sido registrado e deve haver registros CNAME apontando o nome de domínio para o nome de subdomínio do grupo ao qual a API de destino pertence. Não é possível vincular nomes de domínio privados ou nomes de domínio que não ofereçam suporte ao acesso público a grupos de API.

Em um gateway dedicado, você pode adicionar um nome de domínio privado e adicionar um registro A para apontar o nome de domínio para o endereço de acesso de entrada do gateway.

2.11 Por que uma API não pode ser chamada entre domínios?

1. Verifique se o CORS foi ativado para a API.

   Vá para a página de detalhes da API, clique em **Edit** e verifique se o CORS está ativado. Se não estiver, habilite-o.

2. Verifique se uma API com o método OPTIONS foi criada. Apenas uma dessas APIs é necessária para cada grupo de APIs.

NOTA

Os parâmetros são os seguintes:

API Group: o mesmo grupo ao qual a API com CORS habilitado pertence.

Method: selecione **OPTIONS**.

Protocol: o mesmo protocolo usado pela API com o CORS ativado.

Path: igual ou prefixo correspondente ao caminho definido para a API com o CORS ativado.

Matching: selecione **Prefix match**.

Authentication Mode: **None** significa que todos os usuários terão acesso. Não é recomendado.

CORS: habilite essa opção.

3 Chamada de API

3.1 Quais são as possíveis causas para uma falha de chamada de API?

Rede

As falhas de chamada de API podem ocorrer em três cenários: dentro de uma VPC, entre VPCs e em uma rede pública.

- Dentro de uma VPC: verifique se o nome de domínio é o mesmo que o alocado automaticamente para a API.
- Entre VPCs: verifique se as duas VPCs estão conectadas. Se elas não estiverem conectadas, crie uma conexão de emparelhamento de VPC para conectar as duas VPCs.

  Para obter detalhes sobre como criar e usar conexões de emparelhamento de VPC, consulte **Visão geral da conexão de emparelhamento de VPC** ou **Exposição de serviços de back-end entre VPCs**.
- Em uma rede pública:
  - A API não está vinculada a um EIP e não tem um endereço válido para acesso à rede pública.

    Vincule um EIP à API e tente novamente. Para obter detalhes, consulte **Ambiente de rede**.
  - As regras de entrada estão configuradas incorretamente.

    Para obter detalhes sobre como configurar regras de entrada, consulte **Ambiente de rede**.
  - O cabeçalho da solicitação "host:*Group domain name*" não é adicionado quando você chama a API. Adicione o cabeçalho da solicitação e tente novamente.

Nome de domínio

- Verifique se o nome de domínio vinculado ao grupo de APIs ao qual a API pertence foi licenciado com sucesso e pode ser resolvido.
- Verifique se o nome de domínio foi vinculado ao grupo de API correto.

- O nome do subdomínio (nome do domínio de depuração) alocado automaticamente ao grupo de APIs é acessado muitas vezes. O nome do subdomínio pode ser acessado apenas 1.000 vezes por dia. É único e não pode ser modificado. Adicione nomes de domínio independentes para o grupo para tornar as APIs do grupo acessíveis.

Publicação de API

Verifique se a API foi publicada. Se a API foi modificada, publique-a novamente. Se a API tiver sido publicada em um ambiente que não seja RELEASE, especifique o cabeçalho **X-Stage** como o nome do ambiente.

Autenticação da API

Se a API usar autenticação de aplicação, verifique se AppKey e AppSecret usados para chamar a API estão corretos.

Políticas de controle da API

- Verifique se a política de controle de acesso vinculada à API está correta.
- Verifique se o limite de limitação de solicitações da API foi atingido. Se nenhuma política de limitação de solicitações for criada para uma API, ela poderá ser acessada 200 vezes por segundo por padrão. Para alterar esse limite, vá para a página **Gateway Information**, clique na guia **Configuration Parameters** e modifique o parâmetro **ratelimit_api_limits**.

3.2 O que devo fazer se um código de erro for retornado durante a chamada da API?

Se um código de erro for retornado quando você chamar suas próprias APIs, **encontre a solução em "Códigos de erro".**

Se um código de erro for retornado ao gerenciar suas APIs, **encontre a solução em "Códigos de erro".**

3.3 Por que estou vendo a mensagem de erro "414 Request-URI Too Large" quando chamo uma API?

O URL da solicitação (incluindo os parâmetros da solicitação) é muito longo. Coloque os parâmetros da solicitação no corpo da solicitação e tente novamente.

3.4 O que devo fazer se a mensagem "The API does not exist or has not been published in the environment." é exibida?

Se uma API aberta no APIG não for chamada, solucione a falha executando as seguintes operações:

1. O nome de domínio, método de solicitação ou caminho usado para chamar a API está incorreto.

  - Por exemplo, uma API criada usando o método POST é chamada com GET.
  - A falta de uma barra (/) no URL de acesso levará a uma falha na correspondência do URL nos detalhes da API. Por exemplo, os URLs **http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test/** e **http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test** representam duas APIs diferentes.

2. A API não foi publicada. As APIs só podem ser chamadas depois de terem sido publicadas em um ambiente. Para obter detalhes, consulte **Publicação de uma API**. Se a API tiver sido publicada em um ambiente que não seja de produção, verifique se o cabeçalho **X-Stage** na solicitação é o nome do ambiente.
3. O nome de domínio foi resolvido incorretamente. Se o nome de domínio, o método de solicitação e o caminho para chamar a API estiverem corretos e a API tiver sido publicada em um ambiente, a API poderá não ser resolvida corretamente para o grupo ao qual a API pertence. Por exemplo, se você tiver vários grupos de API e cada grupo tiver um nome de domínio independente, a API poderá ser chamada usando o nome de domínio independente de outro grupo. Certifique-se de que a API está sendo chamada usando o nome de domínio correto.
4. Verifique se a API permite solicitações entre regiões OPTIONS. Em caso afirmativo, ative o compartilhamento de recursos entre origens (CORS) para a API e crie uma nova API que use o método OPTIONS. Para obter detalhes, consulte **CORS**.

3.5 Por que estou vendo a mensagem "No backend available"?

- Verifique se o serviço de back-end está acessível e modifique o serviço de back-end se estiver inacessível.
- Verifique as configurações do grupo de segurança de ECS do serviço de back-end e verifique se a porta necessária foi habilitada.
- Verifique se as configurações de ACL da VPC restringem a comunicação entre o gateway da API e a sub-rede onde o serviço de back-end está localizado.
- Se você usar um canal de VPC, verifique se a porta de serviço, a porta de verificação de integridade e os servidores de back-end do canal de VPC foram configurados corretamente.

  NOTA

  Os back-ends do gateway compartilhado não suportam a configuração de balanceadores de carga de rede privada.

3.6 Quais são as possíveis causas se a mensagem "Backend unavailable" ou "Backend timeout" for exibida?

A tabela a seguir lista as possíveis causas se um serviço de back-end não for invocado ou a invocação expirar.

Possível causa	Solução
O endereço do serviço de back-end está incorreto.	Altere o endereço do serviço de back-end na definição da API. Se o nome de domínio for usado, verifique se o nome de domínio pode ser resolvido corretamente para o endereço IP do serviço de back-end.
A duração do tempo limite está incorreta. Se um serviço de back-end não retornar uma resposta dentro da duração do tempo limite configurado, o APIG exibe uma mensagem indicando que o serviço de back-end não pode ser invocado.	Aumente a duração do tempo limite de back-end na definição da API.
Se o endereço de back-end for um endereço do ECS, o grupo de segurança ao qual o ECS pertence poderá bloquear a solicitação na direção de entrada ou saída.	Verifique o grupo de segurança ao qual o ECS pertence e certifique-se de que as regras e protocolos de porta de entrada e saída desse grupo de segurança estejam corretos.
O protocolo de solicitação está incorreto. Por exemplo, o serviço de back-end usa HTTP, mas HTTPS é selecionado no APIG.	Certifique-se de que o protocolo da API criada seja o mesmo do serviço de back-end.
O URL do serviço de back-end está inacessível.	Verifique o URL.

3.7 Por que estou vendo a mensagem "Backend domain name resolution failed" quando um serviço de back-end é chamado?

Uma mensagem de erro indicando uma falha de resolução de nome de domínio é exibida quando o serviço de back-end é chamado, embora a resolução de nome de domínio privado seja concluída para a VPC onde o gateway da API está localizado.

Possível causa

A VPC do gateway da API é isolada da VPC do serviço de back-end. Os nomes de domínio privados podem ser resolvidos apenas para a VPC do serviço de back-end.

Solução

- Método 1: ao criar uma API, defina **Backend Address** como um nome de domínio de rede pública.
- Método 2: ao criar uma API, não use um canal de balanceamento de carga. Em vez disso, defina **Backend Address** como o endereço IP do serviço de back-end e adicione um parâmetro constante para especificar o campo **Host** no cabeçalho.
- Método 3: ao criar uma API, especifique um canal de balanceamento de carga.

a. Crie um canal de balanceamento de carga.

b. Adicione o endereço do serviço de back-end.

c. Ao criar uma API, selecione o canal de balanceamento de carga e configure um cabeçalho personalizado.

3.8 Por que a modificação do parâmetro backend_timeout não tem efeito?

Descrição do problema

A modificação do parâmetro **backend_timeout** em um gateway dedicado não tem efeito.

Possíveis causas

O parâmetro **Timeout (ms)** na página **Define Backend Request** não é modificado.

Solução

Faça logon no console do APIG, vá para a página de detalhes da API, clique em **Edit** e modifique o parâmetro **Timeout (ms)** na página **Define Backend Request**.

3.9 Como alternar o ambiente para chamada de API?

Por padrão, a API no ambiente RELEASE é chamada. Se você quiser chamar a mesma API em outro ambiente, adicione o cabeçalho da solicitação **X-Stage** para especificar o nome do ambiente.

3.10 Qual é o tamanho máximo de um pacote de solicitação de API?

Gateway compartilhado: o APIG encaminha apenas solicitações de API cujo corpo não é maior que 12 MB e rejeita solicitações com um corpo maior. Para enviar solicitações com um corpo maior, carregue o corpo da solicitação para o Object Storage Service (OBS).

Gateway dedicado: o APIG encaminha apenas solicitações de API cujo corpo não seja maior que 12 MB. Se o gateway receber solicitações com um corpo maior que 12 MB, modifique o parâmetro **request_body_size** na página de detalhes do gateway. Este parâmetro indica o tamanho máximo de corpo de solicitação permitido. O valor varia de 1 MB a 9536 MB.

3.11 Como executar a autenticação de aplicações no sistema iOS?

O APIG fornece SDKs e demonstrações em várias linguagens, como Java, Python, C, PHP e Go, para autenticação de aplicações. Para usar Objective-C (para iOS) ou outras linguagens, consulte **Princípio de autenticação da aplicação**.

3.12 Por que não posso criar um parâmetro de cabeçalho chamado x-auth-token para uma API chamada por meio da autenticação do IAM?

O parâmetro de cabeçalho **x-auth-token** já foi definido no APIG. Para usar esse parâmetro para chamar uma API, adicione o parâmetro e seu valor ao cabeçalho da solicitação.

3.13 Perguntas frequentes sobre credencial

Quantas credenciais posso criar?

Você pode criar um máximo de 50 credenciais.

Como isolar as informações de chamada entre os terceiros que chamam a mesma API por meio da autenticação da aplicação?

Crie várias credenciais para diferentes terceiros e vincule as credenciais à mesma API.

Há alguma restrição quanto ao número máximo de terceiros que podem chamar a mesma aplicação por meio da autenticação da aplicação?

Sem restrições.

Preciso criar uma credencial para uma API para que ela possa ser chamada por meio da autenticação da aplicação?

Sim, você precisa criar uma credencial e vinculá-la à API. Depois que credencial é criada, AppKey e AppSecret são criados automaticamente. Forneça AppKey e AppSecret para que terceiros chamem a API.

Como uma API pode ser chamada por terceiros por meio da autenticação de aplicações?

Forneça a terceiros AppKey e AppSecret da aplicação que você criou para acessar a API. Os terceiros podem usar AppKey e AppSecret para chamar a API por meio de um SDK. Para obter detalhes sobre como usar um SDK, consulte **Chamada de APIs por meio de autenticação de aplicações**.

3.14 Aplicações de móveis podem chamar APIs?

Sim, as aplicações de móveis podem chamar APIs. No modo de autenticação da aplicação, AppKey e AppSecret de uma aplicação de móvel são substituídos pelos do SDK relevante para assinar a aplicação.

3.15 As aplicações implementadas em uma VPC podem chamar APIs?

Sim, as aplicações implementadas em uma VPC podem chamar APIs por padrão. Se a resolução de nome de domínio falhar, configure um servidor DNS no ponto de extremidade atual seguindo as instruções em **Configurar um servidor DNS de intranet**. Após a configuração, as aplicações implementadas na VPC podem chamar APIs.

Configurar um servidor DNS de intranet

Para configurar um servidor DNS, especifique seu endereço IP no arquivo **/etc/resolv.conf**.

O endereço IP do servidor DNS da intranet depende da região em que você está localizado. Encontre o endereço IP do servidor DNS da intranet na sua região a partir de **endereços de servidores DNS privados**.

Adicione um servidor DNS da intranet com um dos dois métodos seguintes:

- Método 1: modifique as informações de sub-rede da VPC.
- Método 2: edite o arquivo **/etc/resolv.conf**.

NOTA

As configurações do servidor DNS da intranet tornam-se inválidas depois que o ECS reinicia e o servidor DNS da intranet deve ser configurado novamente. Portanto, o método 1 é recomendado.

Método 1

Execute o procedimento a seguir para adicionar um endereço IP de servidor DNS às configurações de sub-rede do ECS na VPC.

Passo 1 Faça logon no console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo para selecionar uma região.

Passo 3 Na lista de serviços, escolha **Compute** > **Elastic Cloud Server**.

Passo 4 Clique no nome do ECS que você deseja usar.

Passo 5 Na página de detalhes do ECS, exiba as informações da NIC e clique em para exibir o nome da sub-rede do ECS.

Passo 6 Na página de informações básicas do ECS, visualize o nome da VPC do ECS.

Passo 7 Clique no nome da VPC para visitar o console da VPC.

Passo 8 Escolha **Subnets** no painel de navegação esquerdo.

Passo 9 Localize a sub-rede mencionada em **Passo 5** e clique no nome da sub-rede.

Passo 10 Altere o endereço do servidor DNS da sub-rede e clique em **OK**.

Por exemplo, altere o endereço para **100.125.1.250**.

Passo 11 Reinicie o ECS. Verifique se o arquivo **/etc/resolv.conf** contém o endereço IP do servidor DNS a ser configurado e se o endereço IP é menor que o de todos os outros servidores DNS.

A figura a seguir mostra o endereço IP **100.125.1.250** do servidor DNS a ser configurado.

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


NOTA

Modificar as informações de sub-rede de uma VPC afetará todos os ECSs criados usando a sub-rede.

----Fim

Método 2

Adicione o endereço IP do servidor DNS da intranet ao arquivo **/etc/resolv.conf**.

Por exemplo, se você estiver localizado em **region01**, adicione um servidor DNS da intranet com o endereço IP **100.125.1.250** ao arquivo **/etc/resolv.conf**.

NOTA

- O endereço IP do novo servidor DNS deve ser menor que o de todos os outros servidores DNS.
- As configurações de DNS entram em vigor imediatamente após o arquivo **/etc/resolv.conf** ser salvo.

3.16 Como implementar a transmissão de dados de WebSocket?

O APIG suporta transmissão de dados de WebSocket. Ao criar uma API, você pode selecionar HTTP, HTTPS ou HTTP&HTTPS. HTTP é equivalente a WebSocket (ws) e HTTPS é equivalente a Segurança de WebSocket (wss).

3.17 O APIG oferece suporte a conexões persistentes?

Sim. Mas você deve usar conexões persistentes corretamente para evitar ocupar muitos recursos.

3.18 Como as solicitações para uma API com várias políticas de back-end serão correspondidas e executadas?

Se várias políticas de back-end forem configuradas para uma API, o APIG corresponderá às políticas de back-end em sequência. Se uma solicitação de API corresponder a uma das políticas de back-end, o APIG encaminhará imediatamente a solicitação para o back-end correspondente e interromperá a correspondência.

Se nenhuma política de back-end for correspondida, a solicitação da API será encaminhada para o servidor back-end padrão.

3.19 Existe um limite no tamanho da resposta a uma solicitação de API?

Não.

3.20 Como acessar serviços de back-end em redes públicas através do APIG?

Habilite **acesso público** para permitir que serviços externos chamem APIs.

Se você encontrar um problema de rede ao chamar APIs, consulte **Quais são as possíveis causas para uma falha de chamada de API?**

4 Autenticação da API

4.1 O APIG oferece suporte à autenticação bidirecional HTTPS?

Gateway dedicado: sim.

- Autenticação bidirecional de front-end: ao vincular um nome de domínio independente, selecione um **certificado SSL** que contém um certificado de AC. A autenticação do cliente, isto é, a autenticação bidirecional, é ativada por padrão.
- Autenticação bidirecional de back-end: ao criar uma API, ative a autenticação bidirecional para o serviço de back-end. For details, see the description about **Two-Way Authentication** in **Creating an API**.

Gateway compartilhado: não. Somente a autenticação unidirecional HTTPS é suportada.

4.2 Como chamar uma API que não requer autenticação?

Para chamar APIs que não exigem autenticação, crie solicitações HTTP padrão e envie-as para o APIG.

NOTA

O APIG **transmite de forma transparente** solicitações para chamar uma API que não requer autenticação para o serviço de back-end. Se você quiser que as solicitações sejam autenticadas no serviço de back-end da API, defina **Security Authentication** como **None**. O chamador da API transfere os campos necessários para autenticação para o serviço de back-end e o serviço de back-end executa a autenticação.

4.3 Quais versões de TLS o APIG suporta?

APIG suporta TLS 1.1 e TLS 1.2, mas não suporta TLS 1.0 ou TLS 1.3.

4.4 O APIG suporta autenticação personalizada?

Sim. Para obter detalhes, consulte "Autorizadores personalizados" no *Guia de usuário do API Gateway*.

4.5 O corpo de solicitação será assinado para autenticação de segurança?

Sim. O corpo da solicitação é outro elemento que precisa ser assinado além dos parâmetros obrigatórios do cabeçalho da solicitação. Por exemplo, quando uma API usada para fazer upload de um arquivo usando o método POST é chamada, o valor de hash do arquivo a ser carregado é calculado para gerar uma assinatura.

Para obter detalhes sobre assinaturas, consulte **Descrição do algoritmo de autenticação de assinatura**.

4.6 Erros comuns relacionados às informações de autenticação do IAM

Você pode encontrar os seguintes erros relacionados às informações de autenticação do IAM:

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

Incorrect IAM authentication information: verify aksk signature fail

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

Possível causa

O algoritmo de assinatura está incorreto e a assinatura calculada pelo cliente é diferente da calculada pelo APIG.

Solução

Método 1: ver logs.

Passo 1 Obtenha o canonicalRequest calculado pelo APIG.

Obtenha **request_id** no corpo da mensagem de erro, pesquise **error.log** (você pode exibir esse arquivo no CLS) do nó shubao com base em **request_id** e obtenha **canonicalRequest** de **error.log**.

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



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

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

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

Passo 2 Obtenha o canonicalRequest calculado pelo cliente imprimindo logs ou usando interrupções de depuração. A tabela a seguir descreve as funções usadas para calcular o canonicalRequest nos SDKs de diferentes linguagens.

Tabela 4-1 Funções para calcular canonicalRequest nos SDKs de linguagens comuns

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

Exemplo: canonicalRequest obtido em uma interrupção de depuração

```
POST
/app1/

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

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

Passo 3 Verifique se o cannonicalRequest em **Passo 1** é o mesmo que em **Passo 2**.

- Sim: verifique se AK e SK estão corretos, por exemplo, sem espaços.
- Não:
  - Diferente na linha 1: o método de solicitação deve ser o mesmo.
  - Diferente na linha 2: o caminho da solicitação deve ser o mesmo.
  - Diferente na linha 3: os parâmetros de solicitação devem ser os mesmos.

- Diferente nas linhas 4 a 5: o cabeçalho da solicitação deve ser o mesmo em cada linha.
- Diferente na linha 7: o número de parâmetros de cabeçalho da solicitação deve ser o mesmo que o número de linhas de cabeçalho da solicitação.
- Diferente na linha 8: o corpo da solicitação deve ser o mesmo.

Tabela 4-2 canonicalRequest de APIG e um cliente

Linha nº	Parâmetro	APIG	Cliente
1	Request method	GET	POST
2	Request path	/app1/	/app1/
3	Request parameters	Nenhum	Nenhum
4	Request header	host:test.com	host:test.com
5	Request header	x-sdk-date:20190126T033427Z	x-sdk-date:20190126T033950Z
6	Blank line	-	-
7	Request header parameters	host;x-sdk-date	host;x-sdk-date
8	Request body hash value	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

----Fim

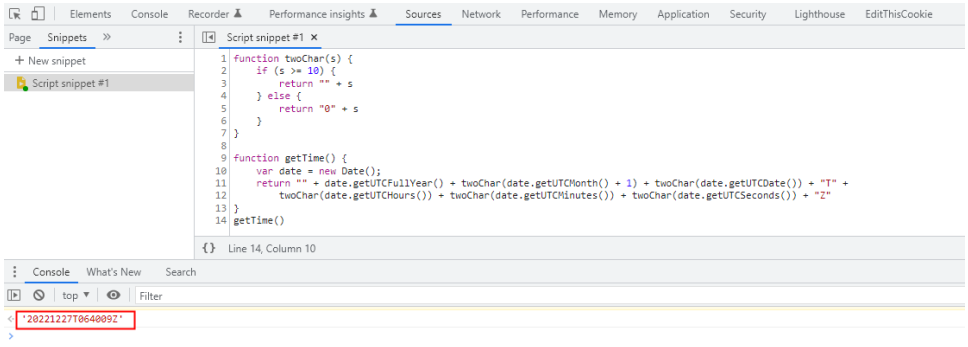
Método 2: comparar a assinatura local com a obtida.

Passo 1 Faça o download do **SDK do JavaScript**, visualize o SDK de assinatura visualizado e obtenha a assinatura.

Passo 2 Descompacte o pacote e abra o arquivo **demo.html** usando um navegador.

Passo 3 Obtenha o valor de **x-sdk-date** e verifique se a diferença entre esse valor e a hora atual está dentro de 15 minutos.

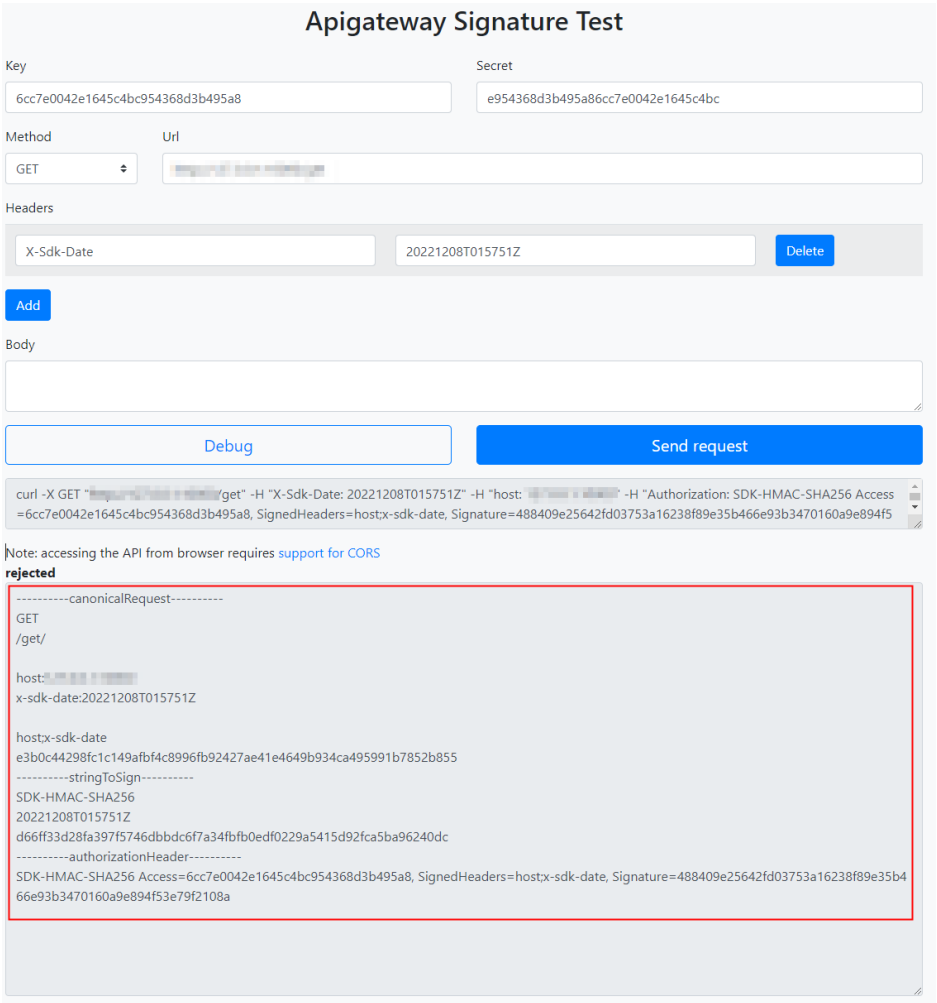
1. Pressione **F12** no teclado e escolha **Sources** > **Snippets** > **New snippet**.
2. Copie o código a seguir para o snippet de script à direita, clique com o botão direito do mouse no nome do snippet à esquerda e selecione **Run** no menu de atalho. O valor exibido na guia **Console** é o valor de **x-sdk-date**.




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

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

Passo 4 Adicione **x-sdk-date** aos **Headers**, defina outros parâmetros e clique em **Debug** para obter a assinatura.



Para todas as solicitações, exceto get, delete e head, adicione um corpo na área **Body** usando o mesmo formato de um corpo de solicitação real.

Passo 5 Copie o comando **curl** na figura de **Passo 4**, execute-o em uma interface de linha de comando e vá para a próxima etapa.

```
curl -X GET "http://192.168.0.1:10000/get" -H "X-Sdk-Date: 20221208T015751Z" -H
"host: 192.168.0.1:10000" -H "Authorization: SDK-HMAC-SHA256
Access=6cc7e0042e1645c4bc954368d3b495a8, SignedHeaders=host;x-sdk-date,
Signature=488409e25642fd03753a16238f89e35b466e93b3470160a9e894f53e79f2108a" -d $''
```

Se um autorizador personalizado for usado, substitua **Authorization** no comando **curl** pelo nome do autorizador.

Passo 6 Compare a assinatura no código local com a assinatura visualizada de JavaScript.

Por exemplo, verifique se os valores de **canonicalRequest**, **stringToSign** e **authorizationHeader** no código de assinatura de Java são os mesmos que os da assinatura visualizada do JavaScript.


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

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

    String messageDigestContent = calculateContentHash(request);

    String[] signedHeaders = getSignedHeaders(request);

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

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

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

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

----Fim

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

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

Possíveis causas

- O cálculo da assinatura de AK/SK está incorreto. Resolva o problema referindo-se a **Incorrect IAM authentication information: verify aksk signature fail**.
- AK e SK não coincidem.
- A autenticação de AK/SK falha por mais de cinco vezes consecutivas e o par de AK/SK é bloqueado por cinco minutos. (As solicitações de autenticação são rejeitadas nesse período).
- Um token expirado é usado para autenticação de token.

Incorrect IAM authentication information: decrypt token fail

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

Possível causa

O token não pode ser analisado para autenticação do IAM da API.

Solução

- Verifique se o token está correto.

- Verifique se o token foi obtido no ambiente onde a API é chamada.

Incorrect IAM authentication information: Get secretKey failed

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

Possível causa

O AK usado para autenticação do IAM da API não existe.

Solução

Verifique se o AK está correto.

5 Políticas de controle da API

5.1 Limitação de solicitação

5.1.1 Posso configurar o número máximo de solicitações simultâneas?

Não, mas você pode limitar o número máximo de chamadas de API permitidas em um período de tempo específico.

5.1.2 A restrição de 1000 solicitações para um nome de subdomínio (nome de domínio de depuração) é aplicada a contas empresariais?

Sim.

5.1.3 O APIG tem limites de largura de banda?

O gateway compartilhado não tem limites na largura de banda. Ele limita as solicitações com base nas políticas de limitação de solicitações e limita o tamanho máximo do corpo a 12 MB.

Gateways dedicados têm limites de largura de banda. Quando você cria um gateway dedicado, pode definir a largura de banda para acesso público de entrada e saída.

5.1.4 Por que uma política de limitação de solicitações não entra em vigor?

- O limite de chamada da API ou o limite de solicitação de endereço IP de origem da política não entra em vigor.

  Verifique se a política foi vinculada a uma API.
- O limite de solicitação do usuário da política não entra em vigor.

  Verifique se a API vinculada à política usa autenticação da aplicação ou do IAM.
- O limite de solicitação de aplicação da política não entra em vigor.

  Verifique se a API vinculada à política usa autenticação de credencial.

5.2 Controle de acesso

5.2.1 Como fornecer uma API aberta para usuários específicos?

Você pode fornecer uma API aberta para usuários específicos de uma das seguintes maneiras:

- Selecione a autenticação da aplicação ao criar a API e compartilhe AppKey e AppSecret com os usuários-alvo.
- Configure uma política de controle de acesso para permitir o acesso de endereços IP ou nomes de conta específicos e vincule a política de controle de acesso à API.

5.2.2 Como excluir um endereço IP específico para autenticação de identidade de uma API?

Você pode escolher uma das seguintes soluções:

- Solução 1: crie uma API que não exija autenticação e configure uma política de controle de acesso para colocar o endereço IP na lista branca.
- Solução 2: crie duas APIs, uma que use o IAM ou autenticação de aplicação e outra que não exija autenticação e configure uma política de controle de acesso para colocar na lista branca o endereço IP da API que não exija autenticação.

5.2.3 Os endereços IP do cliente são verificados para controle de acesso?

Não necessariamente.

No APIG, o controle de acesso é baseado no valor de **$remote_addr**. **$remote_addr** indica um endereço IP do cliente e é determinado pelo modo de acesso. Se um cliente acessa o APIG sem usar nenhum proxy, **remote_addr** é o endereço IP do cliente. Se um cliente acessa o APIG usando um proxy, o cliente primeiro acessa o proxy e o proxy encaminha a solicitação para o APIG. Nesse caso, **remote_addr** é o endereço IP do proxy.

6 Publicação de API

6.1 É necessário publicar uma API novamente após a modificação?

Sim. Depois de modificar os parâmetros de uma API publicada, você deve publicar a API novamente para sincronizar as modificações no ambiente.

6.2 Por que não é possível acessar as APIs publicadas em um ambiente que não seja RELEASE?

Para tornar uma API publicada em um ambiente que não seja RELEASE acessível, adicione o cabeçalho **x-stage** à solicitação da API.

Exemplo:

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

6.3 Posso invocar diferentes serviços de back-end publicando uma API em diferentes ambientes?

Sim, você pode chamar diferentes serviços de back-end publicando uma API em diferentes ambientes e especificando variáveis de ambiente e parâmetros de back-end.

6.4 Como especificar um ambiente para depuração de API?

O APIG depura APIs em um ambiente de depuração específico. Após a conclusão da depuração, você precisa publicar sua API em um ambiente e usar código ou postman para adicionar o cabeçalho **X-Stage** para especificar o ambiente em que deseja chamar a API.

7 Importação e exportação de API

7.1 Por que a importação de API falha?

Possível causa 1: o número de APIs excede o limite máximo permitido para uma única importação. Para obter mais APIs (300), importe-as em lotes ou envie um tíquete de serviço para aumentar o limite.

Possível causa 2: os parâmetros estão incorretos. Verifique e corrija os parâmetros. Recomendamos que você crie uma API no console de APIG, exporte-a e use-a como um modelo para importar APIs.

Possível causa 3: o arquivo YAML está no formato incorreto. Verifique e modifique o arquivo.

Possível causa 4: a rede de proxy local tem restrições. Altere o ambiente de rede.

Possível causa 5: o cabeçalho da solicitação da API contém **X-Auth-Token**. Remova **X-Auth-Token** do cabeçalho.

7.2 O APIG fornece um modelo para importar APIs de arquivos Swagger?

O modelo está sendo desenvolvido.

Atualmente, você pode configurar uma ou duas APIs no APIG e, em seguida, exportá-las para usar como modelos.

8 Segurança da API

8.1 Como proteger minhas APIs?

- Autenticação de identificação

  Configure a autenticação do IAM ou da aplicação para APIs para evitar chamadas maliciosas.

- Políticas de controle de acesso

  Configure uma lista branca ou uma lista negra de endereços IP/intervalos de endereços IP ou contas de APIs para proteger o acesso.

- Políticas de limitação de solicitações

  Por padrão, uma API pode ser chamada até 200 vezes por segundo. Se o seu serviço de back-end não oferecer suporte a essa taxa de acesso, diminua a cota de acordo.

8.2 Como garantir a segurança dos serviços de back-end invocados pelo APIG?

Você pode garantir a segurança dos serviços de back-end invocados pelo APIG usando os seguintes métodos:

- Vincular chaves de assinatura a APIs

  Depois que uma chave de assinatura é vinculada a uma API, o APIG adiciona informações de assinatura a cada solicitação enviada ao serviço de back-end. O serviço de back-end calcula as informações de assinatura em cada solicitação e verifica se as informações de assinatura são consistentes com as do APIG.

- Criptografar solicitações usando HTTPS

  Verifique se o certificado SSL necessário existe.

- Realizar autenticação de back-end

  Habilite a autenticação de segurança para serviços de back-end das APIs desejadas para processar apenas solicitações de API que contenham informações de autenticação corretas.

8.3 Posso controlar o acesso aos endereços IP privados dos ECSs em um canal de VPC (ou canal de balanceamento de carga)?

Não.

9 Outras perguntas frequentes

9.1 Quais são as relações entre uma API, um ambiente e uma credencial?

Uma API pode ser publicada em diferentes ambientes, como RELEASE (ambiente on-line) e BETA (ambiente de teste).

Uma credencial refere-se à identidade de um chamador de API. Depois de criar uma credencial, o sistema gera automaticamente um AppKey e um AppSecret para autenticar a credencial. Depois que uma API é publicada e atribuída a uma credencial, o proprietário de credencial pode chamar a API.

Depois de publicar uma API em ambientes diferentes, você pode definir diferentes políticas de limitação de solicitações e autorizar diferentes credenciais para chamar a API. Por exemplo, durante o processo de teste, a API v2 é publicada no ambiente BETA e autorizada a testar credenciais. A API v1 é estável e pode ser autorizada a todos os usuários ou credenciais no ambiente RELEASE.

9.2 Como usar o APIG?

Você pode usar o APIG para gerenciar e chamar APIs das seguintes maneiras:

- Console de gerenciamento, uma plataforma de gerenciamento de serviços baseada na Web

  Se você já registrou uma conta, faça logon no console de gerenciamento, clique em no canto superior esquerdo e escolha **APIG**.

  Para obter detalhes sobre as funções e operações do console do APIG, consulte o *Guia de usuário do API Gateway*.
- SDKs para Java, Go, Python, JavaScript, C#, PHP, C++, C e Android

  Baixe um SDK e use-o para chamar APIs. Para obter detalhes, consulte o *Guia de desenvolvedor do API Gateway*.

9.3 Quais linguagens de SDK o APIG suporta?

O APIG suporta SDKs de Java, Go, Python, C#, PHP, JavaScript, C++, C e Android.

9.4 Posso fazer upload de arquivos usando o método POST?

Sim.

O APIG encaminha apenas solicitações de API cujo corpo não seja maior que 12 MB.

Se você estiver usando gateways dedicados, configure o tamanho máximo de corpo da solicitação permitido definindo o parâmetro **request_body_size**. O valor varia de 1 MB a 9536 MB.

NOTA

Atualmente, apenas o corpo da solicitação pode ser transmitido de forma transparente.

9.5 Como são as mensagens de erro retornadas pelo APIG?

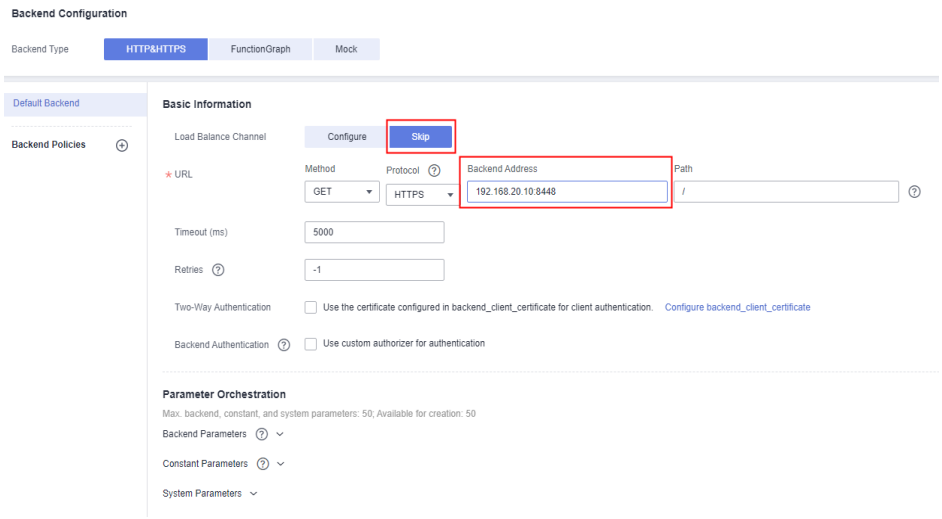
Ao receber uma solicitação de API, o APIG retorna uma resposta. Um corpo de resposta semelhante é o seguinte:

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

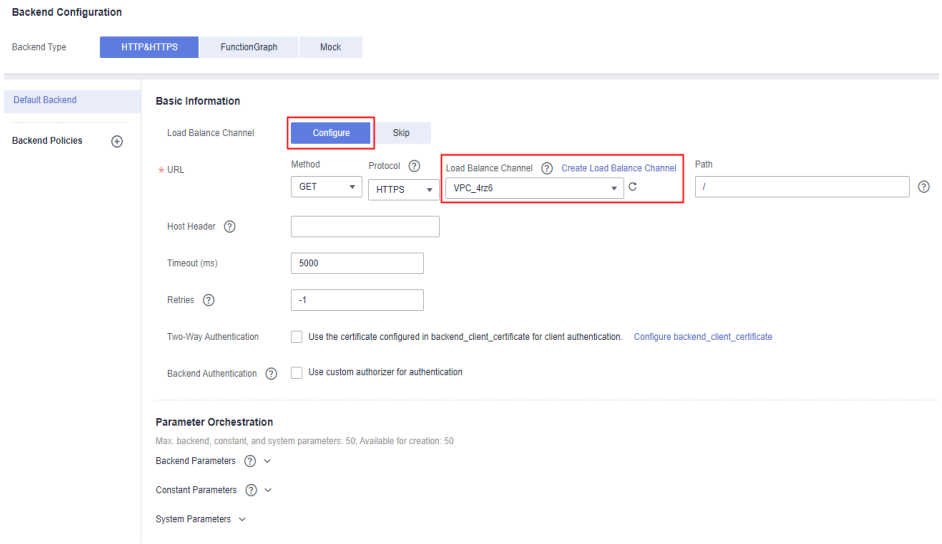
- **"error_code"**: código de erro
- **"error_msg"**: descrição do erro

9.6 Como usar o APIG para abrir os serviços implementados na Huawei Cloud?

- Para um serviço implementado na Huawei Cloud com um **public network IP address**, especifique o endereço IP como o endereço de serviço de back-end ao criar uma API no APIG. Se o serviço tiver sido vinculado a um nome de domínio, use o nome de domínio como o endereço do serviço de back-end. Para obter detalhes sobre como criar uma API, consulte **Criação de uma API**.



- Para um serviço implementado na Huawei Cloud sem um endereço IP de rede pública, especifique um canal de VPC para acesso ao serviço de back-end ao criar uma API no APIG. Para obter detalhes sobre como criar um canal de VPC e uma API, consulte **Criação de um canal de balanceamento de carga** e **Criação de uma API**.



9.7 Posso atualizar o gateway compartilhado para um gateway dedicado?

Atualmente, você não pode atualizar o gateway compartilhado para um gateway dedicado. No entanto, você pode fazer o seguinte para alcançar o mesmo objetivo:

1. Compre um gateway dedicado.
2. Exporte APIs do gateway compartilhado.
3. Importe as APIs para o gateway dedicado.
4. Vincule um novo nome de domínio para as APIs e altere o registro de DNS para CNAME o nome de domínio para o endereço IP de acesso público do gateway dedicado.

9.8 Por que todos os botões no console do APIG estão indisponíveis?

Verifique se a sua conta está em atraso e, se necessário, faça uma recarga.

9.9 O APIG pode ser implementado em um data center local?

Não. O APIG não pode ser implementado em um data center local.

