Guia de usuário do API Gateway

Guia de usuário

Edição 01

Data 2023-05-08

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 Comparação de versões

O novo console do API Gateway (APIG) está disponível desde 26 de setembro de 2022. A tabela a seguir lista as diferenças entre os consoles antigos e novos. Você pode saber mais sobre o novo console clicando em **Video Tutorial** na página **Overview**.

Tabela 1-1 Comparação de versões

Diferença	Antigo	Novo
Autenticação de dois fatores	Não suportado	Suportado
Configuração de tentativas para serviços de back-end HTTP&HTTPS	Não suportado	Suportado
Importação de API	Para registrar APIs	Para registrar APIs ou criar grupos de APIs
Depuração de API com um corpo personalizado	Não suportado	Suportado
Página de detalhes da API	Média	Altamente integrado
Topologia da API	Suportado	Não suportado
Exibição visual das políticas da API	Não suportado	Suportado
Criação de política por script	Não suportado	Suportado
Tipo de plug-in	CORS, gerenciamento de cabeçalho de resposta HTTP, limitação de solicitações	CORS, gerenciamento de cabeçalho de resposta HTTP, limitação de solicitações 2.0, Kafka log push, disjuntor. Esses plug-ins são gerenciados em conjunto com as políticas tradicionais.
Gerenciamento de certificados SSL	Não suportado	Suportado

Diferença	Antigo	Novo
Criação de grupos de servidores para canais de balanceamento de carga	Não suportado (canais de VPC)	Suportado
Interruptor de verificação de integridade para canais de balanceamento de carga	Não suportado (canais de VPC)	Suportado
Exibição de nós em espera e status para canais de balanceamento de carga	Não suportado (canais de VPC)	Suportado
Aplicações	Suportado	Agora chamado de "credenciais"
Políticas de cota de credenciais	Não suportado	Suportado
Políticas de controle de acesso	Não suportado	Suportado
Monitoramento de API	Fornecido na página **Dashboard**	Agora chamado de "Monitoramento de API"
Nome do subdomínio	Suportado	Agora chamado de "nome de domínio de depuração"
Gerenciamento de variáveis	Variáveis	Agora chamado de **Environment Variables**
Seleção de gateway no painel de navegação esquerdo	Não suportado	Suportado
Platinum 2 e versões posteriores	Não suportado	Suportado
Monitoramento da largura de banda	Não suportado	Suportado
Importação de cargas de trabalho do CCE	Não suportado	Suportado

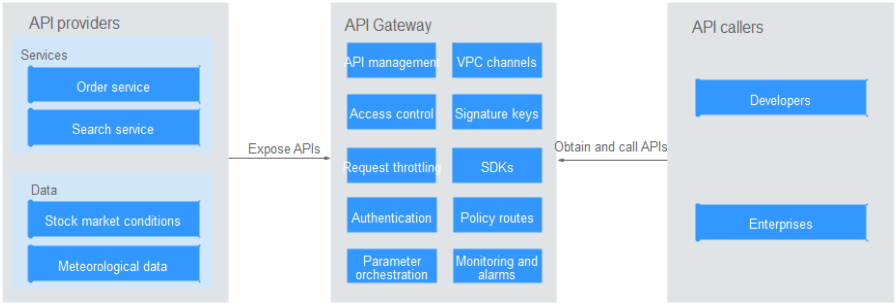
2 Visão geral

O APIG é um serviço totalmente gerenciado que permite criar, gerenciar e implementar APIs com segurança em qualquer escala, com alto desempenho e disponibilidade. Com o APIG, você pode facilmente integrar seus sistemas de serviços internos e expor e monetizar seletivamente seus recursos de serviços.

Procedimento geral

A figura a seguir mostra o procedimento para usar APIG para hospedar APIs.

Figura 2-1 APIG

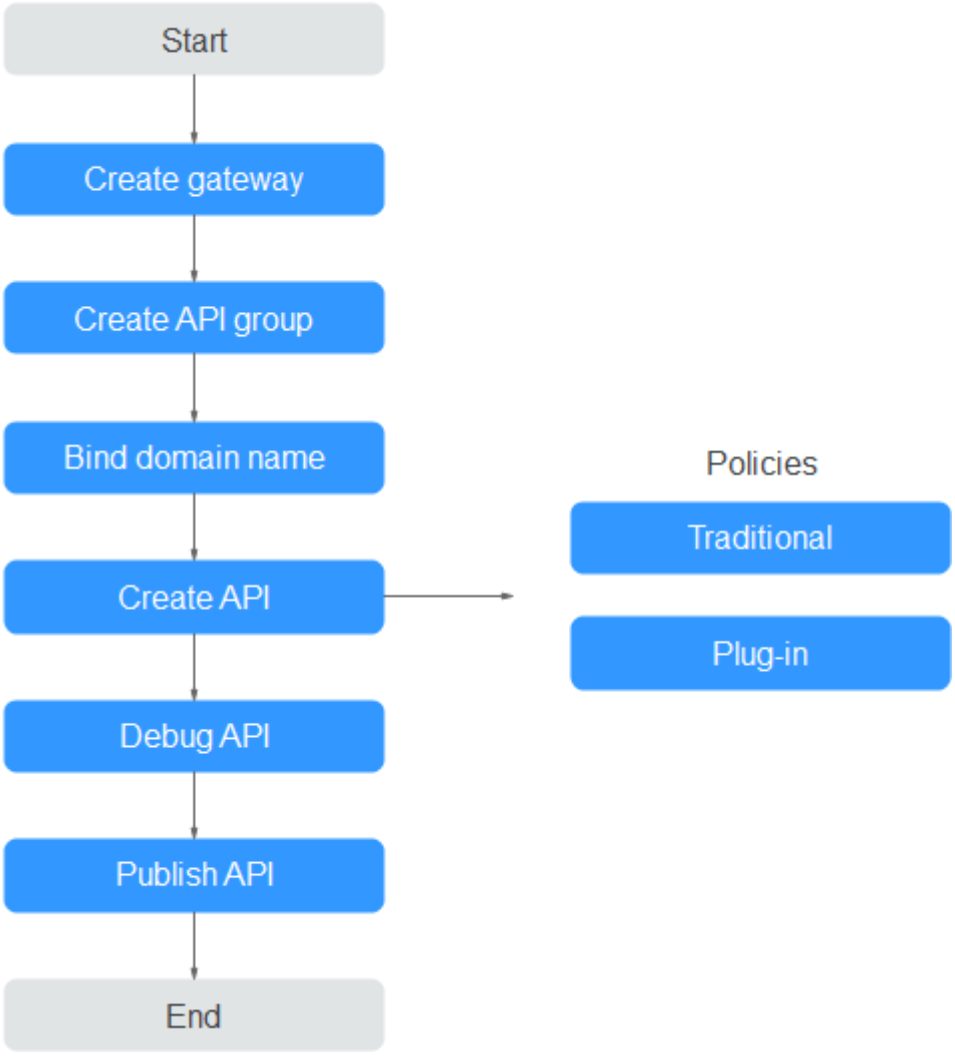


Você pode **expor seus serviços de API** ou **obter e chamar APIs de outras** por meio do APIG.

Exposição de APIs

Empresas ou desenvolvedores expõem e monetizam seletivamente seus serviços e dados através do APIG.

Figura 2-2 Processo de exposição da API



1. **Compre um gateway.**

   Um gateway é um espaço de recursos independente onde todas as operações são realizadas. Os recursos de diferentes gateways são isolados uns dos outros.

2. **Crie um grupo de APIs**.

   Cada API pertence a um grupo de APIs. Crie um grupo de APIs antes de criar uma API.

3. **Vincule um nome de domínio.**

   Antes de expor uma API, vincule um nome de domínio independente ao grupo de destino para que os chamadores da API possam acessar a API.

   Você pode depurar a API usando o nome de domínio de depuração alocado ao grupo ao qual a API pertence. O nome de domínio pode ser acessado no máximo 1000 vezes por dia.

4. **Crie uma API.**

   Encapsule os serviços de back-end existentes em APIs RESTful padrão e os exponha a sistemas externos.

   Depois de criar uma API, defina as seguintes configurações para controlar o acesso à API:

- Políticas tradicionais
  - **Limitação de solicitação**

    A limitação de solicitações controla o número de vezes que uma API pode ser chamada dentro de um período de tempo para proteger os serviços de back-end.
  - **Controle de acesso**

    Defina uma lista negra ou uma lista branca para negar ou permitir acesso à API de endereços IP ou contas específicas.
  - **Chaves de assinatura**

    As chaves de assinatura são usadas pelos serviços de back-end para verificar a identidade do APIG.
- Políticas de plug-in
  - **CORS**

    Essa política fornece os recursos de especificar cabeçalhos de solicitação de comprovação e cabeçalhos de resposta e criar automaticamente APIs de solicitação de comprovação para acesso à API de origem cruzada.
  - **Gerenciamento de cabeçalho de resposta HTTP**

    Você pode personalizar cabeçalhos de resposta HTTP que estarão contidos em uma resposta da API.
  - **Limitação de solicitação 2.0**

    Essa política permite limitar o número de vezes que uma API pode ser chamada em um período de tempo específico. A limitação baseada em parâmetro, básica e excluída é suportada.
  - **Push de log de Kafka**

    Essa política envia logs de chamada de API para o Kafka para que os usuários possam obtê-los facilmente.
  - **Disjuntor**

    Essa política protege seu serviço de back-end quando ocorre um problema de desempenho.

5. **Depure a API.**

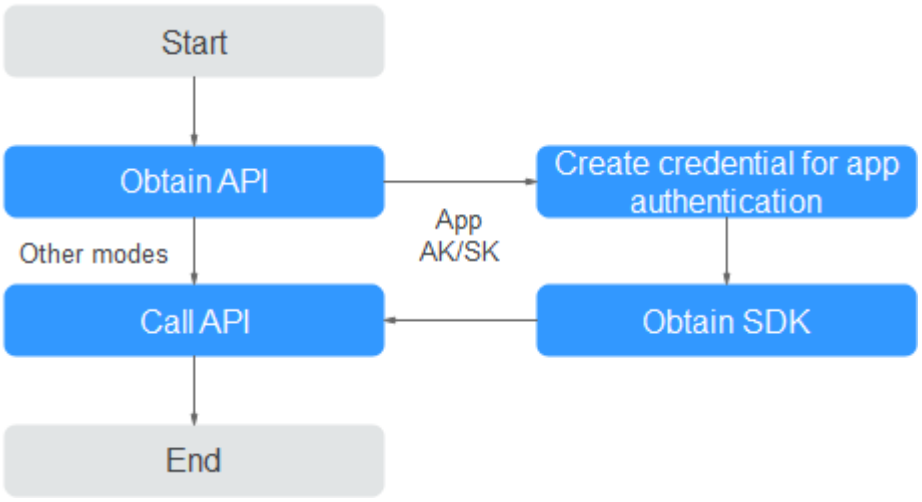
   Verifique se a API está funcionando normalmente.
6. **Publique a API.**

   A API só pode ser chamada depois de ter sido publicada em um ambiente.

Chamada das APIs

Empresas e desenvolvedores obtêm e chamam APIs de outros provedores, reduzindo assim o tempo e os custos de desenvolvimento.

Figura 2-3 Processo de chamada da API



1. **Obtenha uma API.**

   Obtenha as informações de solicitação da API, incluindo o nome de domínio, o protocolo, o método, o caminho e o modo de autenticação.

2. **Crie uma credencial.**

   Para uma API que usa autenticação de aplicação, crie uma credencial para gerar um ID de credencial e um par de chave/segredo. Vincule a credencial à API para que você possa chamar a API por meio da autenticação da aplicação.

3. **Obtenha um SDK.**

   Use o SDK para gerar uma assinatura para a AK/SK e chamar a API.

4. **Chame a API.**

   Chame a API usando seu endereço de acesso e execute a autenticação com base em seu modo de autenticação.

Acessar o novo console do APIG

Passo 1 Faça logon na Huawei Cloud e clique em **Console** no canto superior direito.

Passo 2 Passe o mouse sobre ☰ a esquerda para expandir a lista de serviços e insira **apig**.

Passo 3 Clique em **API Gateway** para acessar o novo console.

O novo console suporta apenas gateways dedicados. Compre um gateway seguindo as instruções neste documento antes de usar o console.

----Fim

3 Gerenciamento de API

3.1 Criação de um grupo de APIs

Um grupo de APIs contém APIs usadas para o mesmo serviço. Você pode gerenciar APIs por grupo e deve criar um grupo antes de criar uma API.

Você pode criar um grupo de APIs usando um dos seguintes métodos:

- **Criação de um grupo de APIs diretamente**

  Você pode criar APIs para o grupo conforme necessário.
- **Importar um arquivo de design de API**

  Importe um arquivo de API para criar um grupo.

NOTA

- Para disponibilizar suas APIs para acesso dos usuários, vincule nomes de domínio independentes ao grupo ao qual as APIs pertencem.
- Cada API pode pertencer a apenas um grupo.
- O sistema aloca automaticamente um nome de subdomínio para cada grupo de API para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia.
- Um grupo de APIs padrão é gerado automaticamente para cada gateway. As APIs no grupo padrão podem ser chamadas usando o endereço IP da Virtual Private Cloud (VPC) onde o gateway é implementado.

Pré-requisitos

Você **comprou um gateway**.

Criação de um grupo de APIs diretamente

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Escolha **Create API group** > **Create Directly** e insira as informações do grupo.

Tabela 3-1 Informações do grupo

Parâmetro	Descrição
Name	Nome do grupo de APIs.
Description	Descrição do grupo de APIs.

Passo 5 Clique em **OK**.

----Fim

Importar um arquivo de design de API

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Escolha **Create API Group** > **Import API Design File**.

Passo 5 Selecione um arquivo de API e clique em **Open**.

Passo 6 Defina os parâmetros de importação.

Tabela 3-2 Parâmetros para importar APIs

Parâmetro	Descrição
Import	Opções: ● **New group**: importar APIs para um novo grupo de APIs. Se você selecionar essa opção, o sistema criará automaticamente um grupo de APIs e importará as APIs para esse grupo. ● **Existing group**: importar APIs para um grupo de APIs existente. Se você selecionar essa opção, o sistema adicionará as APIs ao grupo de APIs selecionado, mantendo as APIs existentes no grupo de APIs.
API group	Selecione um grupo de API se você definir **Import** para **Existing group**.
Basic Definition Overwrite	Determine se deve substituir uma API existente se o nome da API for o mesmo de uma API importada. Este parâmetro está disponível somente se você definir **Import** para **Existing group**.
Extended Definition Overwrite	Se essa opção estiver selecionada, os itens de definição estendida (controle de acesso e políticas de limitação de solicitações) de uma API importada substituirão as políticas existentes com o mesmo nome.

Passo 7 (Opcional) Para configurar as APIs, clique em **Configure Global Settings**.

1. Altere o modo de autenticação. Para mais detalhes, consulte **5.2**.

2. Modifique a configuração da solicitação de back-end. Para mais detalhes, consulte **Passo 1**.
3. Clique em **Next**. Você pode exibir os detalhes de configuração no formato form, JSON ou YAML.
4. Confirme as configurações e clique em **Submit**.

Passo 8 Clique em **Import Now** e determine se deseja publicar as APIs.

- **Now**: publique as APIs em um ambiente especificado agora.
- **Later**: **publique as APIs** mais tarde.

Passo 9 Clique em **OK**. A página de guia **APIs** é exibida, mostrando as APIs importadas.

----Fim

Operações de acompanhamento

Depois que um grupo de APIs for criado, **vincule nomes de domínio independentes** a ele para que os chamadores da API possam usá-los para chamar APIs abertas no grupo.

3.2 Importação de uma carga de trabalho do CCE

Ao importar cargas de trabalho do Cloud Container Engine (CCE), você pode abrir seus recursos de serviço CCE por meio de APIs.

Precauções

- Somente os clusters do CCE Turbo e os clusters do CCE que usam o modelo de rede VPC são suportados.
- O cluster do CCE e o gateway devem estar na mesma VPC ou conectados de outra forma.
- Se você selecionar um cluster do CCE que usa um modelo de rede VPC, adicione o bloco CIDR do contêiner do cluster a **Routes** na página de detalhes do gateway.
- Após a importação, as APIs serão geradas, juntamente com um canal de balanceamento de carga de microsserviço que monitora e atualiza as alterações de endereço de todos os pods na carga de trabalho.

Pré-requisitos

Você criou uma **carga de trabalho CCE**.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Groups**.

Passo 4 Escolha **Create API Group** > **Import CCE Workload**. Defina os parâmetros de acordo com a tabela a seguir.

Tabela 3-3 Descrição do parâmetro

Parâmetro	Descrição
Group	Grupo ao qual pertence a carga de trabalho do CCE que você criará. Você pode optar por criar um grupo ou selecionar um grupo existente.
Cluster	Selecione um cluster. Clique em **View CCE Console** para exibir os clusters disponíveis.
Namespace	Namespace ao qual a carga de trabalho pertencerá. Um namespace é uma coleção abstrata de recursos e objetos.
Workload Type	● **Deployment**: as implementações não armazenam dados ou status enquanto estão em execução. ● **StatefulSet**: os StatefulSets armazenam dados e status durante a execução. ● **DaemonSet**: DaemonSet garantem que apenas um pod seja executado em todos ou em alguns nós. Quando um nó é adicionado a um cluster, um novo pod também é adicionado para o nó. Quando um nó é removido de um cluster, o pod também é recuperado. Se um DaemonSet for excluído, todos os pods criados por ele serão excluídos. Para obter detalhes sobre esses tipos de carga de trabalho, consulte **Visão geral**.
Protocol	**HTTP** e **HTTPS** são suportados. O **HTTPS** é recomendado para a transmissão de dados importantes ou sensíveis.
Request Path	Você pode usar um sinal de adição (+) para correspondência de prefixo. Por exemplo, **/a/{b+}**.
Port	Porta de escuta da carga de trabalho do CCE.
Authentication Mode	Autenticação de aplicações e IAM é suportada. Você também pode optar por não autenticar as solicitações. ● **App**: as solicitações serão autenticadas pelo APIG. Este modo de autenticação é recomendado. ● **IAM**: as solicitações serão autenticadas pelo IAM. ● **None**: nenhuma autenticação será necessária.
CORS	Determine se deve ativar o compartilhamento de recursos de origem cruzada (CORS). O CORS permite que navegadores enviem XMLHttpRequest para servidores em outros domínios, superando a limitação de que Asynchronous JavaScript and XML (AJAX) podem ser usados apenas no mesmo domínio. Existem dois tipos de solicitações CORS: ● Solicitações simples: solicitações que possuem o campo **Origin** no cabeçalho. ● Solicitações não tão simples: solicitações HTTP enviadas antes da solicitação real. Se o CORS (solicitação não tão simple) estiver ativado para uma API, outra API que use o método OPTIONS deve ser criada. Para obter detalhes, consulte **Ativar CORS**.

Parâmetro	Descrição
Timeout (ms)	Tempo limite de solicitação de back-end. Se ocorrer um erro de tempo limite de back-end durante a depuração da API, aumente o tempo limite para localizar o motivo. **NOTA** Modifique o tempo limite máximo fazendo referência a **Configuração de parâmetros**. O intervalo de valores é de 1 ms a 600.000 ms.

Passo 5 Clique em **OK**.

----Fim

3.3 Gerenciamento de nomes de domínio

Antes de expor as APIs, vincule nomes de domínio independentes ao grupo ao qual as APIs pertencem, para que os chamadores da API possam acessar essas APIs. As APIs também podem ser acessadas usando o nome de domínio de depuração alocado ao grupo.

- Depuração de nome de domínio: o sistema aloca automaticamente um nome de domínio de depuração exclusivo para cada grupo de API para teste interno. O nome de domínio pode ser acessado 1000 vezes por dia e não pode ser modificado.
- Nome de domínio independente: um nome de domínio independente é um nome de domínio personalizado usado para que os chamadores da API chamem APIs abertas no serviço ao qual o nome de domínio está vinculado.

NOTA

- Grupos sob o mesmo gateway não podem ser vinculados a um mesmo nome de domínio independente.
- Por padrão, o nome de domínio de depuração de um grupo de APIs só pode ser resolvido para um servidor na mesma VPC que o gateway. Se você quiser resolver o nome de domínio para uma rede pública, vincule um EIP ao gateway.

Pré-requisitos

1. Existe um nome de domínio independente disponível.
2. Um registro CNAME aponta um nome de domínio independente para o nome de subdomínio de um grupo de APIs. Para obter detalhes, consulte **Adição de um conjunto de registros CNAME**.
3. Se o grupo de API contiver APIs HTTPS, **crie um certificado SSL** para o nome independente.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Clique na guia **Group Information**.

Passo 6 Na área **Independent Subdomain Names**, clique em **Bind Independent Domain Name**. Em seguida, configure as informações do nome de domínio.

Tabela 3-4 Configuração de nome de domínio independente

Parâmetro	Descrição
Domain Name	Nome de domínio a ser vinculado ao grupo de APIs.
Minimum TLS Version	A versão mínima do TLS que pode ser usada para acessar o nome de domínio. TLS 1.1 e TLS 1.2 (recomendado) são suportados. Este parâmetro aplica-se apenas a HTTPS e não tem efeito para HTTP e outros modos de acesso.

Passo 7 Clique em **OK**.

Se o nome de domínio não for mais necessário, clique em **Unbind Domain Name** para desvinculá-lo do grupo de APIs.

Passo 8 (Opcional) Se o grupo de APIs contiver APIs HTTPS, vincule um certificado SSL ao nome de domínio independente.

1. Na linha que contém o nome de domínio, clique em **Select SSL Certificate**.
2. Selecione um certificado SSL e clique em **OK**.

   Se nenhum certificado SSL estiver disponível, clique em **Create SSL Certificate** para criar um. Para mais detalhes, consulte **Certificados SSL**.

----Fim

Solução de problemas

- Falha na vinculação de um nome de domínio independente: ele já existe ou não é CNAMEd para o nome de domínio de depuração do grupo de APIs.
- Falha na vinculação de um certificado SSL: o nome de domínio usado para gerar o certificado SSL é diferente do nome de domínio independente de destino.

Operações de acompanhamento

Depois de vincular nomes de domínio independentes ao grupo de APIs, crie APIs no grupo para expor seletivamente os recursos de back-end. Para mais detalhes, consulte **Criação de uma API**.

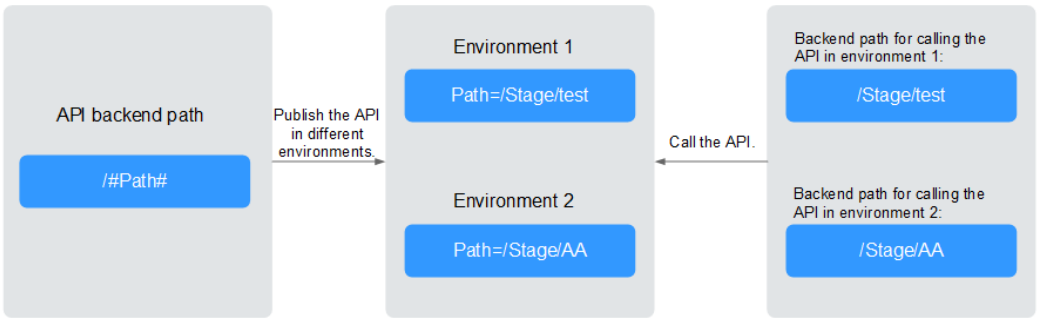
3.4 Adição de uma variável de ambiente

Você pode definir variáveis de ambiente para permitir que uma API seja chamada em ambientes diferentes.

As variáveis de ambiente são gerenciáveis e específicas para ambientes. Você pode adicionar variáveis em diferentes ambientes para chamar diferentes serviços de back-end usando a mesma API.

Para variáveis definidas durante a criação da API, você deve criar variáveis e valores correspondentes. Por exemplo, a variável **Path** é definida para uma API e duas variáveis com o mesmo nome são criadas e atribuídas valores **/Stage/test** e **/Stage/AA** nos ambientes 1 e 2, respectivamente. Se a API for publicada e chamada no ambiente 1, o caminho **/Stage/test** será usado. Se a API for publicada e chamada no ambiente 2, o caminho **/Stage/AA** será usado.

Figura 3-1 Uso de variáveis de ambiente



Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Clique na guia **Group Information**.

Passo 6 Na área **Environment Variables**, selecione um ambiente. Se nenhum ambiente estiver disponível, clique em **Create Environment** para criar um.

Passo 7 Clique em **Add Environment Variable** e insira as informações da variável.

AVISO

Os nomes e valores das variáveis de ambiente serão exibidos em texto sem formatação nas solicitações da API. Não inclua informações confidenciais nos nomes e valores das variáveis.

Tabela 3-5 Adição de uma variável de ambiente

Parâmetro	Descrição
Name	Nome da variável. Verifique se o nome é igual ao nome da variável definida para a API.
Value	O caminho a ser usado no ambiente selecionado.

Passo 8 Clique em **OK**.

----Fim

3.5 Criação de uma resposta de gateway

Uma resposta de gateway é exibida se o APIG falhar ao processar uma solicitação de API. O APIG fornece um conjunto de respostas padrão e também permite que você crie respostas com códigos de status e conteúdo personalizados. O conteúdo da resposta deve estar no formato JSON.

Por exemplo, o conteúdo de uma resposta de gateway padrão é o seguinte:

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

Você pode adicionar uma resposta com o seguinte conteúdo:

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

Você pode adicionar mais campos ou excluir campos existentes do corpo JSON.

NOTA

- Você pode criar um máximo de quatro respostas de gateway para cada grupo.
- O tipo de uma resposta padrão ou personalizada não pode ser modificado, mas o código de status e o conteúdo da resposta podem.
- O tipo de resposta de gateway não pode ser alterado. Para mais detalhes, consulte **Tipos de respostas**.
- As respostas do gateway podem conter as variáveis de contexto do gateway da API (começando com **$context**). Para mais detalhes, consulte **Variáveis de contexto**.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Clique na guia **Group Information**.

Passo 6 Na área **Gateway Responses**, crie ou modifique as respostas do gateway.

Para cancelar modificações em uma resposta padrão, clique em **Restore Defaults** no canto superior direito.

----Fim

Tipos de respostas

A tabela a seguir lista os tipos de resposta suportados pelo APIG. Você pode definir códigos de status para atender aos seus requisitos de serviço.

Tabela 3-6 Tipos de resposta de erro suportados pelo APIG

Nome da resposta	Código de status padrão	Descrição
Acesso negado	403	Acesso negado. Por exemplo, a política de controle de acesso é acionada ou um ataque é detectado.
Erro de configuração do autorizador	500	Ocorreu um erro de autorizador personalizado. Por exemplo, a comunicação falhou ou uma resposta de erro foi retornada.
Autorizador falhou	500	Falha na autorização personalizada.
Fonte de identidade incorreta	401	A origem de identidade do autorizador personalizado está ausente ou é inválida.
Falha de autenticação	401	Falha na autenticação do IAM ou da aplicação.
Fonte de identidade não encontrada	401	Nenhuma fonte de identidade foi especificada.
Tempo limite de back-end	504	A comunicação com o serviço de back-end expirou.
Back-end indisponível	502	O serviço de back-end não está disponível devido a um erro de comunicação.
Padrão 4XX	-	Outro erro 4XX ocorreu.
Padrão 5XX	-	Outro erro 5XX ocorreu.
Nenhuma API encontrada	404	Nenhuma API foi encontrada.
Parâmetros de solicitação incorretos	400	Os parâmetros de solicitação estão incorretos ou o método HTTP não é suportado.
Solicitação limitada	429	A solicitação foi rejeitada devido à limitação de solicitação.
Credencial não autorizada	401	A credencial que você está usando não foi autorizada a chamar a API.

Variáveis de contexto

Tabela 3-7 Variáveis que podem ser usadas no corpo da mensagem de resposta

Variável	Descrição
$context.apiId	ID da API.
$context.appId	ID da credencial que chama a API.

Variável	Descrição
$context.requestId	ID da solicitação gerada quando a API é chamada.
$context.stage	Ambiente de implementação no qual a API é chamada.
$context.sourceIp	Endereço IP de origem do chamador da API.
$context.authorizer.frontend.property	Valores dos pares de valor do atributo especificados mapeados para o contexto na resposta do autorizador personalizado do front-end
$context.authorizer.backend.property	Valores dos pares de valor do atributo especificados mapeados para o contexto na resposta do autorizador personalizado de back-end
$context.error.message	Mensagem de erro.
$context.error.code	Código de erro.
$context.error.type	Tipo de erro.

3.6 Criação de uma API

Você pode expor seletivamente seus back-ends configurando suas APIs no APIG. Para fazer isso, crie uma API com as seguintes etapas:

- **Configurar configurações de front-end**

  Definições de front-end, configurações de segurança e parâmetros de solicitação
- **Configurar configurações de back-end**

  Back-end padrão, políticas de back-end e respostas
- **(Opcional) Criação de uma política**

  Políticas tradicionais e de plug-in

NOTA

O APIG usa uma arquitetura de API baseada em REST, portanto, a abertura e a chamada da API devem estar em conformidade com as especificações da API RESTful relacionadas.

Pré-requisitos

- Você criou um grupo de APIs. Se nenhum grupo de APIs estiver disponível, crie um fazendo referência a **Criação de um grupo de APIs**.
- Se o serviço de back-end precisar usar um canal de balanceamento de carga, **crie um canal** primeiro.
- Se você precisar usar um autorizador personalizado para autenticação de API, **crie um**.

Configurar configurações de front-end

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Na página **APIs**, clique em **Create**.

1. Configure os parâmetros de front-end descritos na tabela a seguir.

Tabela 3-8 Definição de front-end

Parâmetro	Descrição
API Name	Digite um nome de API que esteja em conformidade com regras específicas para facilitar a pesquisa.
Group	O grupo ao qual a API pertence.
URL	Endereço de front-end, que consiste em um método, protocolo, nome de subdomínio e caminho. - **Method**: selecione **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS** ou **ANY**. **ANY** indica que todos os métodos de requisição são suportados. - **Protocol**: selecione **HTTP**, **HTTPS** ou **HTTP&HTTPS**. O **HTTPS** é recomendado para a transmissão de dados importantes ou sensíveis. - **Subdomain Name**: depuração do nome de domínio do grupo ao qual a API pertence. - **Path**: caminho para solicitar a API. Inclua parâmetros em chaves. Por exemplo: **/a/{b}**. Ou use um sinal de mais (+) para corresponder aos parâmetros que começam com caracteres específicos. Por exemplo: **/a/{b+}**.
Gateway Response	Exibido se uma solicitação de API não for processada. O APIG fornece um conjunto de respostas padrão e também permite que você **crie novas respostas** com códigos de status personalizados e conteúdo na página **Group Information**. O conteúdo da resposta deve estar no formato JSON.

Parâmetro	Descrição
Matching	Opções: - **Exact match**: a API pode ser chamada apenas usando o caminho de solicitação especificado. - **Prefix match**: a API pode ser chamada usando caminhos começando com os caracteres correspondentes. Por exemplo, se você definir o caminho da solicitação como **/test/AA** e o modo de correspondência como **Prefix match**, a API poderá ser chamada usando **/test/AA/CC**, mas não poderá ser chamada usando **/test/AACC**. **NOTA** Se você definir o modo de correspondência como **Prefix match**, os caracteres do caminho da solicitação da API excluindo o prefixo serão transmitidos de forma transparente para o back-end. Por exemplo, se você definir os caminhos de solicitação de front-end e back-end de uma API como **/test/** e **/test2/**, respectivamente, e a API for chamada usando **/test/AA/CC**, os caracteres **AA/CC** serão transmitidos de forma transparente para o back-end. O URL de solicitação recebida pelo back-end é **/test2/AA/CC/**.
Tags	Atributos usados para identificar rapidamente a API de outras APIs.
Description	Descrição da API.

2. Defina as configurações de segurança com base na tabela a seguir.

Tabela 3-9 Configuração de segurança

Parâmetro	Descrição
Authentication Mode	Os seguintes modos de autenticação estão disponíveis: - **App**: as solicitações para a API serão autenticadas pelo APIG. A autenticação da aplicação é recomendada. - **IAM**: as solicitações para a API serão autenticadas pelo Identity and Access Management (IAM). - **Custom**: as solicitações para a API serão autenticadas usando seu próprio sistema ou serviço de autenticação (por exemplo, um sistema de autenticação baseado em OAuth). - **None**: nenhuma autenticação será necessária. A chamada da API varia dependendo do modo de autenticação. Para obter detalhes, consulte **Guia de desenvolvedor**. **AVISO** – Se você definir o modo de autenticação como **IAM** ou **None**, qualquer usuário do APIG poderá acessar a API, o que pode resultar em cobranças excessivas se a API for bombardeada com solicitações maliciosas. – Se você definir o modo de autenticação como **Custom**, poderá criar uma função no FunctionGraph para interconectar com seu próprio sistema ou serviço de autenticação. Certifique-se de que o FunctionGraph esteja disponível na região atual.
Simple Authentication	Esse parâmetro está disponível somente se você definir **Security Authentication** como **App**. Se você selecionar autenticação de aplicação, configure se deseja ativar a autenticação simples. Na autenticação simples, o parâmetro **X-Apig-AppCode** é adicionado ao cabeçalho da solicitação HTTP para uma resposta rápida. O APIG verifica apenas o AppCode e o conteúdo da solicitação não precisa ser assinado. A autenticação simples suporta apenas solicitações HTTPS e não suporta solicitações HTTP. Para mais detalhes, consulte **Adição de um AppCode para autenticação simples**. **NOTA** Depois de ativar a autenticação simples para uma API existente, você precisa publicar a API novamente. Para mais detalhes, consulte **Publicação de uma API**.
Two-Factor Authentication	Esse parâmetro estará disponível somente se o **Authentication Mode** estiver definido como **App** ou **IAM**. Determine se deve ativar a autenticação de dois fatores para a API. Se essa opção estiver ativada, as solicitações de API serão autenticadas usando um autorizador personalizado, além da autenticação da aplicação ou do IAM especificada.

Parâmetro	Descrição
Custom Authorizer	Este parâmetro é obrigatório apenas se **Authentication Mode** estiver definido como **Custom**. Se nenhum autorizador personalizado estiver disponível, clique em **Create Custom Authorizer** para criar um.
CORS	Determine se deve ativar o compartilhamento de recursos de origem cruzada (CORS). O CORS permite que navegadores enviem XMLHttpRequest para servidores em outros domínios, superando a limitação de que Asynchronous JavaScript and XML (AJAX) podem ser usados apenas no mesmo domínio. Existem dois tipos de solicitações CORS: - Solicitações simples: solicitações que possuem o campo **Origin** no cabeçalho. - Solicitações não tão simples: solicitações HTTP enviadas antes da solicitação real. Se o CORS (solicitação não tão simple) estiver ativado para uma API, outra API que use o método OPTIONS deve ser criada. Para obter detalhes, consulte **Ativar CORS**.

3. (Opcional) Defina os parâmetros de solicitação descritos na tabela a seguir.

Tabela 3-10 Configuração de parâmetros de solicitação

Parâmetro	Descrição
Parameter Name	Nome do parâmetro de solicitação. O nome de um parâmetro de caminho será exibido automaticamente nesta coluna. **NOTA** – O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**. – O nome do parâmetro não pode ser **x-stage**. – Se você definir a localização do parâmetro como **HEADER**, verifique se o nome do parâmetro não é **Authorization** ou **X-Auth-Token** e não contém sublinhados (_).
Parameter Type	Opções: **STRING** e **NUMBER**. **NOTA** Defina o tipo de parâmetros Boolean como **STRING**.
Required	Determine se o parâmetro é necessário em cada solicitação enviada para chamar a API. Se você selecionar **Yes**, as solicitações de API que não contiverem o parâmetro serão rejeitadas.
Passthrough	Determine se o parâmetro deve ser transmitido de forma transparente para o serviço de back-end.

Parâmetro	Descrição
Enumerated Value	Valor enumerado do parâmetro. Use vírgulas (,) para separar vários valores enumerados. O valor deste parâmetro só pode ser um dos valores enumerados.
Default Value	O valor que será usado se nenhum valor for especificado para o parâmetro quando a API for chamada. Se o parâmetro não for especificado em uma solicitação, o APIG enviará automaticamente o valor padrão para o serviço de back-end.
Value Restrictions	- Comprimento máximo/valor máximo: se **Parameter Type** estiver definido como **STRING**, defina o comprimento máximo do valor do parâmetro. Se **Parameter Type** estiver definido como **NUMBER**, defina o valor máximo do parâmetro. - Comprimento mínimo/valor mínimo: se **Parameter Type** estiver definido como **STRING**, defina o comprimento mínimo do valor do parâmetro. Se **Parameter Type** estiver definido como **NUMBER**, defina o valor mínimo do parâmetro.
Example	Exemplo de valor para o parâmetro.
Description	Descrição do parâmetro.

Passo 6 Clique em **Next** para prosseguir **Configurar configurações de back-end**.

----Fim

Configurar configurações de back-end

O APIG permite que você defina várias políticas de back-end para diferentes cenários. As solicitações que atendam às condições especificadas serão encaminhadas para o back-end correspondente. Por exemplo, você pode fazer com que certas solicitações para uma API sejam encaminhadas para um back-end específico especificando o endereço IP de origem nas condições de política do back-end.

Você pode definir no máximo cinco políticas de back-end para uma API, além do back-end padrão.

Passo 1 Defina o back-end padrão.

As solicitações de API que não atenderem às condições de qualquer back-end serão encaminhadas para o back-end padrão.

Na página **Backend Configuration**, selecione um tipo de back-end.

A APIG oferece suporte a back-ends **HTTP&HTTPS**, **FunctionGraph** e **Mock**. Para obter detalhes sobre os parâmetros necessários para definir cada tipo de serviço de back-end, consulte **Tabela 3-11**, **Tabela 3-12** e **Tabela 3-13**.

NOTA

- Os back-ends do FunctionGraph podem ser definidos apenas se o FunctionGraph tiver sido implementado no ambiente atual.
- Se o serviço de back-end não estiver disponível, use o modo Mock para retornar o resultado esperado ao chamador da API para depuração e verificação.

Tabela 3-11 Parâmetros para definir um serviço back-end HTTP&HTTPS

Parâmetro	Descrição
Load Balance Channel	Determine se deve usar um canal de balanceamento de carga para acessar o serviço de back-end. Se você selecionar **Configure**, certifique-se de ter **criado um canal de balanceamento de carga**.

Parâmetro	Descrição
URL	Um URL consiste em um método, protocolo, canal de balanceamento de carga/endereço de back-end e caminho. ● Método Selecione **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS** ou **ANY**. **ANY** indica que todos os métodos de requisição são suportados. ● Protocolo **HTTP** ou **HTTPS**. O **HTTPS** é recomendado para a transmissão de dados importantes ou sensíveis. **NOTA** – O WebSocket é compatível com HTTP e HTTPS. – Este protocolo deve ser o utilizado pelo serviço de back-end. ● Canal de balanceamento de carga (se aplicável) Selecione um canal de balanceamento de carga. **NOTA** Para garantir uma verificação de integridade bem-sucedida e a disponibilidade do serviço, configure os grupos de segurança dos servidores em nuvem em cada canal para permitir o acesso a partir de 100.125.0.0/16. ● Endereço de back-end (se aplicável) **Defina este parâmetro se nenhum canal de balanceamento de carga for usado.** Digite um endereço de back-end no formato de "endereço IP do host ou nome de domínio":"número da porta". A porta padrão (80 para HTTP e 443 para HTTPS) será usada se você não especificar uma porta. Portas disponíveis: 1 a 65535. Se você quiser usar uma variável, coloque o nome da variável em sinais numéricos (#), por exemplo, **#ipaddress#**. Você pode usar múltiplas variáveis, por exemplo, **#ipaddress##test#**. **NOTA** Gateways dedicados criados após 30 de outubro de 2022 podem transmitir a indicação de nome do servidor (SNI) para serviços de back-end durante o handshake TLS. ● Caminho O caminho de solicitação (URI) do serviço de back-end. Certifique-se de que todos os parâmetros no caminho estejam entre chaves ({}). Por exemplo, **/getUserInfo/*{userId}***. Se o caminho contiver uma variável de ambiente, coloque a variável de ambiente em sinais numéricos (#), por exemplo, **/#path#**. Você pode usar várias variáveis de ambiente, por exemplo, **/#path##request#**.

Parâmetro	Descrição
Host Header (if applicable)	**Defina esse parâmetro somente se um canal de balanceamento de carga for usado.** Defina um cabeçalho de host para as solicitações a serem enviadas aos servidores de nuvem associados ao canal de balanceamento de carga. Por padrão, o cabeçalho do host original em cada solicitação é usado.
Timeout (ms)	Tempo limite de solicitação de back-end. Se ocorrer um erro de tempo limite de back-end durante a depuração da API, aumente o tempo limite para localizar o motivo. **NOTA** Modifique o tempo limite máximo fazendo referência a **Configuração de parâmetros**. O intervalo de valores é de 1 ms a 600.000 ms.
Retries	O valor desse parâmetro não pode exceder o número de serviços de back-end no canal de balanceamento de carga.
Two-Way Authentication	Determine se deve usar o certificado configurado usando **backend_client_certificate** para autenticação de cliente. Se ativar esta opção, certifique-se de que configurou um certificado na página **Parameters** do gateway.
Backend Authentication	Determine se seu serviço de back-end precisa autenticar solicitações de API. Se você habilitar essa opção, selecione um autorizador personalizado para autenticação de back-end. **Autorizadores personalizados** são funções criadas no FunctionGraph para implementar uma lógica de autenticação ou invocar um serviço de autenticação. **NOTA** A autenticação de back-end depende do FunctionGraph e só está disponível em determinadas regiões.

Tabela 3-12 Parâmetros para definir um serviço de back-end do FunctionGraph

Parâmetro	Descrição
Function Name	Exibido automaticamente quando você seleciona uma função.
Function URN	Identificador da função. Clique em **Select** para especificar uma função.
Version/Alias	Selecione uma versão de função ou alias. Para obter detalhes, consulte as seções "Gerenciamento de versões" e "Gerenciamento de aliases" no *Guia de usuário do FunctionGraph*.

Parâmetro	Descrição
Invocation Mode	● **Synchronous**: ao receber uma solicitação de invocação, o FunctionGraph processa imediatamente a solicitação e retorna um resultado. O cliente fecha a conexão uma vez que recebeu uma resposta do back-end. ● **Asynchronous**: os resultados de invocação de função de solicitações de clientes não importam para os clientes. Quando recebe uma solicitação, o FunctionGraph a enfileira, retorna uma resposta e processa uma a uma no estado ocioso.
Timeout (ms)	Tempo limite de solicitação de back-end. Para mais detalhes, consulte **Tabela 3-11**.
Backend Authentication	Para obter detalhes, consulte a descrição sobre autenticação de back-end em **Tabela 3-11**.

Tabela 3-13 Parâmetros para definição de um serviço de back-end Mock

Parâmetro	Descrição
Status Code	Este parâmetro só está disponível depois de actualizar o componente Shubao.
Response	Você pode usar o Mock para desenvolvimento, depuração e verificação de APIs. Ele permite que o APIG retorne uma resposta sem enviar a solicitação para o back-end. Isso é útil se você precisar testar APIs quando o back-end não estiver disponível.
Backend Authentication	Para obter detalhes, consulte a descrição sobre autenticação de back-end em **Tabela 3-11**.
Header Parameters	Cabeçalhos de resposta da API. Clique em **Add Header** e insira o nome do parâmetro, o valor e a descrição.

NOTA

- As APIs cujos URLs contenham variáveis não podem ser depuradas na página depuração da API.
- Para variáveis definidas em URLs de APIs, variáveis de ambiente correspondentes e seus valores devem ser configurados. Caso contrário, as APIs não podem ser publicadas porque não haverá valores que possam ser atribuídos às variáveis.
- O nome da variável faz distinção entre maiúsculas e minúsculas.

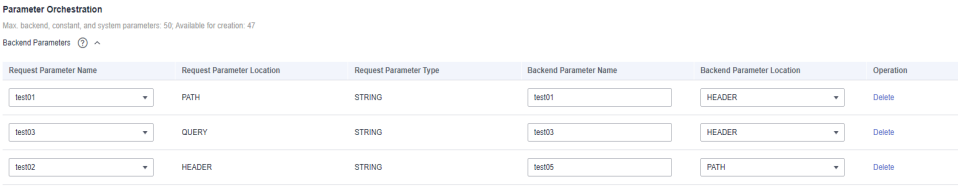
Passo 2 (Opcional) Configure parâmetros de back-end para mapeá-los para os parâmetros de solicitação definidos nos locais correspondentes. Se nenhum parâmetro de solicitação estiver definido em **5.3**, pule esta etapa.

1. Na área **Backend Parameters**, adicione parâmetros de uma das seguintes maneiras:

- Clique em **Import Request Parameter** para sincronizar todos os parâmetros de solicitação definidos.
- Clique em **Add Backend Parameter Mapping** para adicionar um parâmetro de back-end.

2. Modifique os mapeamentos (consulte **Figura 3-2**) com base nos parâmetros e em suas localizações nas solicitações de back-end.

Figura 3-2 Configurar parâmetros de back-end



a. Se a localização do parâmetro for definido como **PATH**, o nome do parâmetro deverá ser o mesmo definido no caminho de solicitação do back-end.

b. O nome e o local de um parâmetro de solicitação podem ser diferentes daqueles do parâmetro de back-end mapeado.

NOTA

- O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**.
- O nome do parâmetro não pode ser **x-stage**.
- Se você definir a localização do parâmetro como **HEADER**, verifique se o nome do parâmetro não começa com um sublinhado (_).

c. Na figura anterior, os parâmetros **test01** e **test03** estão localizados nas posições de caminho e consulta das solicitações da API e seus valores serão recebidos no cabeçalho das solicitações de back-end. O **test02** está localizado no cabeçalho das solicitações da API, e seu valor será recebido através do **test05** no caminho das solicitações de back-end.

Suponha que **test01** é **aaa**, **test02** é **bbb** e **test03** é **ccc**.

A solicitação da API é a seguinte:

```
curl -ik -H 'test02:bbb' -X GET https://example.com/v1.0/aaa?test03=ccc
```

Solicitação de back-end:

```
curl -ik -H 'test01:aaa' -H 'test03:ccc' -X GET https://example.com/
v1.0/bbb
```

Passo 3 (Opcional) Configure parâmetros constantes para o back-end padrão para receber constantes que são invisíveis para os chamadores da API. Ao enviar uma solicitação para o serviço de back-end, o APIG adiciona esses parâmetros aos locais especificados na solicitação e, em seguida, envia a solicitação para o serviço de back-end.

Na área **Constant Parameters**, clique em **Add Constant Parameter**.

Tabela 3-14 Configuração de parâmetro constante

Parâmetro	Descrição
Constant Parameter Name	Se **Parameter Location** for definido como **PATH**, o nome do parâmetro deve ser o mesmo que no **Path**. **NOTA** ● O nome do parâmetro não faz distinção entre maiúsculas e minúsculas. Não pode ser **x-stage** ou começar com **x-apig-** ou **x-sdk-** ● Se **Parameter Location** for definido como **HEADER**, o nome do parâmetro não diferencia maiúsculas de minúsculas e não pode começar com um sublinhado (_).
Parameter Location	Especifique o local do parâmetro constante nas solicitações de serviço de back-end. As opções incluem **PATH**, **HEADER** e **QUERY**.
Parameter Value	Valor do parâmetro constante.
Description	Descrição sobre o parâmetro constante.

NOTA

- O APIG envia solicitações contendo parâmetros constantes para um serviço de back-end após a codificação percentual de valores de parâmetros especiais. Certifique-se de que o serviço de back-end ofereça suporte à codificação de porcentagem. Por exemplo, o valor do parâmetro **[api]** torna-se **%5Bapi%5D** após a codificação por cento.
- Para valores de parâmetros de caminho, APIG percentual codifica os seguintes caracteres: códigos ASCII 0-31 e 127-255, espaços e outros characters especiais ?></%#"[\]^` {|}
- Para valores de cadeias de consulta, APIG percentual codifica os seguintes caracteres: códigos ASCII 0–31 e 127–255, espaços e outros caracteres especiais >=<+&%#"[\]^` {|}

Passo 4 (Opcional) Configure os parâmetros do sistema para que o back-end padrão receba parâmetros de gateway padrão, parâmetros de autenticação de front-end e parâmetros de autenticação de back-end. Ao enviar uma solicitação para o serviço de back-end, o APIG adiciona esses parâmetros aos locais especificados na solicitação e, em seguida, envia a solicitação para o serviço de back-end.

1. Na área **System Parameters**, clique em **Add System Parameter**.

Tabela 3-15 Configuração do parâmetro do sistema

Parâmetro	Descrição
System Parameter Type	Opções: - **Default gateway parameter**: parâmetros suportados pelo APIG. - **Frontend authentication parameter**: parâmetros a serem exibidos no resultado de autenticação personalizada do front-end. Essa opção estará disponível somente se você tiver definido o **Authentication Mode** como **Custom** em **Configurar configurações de front-end**. - **Backend authentication parameter**: parâmetros a serem exibidos no resultado de autenticação personalizada do back-end. Esta opção só está disponível se tiver ativado a autenticação de back-end no **Configurar configurações de back-end**.

System Parameter Name	Nome do parâmetro do sistema.
	- Se **System Parameter Type** for **Default gateway parameter**, selecione qualquer um dos seguintes parâmetros.
	  ■ **sourceIp**: endereço IP de origem de um chamador da API
	  ■ **stage**: ambiente no qual a API é chamada
	  ■ **apiId**: ID da API
	  ■ **appId**: ID da aplicação que chama a API
	  ■ **requestId**: ID da solicitação gerada quando a API é chamada
	  ■ **serverAddr**: endereço IP do servidor de gateway
	  ■ **serverName**: nome do servidor de gateway
	  ■ **handleTime**: tempo de processamento da solicitação da API
	  ■ **providerAppId**: ID da credencial do provedor da API
	  ■ **apiName**: nome da API. Esse parâmetro fica disponível somente após a publicação da API.
	  ■ **appName**: nome da credencial usada para chamar a API
	- Se **System Parameter Type** estiver **Frontend authentication parameter** ou **Backend authentication parameter**, insira um parâmetro que tenha sido definido para resultados de autenticação personalizados.
	Para obter detalhes sobre como criar uma função de autorizador personalizada e obter parâmetros de resultado, consulte **Guia de desenvolvedor**.

Parâmetro	Descrição
Backend Parameter Name	Nome de um parâmetro de back-end para mapear o parâmetro do sistema. **NOTA** – O nome do parâmetro não faz distinção entre maiúsculas e minúsculas. Não pode ser **x-stage** ou começar com **x-apig-** ou **x-sdk-** – Se **Parameter Location** for definido como **HEADER**, o nome do parâmetro não diferencia maiúsculas de minúsculas e não pode começar com um sublinhado (_).
Backend Parameter Location	Especifique o local do parâmetro de back-end nas solicitações de serviço de back-end. As opções incluem **PATH**, **HEADER** e **QUERY**.
Description	Descrição sobre o parâmetro do sistema.

Passo 5 (Opcional) Adicione uma política de back-end.

Você pode adicionar políticas de back-end para encaminhar solicitações para diferentes serviços de back-end.

1. Clique em  para adicionar uma política de back-end.
2. Definir parâmetros de política descritos em **Tabela 3-16**. Para obter detalhes sobre outros parâmetros, consulte **Tabela 3-11**, **Tabela 3-12** e **Tabela 3-13**.

Tabela 3-16 Parâmetros de política de back-end

Parâmetro	Descrição
Name	O nome da política de back-end.
Effective Mode	– **Any condition met**: a política de back-end entra em vigor se alguma das condições da política tiver sido cumprida. – **All conditions met**: a política de back-end entra em vigor somente quando todas as condições da política forem atendidas.
Policy Conditions	Condições que devem ser atendidas para que a política de back-end entre em vigor. Estabeleça condições referindo-se a **Tabela 3-17**.

Tabela 3-17 Configuração da condição de política

Parâmetro	Descrição
Source	- Endereço IP de origem: endereço IP a partir do qual a API é chamada - Parâmetro de solicitação: um parâmetro de solicitação definido para a API - **Cookie**: cookies de uma solicitação de API - Parâmetro do sistema: um parâmetro do sistema que define o tempo de execução do sistema para a API **AVISO** – Os parâmetros de solicitação (por exemplo, cabeçalhos) definidos como condições de política já devem ter sido definidos para a API. – Se **System parameter** não for exibido, entre em contato com o suporte técnico para atualizar o gateway.
Parameter Name	- Ao definir o **Source** como **Request parameter**, selecione um parâmetro de solicitação. - Ao definir o **Source** para **System parameter**, selecione um parâmetro do sistema. ■ **reqPath**: URI de solicitação, por exemplo, **/a/b/c**. ■ **reqMethod**: método de solicitação, por exemplo, **GET**. - Ao definir **Source** como **Cookie**, insira o nome de um parâmetro de cookie.
Parameter Location	A localização do parâmetro é exibida somente se você definir **Source** para **Request parameter**.
Condition Type	Este parâmetro só é necessário se você definir o **Source** para **Request parameter**, **System parameter** ou **Cookie**. - **Equal**: o parâmetro de solicitação deve ser igual ao valor especificado. - **Enumerated**: o parâmetro de solicitação deve ser igual a qualquer um dos valores enumerados. - **Matching**: o parâmetro de solicitação deve ser igual a qualquer valor da expressão regular. **NOTA** Ao definir o **Source** para **System parameter** e selecionar um parâmetro chamado **reqMethod**, você pode definir o tipo de condição apenas como **Equal** ou **Enumerated**.

Parâmetro	Descrição
Condition Value	- Se **Condition Type** estiver **Equal**, insira um valor. - Se **Condition Type** estiver **Enumerated**, insira vários valores e separe-os com vírgulas (,). - Se **Condition Type** for **Matching**, insira um intervalo de valores, por exemplo, **[0-5]**. - Se **Source** for **Source IP address**, digite um ou mais endereços IP e separe-os com vírgulas (,).

Passo 6 Definição de respostas.

Na área **Responses**, defina as respostas de exemplo.

Tabela 3-18 Definição de respostas

Parâmetro	Descrição
Example Success Response	A resposta a ser retornada quando a API é chamada com sucesso.
Example Failure Response	A resposta a ser retornada quando a API não é chamada.

Passo 7 Clique em **Finish**. Você pode ver os detalhes da API na página **APIs** exibida.

----Fim

(Opcional) Criação de uma política

Você pode criar políticas para a API depois de publicá-la.

Passo 1 Na página **APIs**, clique em **Create Policy**.

Passo 2 Selecione um tipo de política e defina parâmetros.

- Selecionar política existente
- Criar nova política (consulte **Criação de uma política**)

Passo 3 Clique em **OK**.

----Fim

Perguntas frequentes sobre a criação de APIs

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

Como escolher um modo de autenticação?

Quais são as possíveis causas se um serviço de back-end falhar ao ser chamado ou se a chamada expirar?

Por que estar vendo a mensagem "Nenhum back-end disponível"?

Operações de acompanhamento

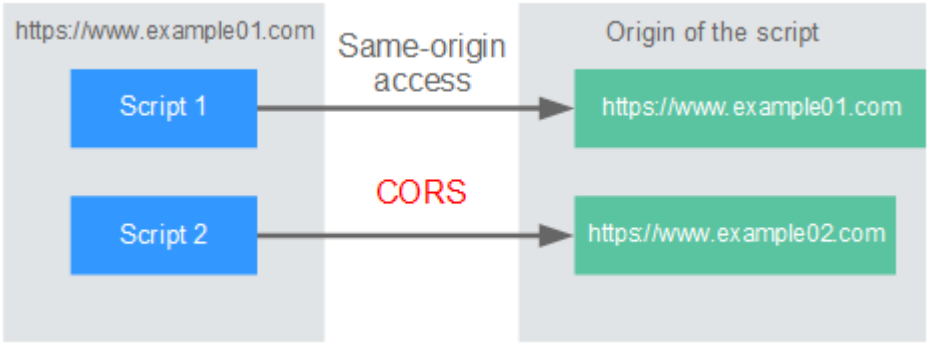
Depois de criar uma API, verifique-a seguindo o procedimento em **Depuração de uma API**.

3.7 CORS

O que é o CORS?

Por motivos de segurança, os navegadores restringem as solicitações entre origens iniciadas a partir de scripts. Isso significa que uma aplicação Web só pode solicitar recursos de sua origem. O mecanismo CORS permite que os navegadores enviem XMLHttpRequest para servidores em outros domínios e solicitem acesso aos recursos lá.

Figura 3-3 Fluxo de processo do mecanismo CORS



Existem dois tipos de solicitações CORS:

- **Solicitações simples**

  As solicitações simples devem atender às seguintes condições:

  a. O método de solicitação é HEAD, GET ou POST.

  b. O cabeçalho da solicitação contém apenas os seguintes campos:

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

  No cabeçalho de uma solicitação simples, os navegadores adicionam automaticamente o campo **Origin** para especificar a origem (incluindo o protocolo, o domínio e a porta) da solicitação. Depois de receber tal solicitação, o servidor de destino determina se a solicitação é segura e pode ser aceita com base na origem. Se o servidor enviar uma resposta contendo o campo **Access-Control-Allow-Origin**, o servidor aceitará a solicitação.

- **Solicitações não tão simples**

  Solicitações que não atendem às condições para solicitações simples são solicitações não tão simples.

  Antes de enviar uma solicitação não tão simples, os navegadores enviam uma solicitação de simulação HTTP ao servidor de destino para confirmar se a origem da página da Web

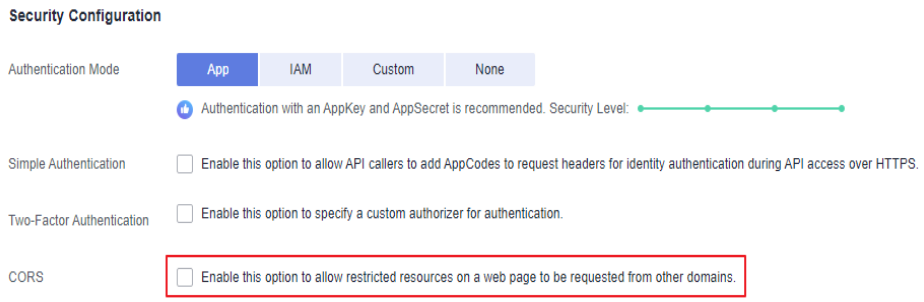
está na lista de origem permitida e para confirmar quais métodos de solicitação HTTP e campos de cabeçalho podem ser usados. Se a solicitação de simulação for bem-sucedida, os navegadores enviam solicitações simples para o servidor.

Configurar o CORS

O CORS está desativado por padrão. Para habilitar o CORS para uma API, execute as operações descritas nesta seção. Para personalizar cabeçalhos de solicitação, métodos de solicitação e origens permitidos para acesso entre domínios, crie uma política de plug-in CORS referindo-se a **CORS**.

- **Solicitações CORS simples**

  Ao criar uma API, habilite o CORS na área **Security Configuration** da página **Create API**. Para obter mais informações, consulte **Solicitação simples**.



- **Solicitações CORS não tão simples**

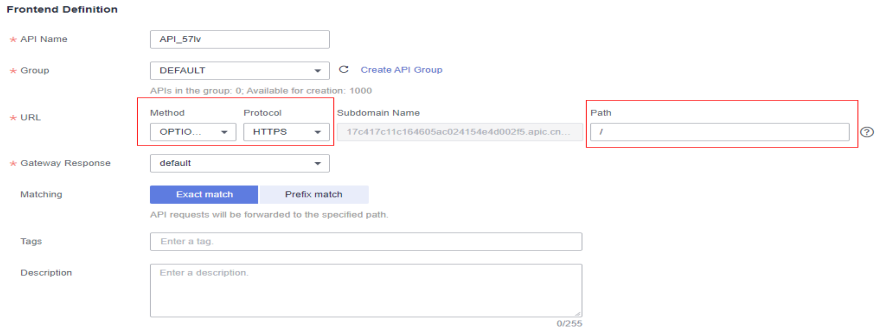
AVISO

Se sua API receber solicitações não tão simples, **crie outra API que será acessada usando o método OPTIONS** no mesmo grupo da API de destino para receber solicitações de simulação.

Siga este procedimento para definir a API de solicitação de simulação. Para obter mais informações, consulte **Solicitações não tão simples**.

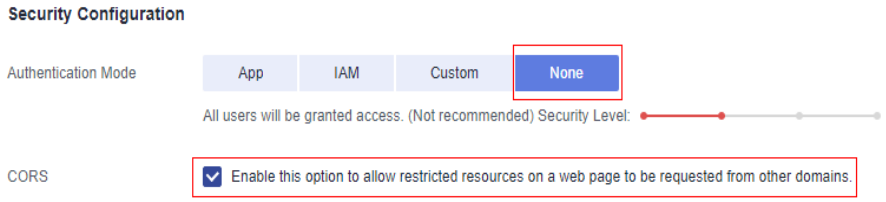
a. Na área **Frontend Definition**, defina os seguintes parâmetros:
   - **Method**: selecione **OPTIONS**.
   - **Protocol**: o mesmo protocolo usado pela API com o CORS ativado.
   - **Path**: insira uma barra (/).

Figura 3-4 Definição da solicitação da API



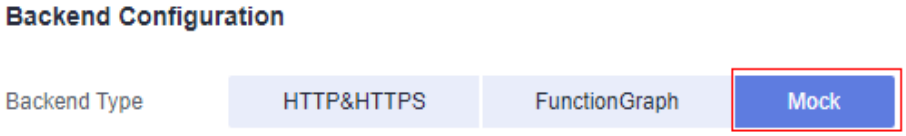
b. Na área **Security Configuration**, selecione **None** e habilite o **CORS**.

Figura 3-5 Nenhuma autenticação



c. Selecione o tipo de back-end **Mock**.

Figura 3-6 Serviço de back-end Mock



Solicitação simples

Ao criar uma API que receberá solicitações simples, **ative o CORS** para a API.

Cenário 1: se o CORS estiver habilitado e a resposta do back-end não contiver um cabeçalho CORS, o APIG tratará solicitações de qualquer domínio e retornará o cabeçalho **Access-Control-Allow-Origin**. Por exemplo:

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origin:

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

Origin: este campo é necessário para especificar a origem (**http://www.cors.com** neste exemplo) da solicitação. O APIG e o serviço de back-end determinam, com base na origem, se a solicitação é segura e pode ser aceita.

Resposta enviada pelo serviço de back-end:

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

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

Resposta enviada pelo APIG:

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

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


Access-Control-Allow-Origin: este campo é obrigatório. O asterisco (*) significa que o APIG lida com solicitações enviadas de qualquer domínio.

Cenário 2: se o CORS estiver habilitado e a resposta do back-end contiver um cabeçalho CORS, o cabeçalho substituirá o adicionado pelo APIG. As seguintes mensagens são usadas como exemplos:

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origin:

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

Origin: este campo é necessário para especificar a origem (**http://www.cors.com** neste exemplo) da solicitação. O APIG e o serviço de back-end determinam, com base na origem, se a solicitação é segura e pode ser aceita.

Resposta enviada pelo serviço de back-end:

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

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

Access-Control-Allow-Origin: indica que o serviço de back-end aceita solicitações enviadas do **http://www.cors.com**.

Resposta enviada pelo APIG:

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

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

O cabeçalho CORS na resposta de back-end substitui o da resposta do APIG.

Solicitações não tão simples

Ao criar uma API que receberá solicitações não tão simples, habilite o CORS para a API seguindo as instruções em **Configurar o CORS** e crie outra API que será acessada usando o método OPTIONS.

> **NOTA**
>
> Se você usar a política de plug-in CORS para uma API, não precisará criar outra API que use o método OPTIONS.

Os parâmetros de solicitação de uma API acessada usando o método OPTIONS devem ser definidos da seguinte forma:

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

- **Security Authentication**: selecione **None**. Nenhuma autenticação é necessária para solicitações recebidas pela nova API, independentemente do modo de autenticação de segurança selecionado.
- **Protocol**: o mesmo protocolo usado pela API com o CORS ativado.
- **Path**: insira uma barra (/) ou selecione o caminho que foi definido ou corresponda à API com CORS ativado.
- **Method**: selecione **OPTIONS**.
- **CORS**: ative esta opção.

A seguir estão exemplos de solicitações e respostas enviadas para ou de um back-end mock.

Solicitação enviada de um navegador para uma API que é acessada usando o método OPTIONS:

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

- **Origin**: esse campo é necessário para especificar a origem da qual a solicitação foi enviada.
- **Access-Control-Request-Method**: este campo é necessário para especificar os métodos HTTP a serem usados pelas solicitações simples subsequentes.
- **Access-Control-Request-Headers**: esse campo é opcional e usado para especificar os campos de cabeçalho adicionais nas solicitações simples subsequentes.

Resposta enviada pelo back-end: nenhuma

Resposta enviada pelo APIG:

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

- **Access-Control-Allow-Origin**: este campo é obrigatório. O asterisco (*) significa que o APIG lida com solicitações enviadas de qualquer domínio.
- **Access-Control-Allow-Headers**: este campo é obrigatório se estiver contido na solicitação. Indica todos os campos de cabeçalho que podem ser usados durante o acesso entre origens.
- **Access-Control-Expose-Headers**: estes são os campos de cabeçalho de resposta que podem ser visualizados durante o acesso entre regiões.
- **Access-Control-Allow-Methods**: este campo é necessário para especificar quais métodos de solicitação HTTP o APIG suporta.

- **Access-Control-Max-Age**: este campo é opcional e usado para especificar o período de tempo (em segundos) durante o qual o resultado da comprovação permanece válido. Não serão enviadas mais solicitações de simulação dentro do período especificado.

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origin:

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

Resposta enviada pelo back-end:

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

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

Resposta enviada pelo APIG:

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

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

3.8 Depuração de uma API

Depois de criar uma API, depure-a no console do APIG definindo cabeçalhos HTTP e corpo para verificar se a API está sendo executada normalmente.

NOTA

- As APIs com caminhos de solicitação de back-end contendo variáveis não podem ser depuradas.
- Se uma API tiver sido vinculada a uma política de limitação de solicitações, a política não funcionará durante a depuração da API.

Pré-requisitos

Você configurou o serviço de back-end da API.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Na página da guia **APIs**, selecione a API de destino e clique em **Debug**.

Passo 6 Defina parâmetros de solicitação e clique em **Debug**.

Passo 7 A caixa no canto inferior direito exibe a resposta da solicitação da API.

- Se a depuração for bem-sucedida, o código de status HTTP **200** e os detalhes da resposta serão exibidos.
- Se a solicitação não for enviada, um código de status HTTP **4xx** ou **5xx** será exibido. Para mais detalhes, consulte **Códigos de erro**.

Passo 8 Você pode enviar mais solicitações com diferentes parâmetros e valores para verificar a API.

----Fim

Operações de acompanhamento

Depois que a API for depurada com sucesso, **publique** a API em um ambiente específico para que ela possa ser chamada pelos usuários. Para garantir a segurança, **crie políticas** para a API.

3.9 Autorização de aplicações a chamar uma API

As APIs que usam a autenticação de aplicações só podem ser chamadas por credenciais que foram autorizadas a chamá-las.

AVISO

- Você pode autorizar credenciais apenas para chamar APIs que usam autenticação de aplicação.
- Uma credencial pode ser autorizada a acessar um máximo de 1000 APIs.

Pré-requisitos

- Você publicou uma API.
- Você criou um ambiente.
- Você criou uma credencial.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Na página de guia **APIs**, selecione a API de destino e escolha **More** > **Authorize Credentials**.

Passo 6 Clique em **Select Credentials**.

Passo 7 Selecione um ambiente, pesquise e selecione as credenciais desejadas e clique em **OK**. As credenciais autorizadas são exibidas na página **Authorize Credentials**.

Para cancelar a autorização de uma credencial, clique em **Cancel Authorization** na coluna **Operation** que contém a credencial.

----Fim

Operações de acompanhamento

Depois de autorizar uma credencial para uma API, a API pode ser chamada pela credencial usando SDKs de diferentes linguagens de programação.

3.10 Publicação de uma API

As APIs só podem ser chamadas depois de terem sido publicadas em um ambiente. Você pode publicar APIs em diferentes ambientes. O APIG permite que você visualize o histórico de publicações (como a versão, a descrição, a hora e o ambiente) de cada API e suporta a reversão de APIs para diferentes versões históricas.

NOTA

- Se você modificar uma API publicada, deverá publicá-la novamente para que as modificações entrem em vigor no ambiente em que a API foi publicada.
- Um máximo de 10 registros de publicação de uma API são retidos em um ambiente.

Pré-requisitos

Você criou um ambiente.

Publicação de uma API

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Na página de guia **APIs**, selecione a API de destino e clique em **Publish**.

Passo 6 Selecione o ambiente onde a API será publicada e insira uma descrição.

NOTA

- Se a API já tiver sido publicada no ambiente, publicá-la novamente substituirá sua definição nesse ambiente.
- Se não houver um ambiente que atenda aos seus requisitos, crie um novo.

Passo 7 Clique em **OK**.

Você pode remover APIs dos ambientes onde elas foram publicadas. Essa operação fará com que as APIs fiquem inacessíveis nos ambientes. Certifique-se de que notificou os usuários antes desta operação. Para remover uma API, clique em **Take Offline**.

----Fim

Visualizar o histórico de publicações

Passo 1 Na página **APIs**, selecione a API de destino.

Passo 2 Escolha **More** > **View Publishing Records**.

Passo 3 Clique em **View Details** na coluna **Operation** de uma versão.

A caixa de diálogo **View Details** exibe as informações básicas, informações de solicitação de front-end e back-end, parâmetros de entrada e constantes, mapeamentos de parâmetros e respostas de exemplo da API.

Passo 4 Para reverter a API para uma versão histórica, clique em **Switch Version** na linha que contém a versão de destino e clique em **Yes**.

Se a "versão atual" for exibida ao lado da versão de destino, a reversão foi bem-sucedida.

Quando a API é chamada, a configuração da versão atual é usada em vez da configuração salva anteriormente.

Por exemplo, uma API foi publicada no ambiente RELEASE em 1º de agosto de 2018. Em 20 de agosto de 2018, a API foi publicada no mesmo ambiente após modificação. Se a versão publicada em 1º de agosto for definida como a versão atual, a configuração dessa versão será usada quando a API for chamada.

----Fim

Perguntas frequentes sobre a publicação de APIs

Precisar publicar uma API novamente após a modificação?

Por que as APIs publicadas em um ambiente não RELEASE não podem ser acessadas?

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

3.11 Deixar uma API off-line

Você pode remover APIs que não são necessárias dos ambientes em que as APIs foram publicadas.

AVISO

Essa operação fará com que as APIs fiquem inacessíveis nos ambientes. Certifique-se de que notificou os usuários antes desta operação.

Pré-requisitos

- Você criou um grupo de API e uma API.
- Você publicou a API.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Groups**.

Passo 4 Clique no nome do grupo de API de destino.

- Para colocar uma API off-line, selecione a API e clique em **Take Offline** no canto superior direito.
- Para colocar várias APIs (≤ 1000) off-line, clique em **Batch**, selecione as APIs e clique no ícone Colocar off-line.

Passo 5 Selecione o ambiente do qual você deseja colocar a API off-line e clique em **Yes**.

----Fim

Operações de acompanhamento

Depois de colocar uma API off-line, exclua-a para liberar recursos.

3.12 Importação de APIs

O APIG permite importar APIs do Swagger 2.0 para grupos de APIs existentes ou novos. Swagger é uma ferramenta de código aberto construída com base nas especificações OpenAPI para projetar, construir, gravar e usar APIs REST.

Você pode importar APIs individualmente ou em lotes, dependendo do número de APIs contidas no seu arquivo Swagger.

Pré-requisitos

- O arquivo Swagger a ser importado está disponível e contém definições de API estendidas. Para obter mais informações, consulte **Definição estendida**.
- Seu grupo de API e cotas de API são suficientes.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **APIs**.

Passo 4 Clique em **Import APIs**. Para mais detalhes, consulte **Importar um arquivo de design de API**.

----Fim

Operações de acompanhamento

Publique as APIs importadas em um ambiente para que elas possam ser chamadas pelos usuários.

3.13 Exportação de APIs

Você pode exportar APIs uma a uma ou em lotes como arquivos JSON ou YAML.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Clique em **Export** e defina os parâmetros de exportação.

Tabela 3-19 Parâmetros para exportação de APIs

Parâmetro	Descrição
API Group	Selecione o grupo de quais APIs serão exportadas.
Environment	Selecione o ambiente onde as APIs a serem exportadas foram publicadas.
API	Por padrão, todas as APIs do grupo que foram publicadas no ambiente selecionado são exportadas. Para exportar apenas APIs específicas, clique em **Select APIs** e especifique as APIs que deseja exportar.
API Definition	● **Basic**: a definição básica de uma API é composta pelas definições de solicitação e resposta. Não inclui a definição de back-end. A definição de solicitação inclui campos Swagger padrão e estendido. ● **Full**: a definição completa de uma API é composta pelas definições de solicitação, back-end e resposta. ● **Extended**: a definição estendida de uma API é composta pelas definições de solicitação, back-end e resposta, bem como pela política de limitação de solicitações, política de controle de acesso e outras configurações da API.
Format	Exporte APIs em formato **JSON** ou **YAML**.
Version	Defina a versão das APIs a serem exportadas. Se você não especificar uma versão, a versão será definida como a data e a hora atuais.

Passo 6 Clique em **Export**. O resultado da exportação é exibido à direita da página e o arquivo API é baixado automaticamente.

----Fim

3.14 Visualização de APIs

A página **APIs** exibe todas as APIs do gateway atual, incluindo o URL, o ambiente em execução e o modo de autenticação.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 Modifique, publique e depure APIs do gateway.

Passo 4 No painel de navegação, escolha **API Management** > **APIs**.

Passo 5 Clique em um nome de API para ir para a página de detalhes do grupo ao qual a API pertence. Para obter detalhes sobre como criar uma API, gerenciar nomes de domínio e definir variáveis de ambiente, consulte as seções anteriores.

----Fim

3.15 HTTP 2.0

O APIG suporta HTTP/2, que é uma grande revisão do HTTP e foi originalmente chamado HTTP 2.0. Ele fornece codificação binária, multiplexação de solicitações em uma única conexão e compactação de cabeçalho de solicitações, melhorando o desempenho de transmissão e a taxa de transferência com menor latência.

NOTA

- O HTTP 2.0 depende fortemente da estabilidade da rede. Para usar o HTTP 2.0, certifique-se de que sua rede seja estável e que seu cliente ofereça suporte a esse protocolo.
- Somente gateways dedicados criados após 22 de junho de 2022 suportam HTTP 2.0. Para usar esse protocolo, entre em contato com o suporte técnico.

- Codificação binária

  Ao contrário do HTTP 1.x, onde os dados são transmitidos em formato de texto, os dados no HTTP 2.0 são divididos em mensagens e quadros para codificação binária. Comparado com a análise de cadeia (texto), a análise binária é mais fácil e menos propensa a erros e oferece maior desempenho de transmissão.

- Multiplexação

  Com a codificação binária, o HTTP 2.0 não depende mais de múltiplas conexões para processar e enviar solicitações e respostas simultaneamente.

  Para o mesmo nome de domínio, todas as solicitações são concluídas em uma única conexão, e cada conexão pode processar qualquer número de mensagens. Uma mensagem consiste em um ou mais quadros, que podem ser enviados fora de ordem e, finalmente, recombinadas com base no ID do fluxo no cabeçalho de cada quadro. Isso encurta a latência e melhora a eficiência.

- Compressão de cabeçalho

  O HTTP 2.0 usa um codificador para reduzir o tamanho dos cabeçalhos a serem transmitidos. Tanto o cliente quanto o servidor armazenam uma tabela de campo de

cabeçalho para evitar transmitir os mesmos cabeçalhos repetidamente, alcançando alta taxa de transferência.

4 Gerenciamento de políticas de API

4.1 Criação de uma política

O APIG fornece políticas flexíveis de controle de API.

Diretrizes

- Uma API pode ser vinculada a apenas uma política do mesmo tipo.
- As políticas são independentes das APIs. Uma política entra em vigor para uma API somente depois que elas são vinculadas uma à outra. Ao vincular uma política a uma API, você deve especificar um ambiente no qual a API foi publicada. A política entra em vigor para a API somente no ambiente especificado.
- Depois de vincular uma política a uma API, desvincular a política da API ou atualizar a política, não é necessário publicar a API novamente.
- Colocar uma API off-line não afeta as políticas vinculadas a ela. As políticas ainda estão vinculadas à API se a API for publicada novamente.
- Políticas que foram vinculadas a APIs não podem ser excluídas.

Criação de uma política

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Policies**.

Passo 4 Na página de guia **Policies**, clique em **Create Policy**.

Passo 5 Clique no tipo de política desejado.

- **Políticas de plug-in**

  Defina as informações da política.

Tabela 4-1 Configuração de política

Parâmetro	Descrição
Name	Insira um nome de política que esteja em conformidade com regras específicas para facilitar a pesquisa.
Type	Tipo da política, que determina os recursos de extensão. - **CORS**: fornece os recursos de especificação de cabeçalhos de solicitação de simulação e cabeçalhos de resposta e criação automática de APIs de solicitação de simulação para acesso à API de origem cruzada. - **HTTP Response Header Management**: permite personalizar cabeçalhos de resposta HTTP que serão exibidos em uma resposta da API. - **Request Throttling 2.0**: limita o número de vezes que uma API pode ser chamada dentro de um período de tempo específico. A limitação baseada em parâmetro, básica e excluída é suportada. - **Kafka Log Push**: envia os logs de chamada da API para o Kafka para que você possa visualizar esses logs. - **Circuit Breaker**: protege seu serviço de back-end quando ocorre um problema de desempenho.
Description	Descrição sobre o plug-in.
Policy Content	Conteúdo do plug-in, que pode ser configurado em um formulário ou usando um script. O conteúdo do plug-in varia dependendo do tipo de plug-in: - **CORS** - **Gerenciamento de cabeçalho de resposta HTTP** - **Limitação de solicitação 2.0** - **Push de log de Kafka** - **Disjuntor**

- **Políticas tradicionais**

  O conteúdo da política varia dependendo do tipo de política:

  - **Limitação de solicitação**
  - **Controle de acesso**
  - **Chaves de assinatura**

Passo 6 Clique em **OK**.

Depois que a política for criada, execute as operações descritas em **Vinculação de uma política a APIs** para que a política entre em vigor para a API.

----Fim

Vinculação de uma política a APIs

Passo 1 Clique em um nome de política para ir para a página de detalhes da política.

Passo 2 Na área **APIs**, selecione um ambiente e clique em **Select APIs**.

Passo 3 Selecione um grupo de APIs e, em seguida, selecione APIs.

Passo 4 Clique em **OK**.

- Se uma API não precisar mais dessa política, clique em **Unbind** na linha que contém a API.
- Se houver várias APIs que não precisem mais dessa política, selecione essas APIs e clique em **Unbind** acima da lista de APIs. Você pode desvincular uma política de no máximo 1000 APIs por vez.

----Fim

4.2 CORS

Por motivos de segurança, o navegador restringe solicitações entre domínios de serem iniciadas a partir de um script de página. Nesse caso, a página pode acessar apenas os recursos do domínio atual. O CORS permite que o navegador envie XMLHttpRequest para o servidor em um domínio diferente. Para obter mais informações sobre CORS, consulte **CORS**.

O plug-in CORS fornece os recursos de especificação de cabeçalhos de solicitação de simulação e cabeçalhos de resposta e criação automática de APIs de solicitação de simulação para acesso à API entre origens.

Diretrizes de uso

- Você entendeu as **Diretrizes para o uso de plug-ins**.
- As APIs com o mesmo caminho de solicitação em um grupo de APIs só podem ser vinculadas à mesma política de plug-in CORS.
- Se você ativou o CORS para uma API e também vinculou o plug-in CORS à API, o plug-in CORS será usado.
- Não é possível vincular o plug-in CORS a APIs com o mesmo caminho de solicitação de outra API que use o método OPTIONS.
- Ao vincular uma política de plug-in a uma API (consulte **Vinculação de uma política a APIs**), verifique se o método de solicitação da API está incluído em **allow_methods**.

Parâmetros de configuração

Tabela 4-2 Parâmetros de configuração

Parâmetro	Descrição
Allowed Origins	Cabeçalho de resposta **Access-Control-Allow-Origin**, que especifica uma única origem, que diz aos navegadores para permitir que essa origem acesse uma API; ou então — para solicitações sem credenciais — o curinga "*", para dizer aos navegadores para permitir que qualquer origem acesse a API. Separe vários URIs usando vírgulas.
Allowed Methods	Cabeçalho de resposta **Access-Control-Allow-Methods**, que especifica os métodos HTTP permitidos ao acessar a API. Separe vários métodos usando vírgulas.
Allowed Headers	Cabeçalho de resposta **Access-Control-Allow-Headers**, que especifica os cabeçalhos de solicitação que podem ser usados ao fazer um XMLHttpRequest. Separe vários cabeçalhos usando vírgulas. Por padrão, os cabeçalhos de solicitação simples **Accept**, **Accept-Language**, **Content-Language** e **Content-Type** (somente se o valor for **application/x-www-form-urlencoded**, **multipart/form-data** ou **text/plain**) são transportados em solicitações. Você não precisa configurar esses cabeçalhos neste parâmetro.
Exposed Headers	Cabeçalho de resposta **Access-Control-Expose-Headers**, que especifica quais cabeçalhos de resposta podem ser contidos na resposta de XMLHttpRequest. Separe vários cabeçalhos usando vírgulas. Por padrão, os cabeçalhos básicos de resposta **Cache-Control**, **Content-Language**, **Content-Type**, **Expires**, **Last-Modified** e **Pragma** podem ser contidos na resposta. Você não precisa configurar esses cabeçalhos neste parâmetro.
Maximum Age	Cabeçalho de resposta **Access-Control-Max-Age**, que especifica por quantos segundos os resultados de uma solicitação de simulação podem ser armazenados em cache. Não serão enviadas mais solicitações de simulação dentro do período especificado.
Allowed Credentials	Cabeçalho de resposta **Access-Control-Allow-Credentials**, que especifica se solicitações XMLHttpRequest podem levar cookies.

Exemplo de script

```
{
  "allow_origin": "*",
  "allow_methods": "GET,POST,PUT",
  "allow_headers": "Content-Type,Accept,Accept-Ranges,Cache-Control",
  "expose_headers": "X-Request-Id,X-Apig-Latency",
```



```
  "max_age": 172800,
  "allow_credentials": true
}
```

4.3 Gerenciamento de cabeçalho de resposta HTTP

Cabeçalhos de resposta HTTP são parte da resposta retornada pelo APIG para um cliente que chama uma API. Você pode personalizar cabeçalhos de resposta HTTP que estarão contidos em uma resposta da API.

Diretrizes de uso

Você não pode modificar os cabeçalhos de resposta (incluindo **x-apig-*** e **x-request-id**) adicionados pelo APIG ou os cabeçalhos necessários para o CORS.

Parâmetros de configuração

Tabela 4-3 Parâmetros de configuração

Parâmetro	Descrição
Name	Nome do cabeçalho da resposta, que não faz distinção entre maiúsculas e minúsculas e deve ser exclusivo em um plug-in. Você pode adicionar um máximo de 10 cabeçalhos de resposta.
Value	Valor do cabeçalho da resposta. Esse parâmetro não tem efeito e pode ser deixado em branco se você definir **Action** para **Delete**.

Parâmetro	Descrição
Action	Operação de cabeçalho de resposta. Você pode substituir, anexar, excluir, ignorar ou adicionar cabeçalhos de resposta. **Override** ● O valor desse cabeçalho de resposta substituirá o valor do mesmo cabeçalho de resposta que existe em uma resposta da API. ● Se uma resposta da API contiver vários cabeçalhos de resposta com o mesmo nome, somente o valor desse cabeçalho de resposta será retornado. ● Se não houver um cabeçalho de resposta com o mesmo nome em uma resposta da API, o valor desse cabeçalho de resposta será retornado. **Append** ● Se uma resposta da API contiver o cabeçalho especificado, o valor definido aqui será adicionado, seguindo o valor existente. Os dois valores serão separados por vírgulas (,). ● Se uma resposta da API contiver vários cabeçalhos de resposta com o mesmo nome, os valores desses cabeçalhos serão retornados e separados com vírgulas (,), acrescentadas pelo valor desse cabeçalho de resposta. ● Se não houver um cabeçalho de resposta com o mesmo nome em uma resposta da API, o valor desse cabeçalho de resposta será retornado. **Delete** ● Esse cabeçalho de resposta será excluído se um cabeçalho de resposta com o mesmo nome existir em uma resposta da API. ● Se uma resposta da API contiver vários cabeçalhos de resposta com o mesmo nome, todos esses cabeçalhos de resposta serão excluídos. **Skip** ● Esse cabeçalho de resposta será ignorado se um cabeçalho de resposta com o mesmo nome existir em uma resposta da API. ● Se uma resposta da API contiver vários cabeçalhos de resposta com o mesmo nome, os valores de todos esses cabeçalhos de resposta serão retornados. ● Se não houver um cabeçalho de resposta com o mesmo nome em uma resposta da API, o valor desse cabeçalho de resposta será retornado. **Add** O valor desse cabeçalho de resposta será retornado em uma resposta da API, mesmo que a resposta contenha um cabeçalho de resposta com o mesmo nome.

Exemplo de script

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

4.4 Limitação de solicitação 2.0

Uma política de limitação de solicitação 2.0 limita o número de vezes que uma API pode ser chamada dentro de um período de tempo específico. A limitação baseada em parâmetro, básica e excluída é suportada.

- Limitação básica

  Limite as solicitações por API, usuário, aplicação ou endereço IP de origem. Essa função é equivalente a uma política de limitação de solicitações tradicional (consulte **Limitação de solicitação**), mas é incompatível com ela.
- Limitação baseada em parâmetros

  Solicitações de aceleração com base em cabeçalhos, parâmetro de caminho, método, cadeias de consulta ou parâmetros do sistema.
- Limitação excluída

  Solicitações de limitação com base em aplicações ou locatários específicos.

Diretrizes de uso

- Uma política tradicional de limitação de solicitações torna-se inválida se uma política 2.0 de limitação de solicitações estiver vinculada à mesma API que a tradicional.
- Você pode definir um máximo de 100 regras de limitação baseadas em parâmetros.
- O conteúdo da política não pode exceder os caracteres 65.535.

Descrição do parâmetro

Tabela 4-4 Descrição do parâmetro

Parâmetro	Descrição
Throttling	É recomendado a limitação de alto desempenho. ● **High precision**: melhor para cenários de baixa simultaneidade (o desempenho é afetado) ● **High performance**: melhor para cenários de concorrência média (o desempenho é menos afetado, com pequenos erros ocasionais) ● **Single node**: melhor para cenários de alta simultaneidade (limitação de solicitação dentro de cada nó; o desempenho é menos afetado, com pequenos erros ocasionais)
Policy Type	● API específica Monitore e controle as solicitações de uma única API. ● Compartilhamento de API Monitore e controle solicitações para todas as APIs vinculadas à política.
Period	Por quanto tempo você deseja limitar o número de chamadas de API. Este parâmetro pode ser usado em conjunto com os seguintes parâmetros: ● **Max. API Requests**: limite o número máximo de vezes que uma API pode ser chamada em um período específico. ● **Max. User Requests**: limite o número máximo de vezes que uma API pode ser chamada por um usuário dentro de um período específico. ● **Max. Credential Requests**: limite o número máximo de vezes que uma API pode ser chamada por uma credencial dentro de um período específico. ● **Max. IP Address Requests**: limite o número máximo de vezes que uma API pode ser chamada por um endereço IP dentro de um período específico.
Max. API Requests	O número máximo de vezes que cada API vinculada pode ser chamada dentro do período especificado. Este parâmetro deve ser utilizado em conjunto com o **Period**.

Parâmetro	Descrição
Max. User Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um usuário dentro do período especificado. Para APIs com autenticação do IAM, a limitação é baseada em um código de projeto; para APIs com autenticação de aplicação, a limitação é baseada em um código de conta. Para obter detalhes sobre o ID da conta e o ID do projeto, consulte a descrição sobre **Excluded Tenants** nesta tabela. ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**. ● Se houver muitos usuários na sua conta que acessam uma API, os limites de limitação de solicitações da API serão aplicados a todos esses usuários.
Max. Credential Requests	O número máximo de vezes que cada API vinculada pode ser chamada por uma credencial dentro do período especificado. Esse limite se aplica apenas a APIs acessadas por meio de autenticação de aplicação. ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Max. IP Address Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um endereço IP dentro do período especificado. ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Parameter-based Throttling	Habilitar ou desabilitar a limitação baseada em parâmetro. Depois que essa função é ativada, as solicitações de API são reduzidas com base nos parâmetros definidos.
Parameters	Defina parâmetros para correspondência de regras. ● **Parameter Location**: a localização de um parâmetro usado para correspondência de regras. – **path**: URI de solicitação da API. Este parâmetro é configurado por padrão. – **method**: método de solicitação da API. Este parâmetro é configurado por padrão. – **header**: a chave de um cabeçalho de solicitação. – **query**: a chave de uma cadeia de consulta. – **system**: um parâmetro do sistema. ● **Parameter Name**: o nome de um parâmetro que corresponde ao valor especificado em uma regra.

Parâmetro	Descrição
Rules	Defina regras de limitação. Uma regra consiste em condições, uma limitação de solicitações de API e um período. Para adicionar mais regras, clique em **Add Rule**. ● Condições Clique em  para definir expressões de condição. Para definir uma expressão, selecione um parâmetro e um operador e insira um valor. – =: igual a – **!=**: não igual a – **pattern**: expressão regular – **enum**: valores enumerados. Separe-os com vírgulas (,). ● Máx. solicitações de API O número máximo de vezes que uma API pode ser chamada em um período de tempo específico. ● Período Um período de tempo que será aplicado com o limite definido. Se este parâmetro não for especificado, será utilizado o período definido na área **Police Information**. Por exemplo, configure a limitação baseada em parâmetro da seguinte forma: adicione o parâmetro **Host** e especifique o local como **header**; adicione a condição **Host = www.abc.com**, e defina o limite de limitação como **10** e o período como 60s. Para APIs cujo parâmetro **Host** no cabeçalho da solicitação é igual a **www.abc.com**, elas não podem ser chamadas novamente uma vez chamadas 10 vezes em 60s.
Excluded Throttling	Ativar ou desativar a limitação excluída. Depois que essa função é ativada, os limites para locatários e aplicações excluídas substituem o **Max. User Requests** e **Max. App Requests** definidas na área **Basic Throttling**.
Excluded Tenants	**Tenant ID**: um ID de conta ou um ID de projeto. ● Especifique um ID de projeto para uma API que usa autenticação de aplicação. Para obter detalhes, consulte **Obtenção de um ID de projeto**. ● Especifique um ID de conta (não ID de usuário do IAM) para uma API que usa a autenticação do IAM. Para obter detalhes, consulte **Obtenção de um nome de conta e um ID de conta**. **Threshold**: o número máximo de vezes que um locatário específico pode acessar uma API dentro do período especificado. O limite não pode exceder o valor de **Max. API Requests** na área **Basic Throttling**.

Parâmetro	Descrição
Excluded Apps	Selecione uma aplicação e especifique o número máximo de vezes que a aplicação pode acessar uma API dentro do período especificado. O limite não pode exceder o valor de **Max. API Requests** na área **Basic Throttling**.

Exemplo de script

```
{
  "scope": "basic",
  "default_interval": 60,
  "default_time_unit": "second",
  "api_limit": 100,
  "app_limit": 50,
  "user_limit": 50,
  "ip_limit": 20,
  "specials": [
    {
      "type": "app",
      "policies": [
        {
          "key": "e9230d70c749408eb3d1e838850cdd23",
          "limit": 10
        }
      ]
    },
    {
      "type": "user",
      "policies": [
        {
          "key": "878f1b87f71c40a7a15db0998f358bb9",
          "limit": 10
        }
      ]
    }
  ],
  "algorithm": "counter",
  "parameters": [
    {
      "id": "3wuj354lpptv0toe0",
      "value": "reqPath",
      "type": "path",
      "name": "reqPath"
    },
    {
      "id": "53h7e7j11u38l3ocp",
      "value": "method",
      "type": "method",
      "name": "method"
    },
    {
      "id": "vv502bnb6g40td8u0",
      "value": "Host",
      "type": "header",
      "name": "Host"
    }
  ],
  "rules": [
    {
      "match_regex": "[\"Host\",\"==\",\"www.abc.com\"]",
      "rule_name": "u8mb",
      "time_unit": "second",
      "interval": 2,
      "limit": 5
```



```
    }
  ]
}
```

4.5 Push de log de Kafka

As políticas de push de log do Kafka enviam logs de chamadas de APIs abertas para o Kafka para análise.

Diretrizes de uso

- Um máximo de cinco políticas de push de log do Kafka podem ser criadas para um gateway.
- As APIs vinculadas a uma política de push de log do Kafka deteriorarão o desempenho em 30%.

Parâmetros de configuração

Tabela 4-5 Descrição do parâmetro

Parâmetro	Descrição
Informações sobre políticas	
Broker Address	Endereço de conexão do Kafka de destino. Separe vários endereços com vírgulas (,).
Topic	Tópico do Kafka alvo para reportar os logs.
Key	Partição do Kafka para armazenar logs como uma fila de mensagens ordenada. Se esse parâmetro for deixado em branco, os logs serão armazenados em partições diferentes.
Retry	Configuração para tentar novamente quando os logs falham ao serem enviados para o Kafka. ● **Retry Times**: o número de tentativas de repetição em caso de falha. Digite de 0 a 5. ● **Retry Interval**: o intervalo das tentativas de repetição em caso de falha. Digite de 1 a 10 segundos.
Configuração SASL	
Security Protocol	Protocolo usado para se conectar ao Kafka alvo. ● **PLAINTEXT**: protocolo de autenticação do usuário do ponto de acesso padrão ● **SASL_PLAINTEXT**: protocolo de autenticação de usuário SASL ● **SASL_SSL**: protocolo de autenticação de usuário SSL
Message Tx/Rx Mechanism	Mecanismo de transmissão e recebimento de mensagens do alvo Kafka. O valor padrão é **PLAIN**.

Parâmetro	Descrição
SASL Username	Este parâmetro só estará disponível se **Security Protocol** estiver definido como **SASL_PLAINTEXT** ou **SASL_SSL**. Nome de usuário usado para autenticação SASL ou SSL.
SASL Password	Este parâmetro só estará disponível se **Security Protocol** estiver definido como **SASL_PLAINTEXT** ou **SASL_SSL**. Senha de usuário usada para autenticação SASL ou SSL.
Confirm SASL Password	Este parâmetro só estará disponível se **Security Protocol** estiver definido como **SASL_PLAINTEXT** ou **SASL_SSL**. Digite a senha SASL novamente.
Certificate Content	Este parâmetro só está disponível se **Security Protocol** estiver definido como **SASL_SSL**. Certificado CA usado para autenticação SSL.
Configuração de metadados	
System Metadata	Campos do sistema que precisam ser incluídos em logs por push. Por padrão, o **start_time**, **request_id**, **client_ip**, **request_time**, **http_status**, **scheme**, **request_method**, **host**, **uri**, **upstream_addr**, **upstream_status**, **upstream_response_time**, **http_x_forwarded_for**, **http_user_agent** e **error_type** são transportados nos logs. Você também pode especificar outros campos do sistema que precisam ser incluídos.
Request Data	Informações de solicitação da API que precisam ser incluídas nos logs por push. ● **O log contém o cabeçalho da solicitação**: especifique um cabeçalho que precisa ser incluído. Separe vários cabeçalhos com vírgulas (,). O asterisco (*) pode ser usado como curinga. ● **O log contém o QueryString da solicitação**: especifique uma cadeia de consulta que precisa ser incluída. Separe várias cadeias de consulta com vírgulas (,). O asterisco (*) pode ser usado como curinga. ● **O log contém o corpo da solicitação**: se essa opção for selecionada, os logs conterão o corpo das solicitações da API.
Response Data	Informações de resposta da API que precisam ser incluídas nos logs enviados. ● **O log contém o cabeçalho de resposta**: especifique um cabeçalho que precisa ser incluído. Separe vários cabeçalhos com vírgulas (,). O asterisco (*) pode ser usado como curinga. ● **O log contém o corpo da resposta**: se essa opção for selecionada, os logs conterão o corpo das respostas de solicitação da API.

Parâmetro	Descrição
Customized Authentication	Informações de autenticação personalizadas que precisam ser incluídas nos logs empurrados. ● **Front-end**: digite um campo de resposta de autenticação front-end que precisa ser incluído. Separe vários campos por vírgulas (,). ● **Back-end**: digite um campo de resposta de autenticação de back-end que precisa ser incluído. Separe vários campos por vírgulas (,).

4.6 Disjuntor

As políticas de disjuntores protegem seus serviços de back-end quando ocorre um problema de desempenho. Se o serviço de back-end de uma API expirar por *N* vezes consecutivas ou se a latência for longa, o mecanismo de downgrade de uma política de disjuntores será acionado para retornar um erro ao chamador da API ou encaminhar solicitações para um back-end especificado. Depois que o serviço de back-end se recupera, o disjuntor fecha e as solicitações se tornam normais.

Descrição do parâmetro

Tabela 4-6 Descrição do parâmetro

Parâmetro	Descrição
Policy Type	● API específica Controlar solicitações para uma única API. ● Compartilhamento de API Controlar solicitações para todas as APIs vinculadas à política.
Circuit Breaker Type	Tipo de disparo do disjuntor. ● **Timeout downgrade**: o disjuntor será acionado no tempo limite do back-end. ● **Condition downgrade**: o disjuntor será disparado quando as condições de correspondência configuradas forem atendidas.
Condition Type	Modo de acionamento do disjuntor. ● **Count**: quando o número de solicitações que atendem às condições dentro de uma janela de tempo especificada atinge o limite, o disjuntor é acionado imediatamente. ● **Percentage**: quando a porcentagem de solicitações que atendem às condições dentro de uma janela de tempo especificada atinge o limite, o disjuntor é acionado após a expiração da janela de tempo.

Parâmetro	Descrição
Match Condition	Este parâmetro só é necessário quando **Circuit Breaker Type** é definido como **Condition downgrade**. Configure condições de disparo para o disjuntor. ● **Response Error Codes**: o disjuntor será acionado se o back-end responder com códigos de status especificados. ● **Response Latency**: o disjuntor será acionado se a latência da resposta do back-end atingir um limite especificado.
Time Window	O período para determinar quantas vezes as condições foram satisfeitas. Use este parâmetro junto com **Threshold** ou **Min Percentage**. Se o limite ou porcentagem for atingido, o disjuntor é acionado.
Threshold	Este parâmetro é necessário somente quando **Condition Type** é definido como **Count**. Defina o limite para acionar o disjuntor. Use este parâmetro junto com **Time Window**. Uma vez que o número de solicitações de back-end que atendem às condições dentro da janela de tempo atinge o limite, o disjuntor é acionado. **NOTA** Uma política de disjuntor é acionada para um único componente de gateway. Se o gateway tiver vários componentes, o acionamento para cada componente será determinado separadamente. Se o limiar for atingido dentro da janela de tempo para um componente de gateway, as solicitações enviadas ao componente acionam o disjuntor e outros componentes de gateway ainda encaminham solicitações normalmente. Um componente de gateway é um endereço de conexão do gateway. Para exibir o número de componentes de gateway, vá para a página **Gateway Information** do gateway e exiba o número de endereços IP em **Private Network Access IP**.
Min Calls	Este parâmetro só é necessário quando **Condition Type** é definido como **Percentage**. Defina o número mínimo de chamadas de API que acionarão o disjuntor dentro do período de tempo. O disjuntor não será acionado se o número de chamadas de API dentro do período de tempo for menor que esse valor.
Min Percentage	Este parâmetro só é necessário quando **Condition Type** é definido como **Percentage**. Defina o limite para acionar o disjuntor. Use este parâmetro junto com **Time Window**. Uma vez que a porcentagem de solicitações de back-end que atendem às condições dentro da janela de tempo atinge o limite, o disjuntor é acionado.
Control Duration	Tempo para o qual o disjuntor estará ligado. Quando o tempo é alcançado, o disjuntor será desligado.

Parâmetro	Descrição
Backend Downgrade	Determine se deve habilitar o downgrade do back-end. ● Habilitar: solicitações de APIs que acionaram um downgrade serão encaminhadas para um back-end especificado. ● Desabilitar: as solicitações de APIs que desencadearam um downgrade não serão encaminhadas para nenhum back-end. Em vez disso, uma mensagem de erro indicando que o serviço não está disponível será retornada.

Parâmetro	Descrição
Backend Type	Este parâmetro é necessário apenas quando o **Backend Downgrade** está habilitado. Especifique o tipo de back-end para o qual as solicitações serão encaminhadas quando o disjuntor estiver ligado. ● **Mock**: a resposta definida será retornada. – **Status Code**: o código de status a ser incluído na resposta – **Response**: o corpo da resposta, que está no formato JSON – **Response Header**: parâmetros de cabeçalho a serem incluídos na resposta ● **HTTP&HTTPS**: as solicitações de back-end serão encaminhadas para um serviço de back-end HTTP&HTTPS especificado. – **Load Balance Channel**: determine se deve usar um canal de balanceamento de carga para acessar o serviço de back-end. Se sim, **crie um canal de balanceamento de carga** com antecedência. – **Backend URL**: endereço do serviço de back-end para encaminhar solicitações. – **Timeout (ms)**: tempo limite de solicitação de back-end. O valor padrão é 5000 ms. ● **FunctionGraph**: as solicitações de back-end serão encaminhadas para uma função especificada. – **Function URN**: o identificador único de uma função. Clique em **Select** para selecionar uma função. – **Function Name**: exibido automaticamente após a seleção de uma função. – **Version**: versão da função a ser usada para receber solicitações de back-end. – **Invocation Mode**: o modo em que a função é invocada. **Synchronous**: ao receber uma solicitação de invocação, o FunctionGraph processa imediatamente a solicitação e retorna um resultado. O cliente fecha a conexão uma vez que recebeu uma resposta do back-end. **Asynchronous**: após receber uma solicitação de chamada, o FunctionGraph enfileira a solicitação e retorna o resultado após a solicitação ser processada com sucesso. O servidor processa as solicitações de enfileiramento uma a uma quando está ocioso. O cliente não se preocupa com o resultado da invocação. – **Timeout (ms)**: tempo limite de solicitação de back-end. O valor padrão é 5000 ms. ● **Passthrough**: as solicitações de back-end serão encaminhadas para o back-end da API original.

Parâmetro	Descrição
	Para adicionar parâmetros de cabeçalho a solicitações de back-end, clique em **Add Parameter**.
Downgrade Parameter Settings	Determine se deve ativar a configuração do parâmetro de downgrade. Depois que essa opção for ativada, as regras personalizadas terão precedência sobre as condições de disparo padrão e as configurações de downgrade configuradas acima. ● Se uma regra personalizada for correspondida, as condições de disparo e as configurações de downgrade definidas na regra serão aplicadas. Se a regra personalizada correspondente não contiver nenhuma condição de acionamento ou configurações de downgrade, as configurações padrão em **Trigger Configuration** e **Backend Downgrade** serão aplicadas. ● Se nenhuma regra personalizada for correspondida, as configurações padrão serão aplicadas.
Parameters	Defina parâmetros para correspondência de regras. ● **Parameter Location**: posição de um parâmetro nas solicitações da API. ● **Parameter Name**: nome de um parâmetro usado para correspondência de regras. Por padrão, o sistema fornece os parâmetros **reqPath** (caminho de solicitação) e **method** (método de solicitação). Clique em **Add Parameter** para adicionar parâmetros.

Parâmetro	Descrição
Rules	Personalize as regras de correspondência para o disjuntor. Clique em **Add Rule** para adicionar regras. O sistema combina regras de cima para baixo. Ajuste a prioridade da regra movendo as regras para cima ou para baixo. ● **Conditions**: clique em para definir expressões de condição. Se houver três ou mais expressões, você pode colocá-las em camadas clicando em **Set Lower Level**. – =: igual a – **!=**: não igual a – **pattern**: expressão regular – **enum**: valores enumerados. Separe-os com vírgulas (,). ● Para obter detalhes sobre como configurar as condições de acionamento e o downgrade do back-end, consulte as instruções para as configurações padrão acima. Exemplo: você habilitou **Downgrade Parameter Settings** e adicionou regras **rule01** e **rule02** em sequência. E você desabilitou a **Trigger Configuration** e habilitou **Backend Downgrade** para **rule01** e habilitou ambas as opções para **rule02**. Com essas configurações, o disjuntor primeiro verifica se as condições da **rule01** são atendidas. Em caso afirmativo, o disjuntor é ativado com base nas configurações padrão porque nenhuma condição de disparo foi definida na **rule01** e o downgrade do back-end configurado na **rule01** é executado. Se não, a verificação é continuada para a **rule02**.

Exemplo de script

```
{
  "breaker_condition":{
    "breaker_type":"timeout",
    "breaker_mode":"counter",
    "unhealthy_threshold":30,
    "time_window":15,
    "open_breaker_time":15,
    "unhealthy_percentage":51,
    "min_call_threshold":20
  },
  "scope":"share",
  "downgrade_default":{
    "type":"http",
    "passthrough_infos":null,
    "func_info":null,
    "mock_info":null,
    "http_info":{
      "isVpc":false,
      "vpc_channel_id":"",
      "address":"10.10.10.10",
      "scheme":"HTTP",
      "method":"GET",
      "path":"/demo",
      "timeout":5000
    },
    "http_vpc_info":null
  },
```



```
  "downgrade_parameters":[
  {
    "name":"reqPath",
    "type":"path",
    "value":"path",
    "disabled":true,
    "focused":true,
    "id":"92002eqbpilg6g"
  },
  {
    "name":"method",
    "type":"method",
    "value":"method",
    "disabled":true,
    "focused":true,
    "id":"tuvxetsdqvcos8"
  }],
  "downgrade_rules":[
  {
    "rule_name":"rule-test1",
    "parameters":[
      "reqPath",
      "method"
    ],
    "match_regex":"[\"reqPath\",\"==\",\"/test\"]",
    "downgrade_backend":{
      "type":"mock",
      "passthrough_infos":null,
      "func_info":null,
      "mock_info":{
        "status_code":200,
        "result_content":"{status: ok}",
        "headers":[]
      },
      "http_info":null,
      "http_vpc_info":null
    },
    "breaker_condition":{
      "breaker_type":"timeout",
      "breaker_mode":"percentage",
      "unhealthy_threshold":30,
      "time_window":15,
      "open_breaker_time":15,
      "unhealthy_percentage":51,
      "min_call_threshold":20
    }
  }]
}
```


4.7 Limitação de solicitação

A limitação de solicitações limita o número de vezes que as APIs podem ser chamadas por um usuário ou aplicação em um período específico para proteger os serviços de back-end. A limitação pode ser até o minuto ou segundo. Para garantir a continuidade do serviço de uma API, crie uma política de limitação de solicitações para a API.

Diretrizes de uso

- Adicionar uma política de limitação de solicitações a uma API significa vinculá-las umas às outras. Uma API pode ser vinculada a apenas uma política de limitação de solicitações para um determinado ambiente, mas cada política de limitação de solicitações pode ser vinculada a várias APIs.
- Para APIs não vinculadas a uma política de limitação de solicitações, o limite de limitação é o valor de **ratelimit_api_limits** definido na página **Parameters** do gateway.

Parâmetros de configuração

Tabela 4-7 Descrição do parâmetro

Parâmetro	Descrição
Name	Nome da política de limitação de solicitação.
Type	Limitação de solicitação baseada em API ou compartilhada por API. ● **API específica**: a limitação de solicitações é baseada em todas as APIs às quais a política está vinculada. ● **Compartilhamento de API**: a limitação de solicitações baseia-se em todas as APIs como um todo às quais a política está vinculada.
Period	Por quanto tempo você deseja limitar o número de chamadas de API. Este parâmetro pode ser usado em conjunto com os seguintes parâmetros: ● **Max. API Requests**: limite o número máximo de vezes que uma API pode ser chamada em um período específico. ● **Max. User Requests**: limite o número máximo de vezes que uma API pode ser chamada por um usuário dentro de um período específico. ● **Max. Credential Requests**: limite o número máximo de vezes que uma API pode ser chamada por uma credencial dentro de um período específico. ● **Max. IP Address Requests**: limite o número máximo de vezes que uma API pode ser chamada por um endereço IP dentro de um período específico.
Max. API Requests	O número máximo de vezes que cada API vinculada pode ser chamada dentro do período especificado. Este parâmetro deve ser utilizado em conjunto com o **Period**.
Max. User Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um usuário dentro do período especificado. **Esse limite se aplica apenas às APIs acessadas por meio da autenticação do IAM.** ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**. ● Se houver muitos usuários na sua conta que acessam uma API, os limites de limitação de solicitações da API serão aplicados a todos esses usuários.
Max. Credential Requests	O número máximo de vezes que cada API vinculada pode ser chamada por uma credencial dentro do período especificado. **Esse limite só se aplica a APIs acessadas por meio da autenticação da aplicação.** ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.

Parâmetro	Descrição
Max. IP Address Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um endereço IP dentro do período especificado. ● O valor deste parâmetro não pode exceder o de **Max. API Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Description	Descrição da política de limitação de solicitação.

Operações de acompanhamento

Para controlar o número máximo de chamadas de API recebidas de uma credencial ou locatário específico, especifique a credencial ou locatário a ser excluído referindo-se a **Adicionar uma aplicação excluída**. Se uma credencial for excluída em uma política de limitação de solicitação, qualquer limite configurado exclusivamente para essa credencial terá precedência sobre a política. A API e os limites de solicitação do usuário dessa política ainda são válidos. Se um locatário for excluído em uma política de limitação de solicitação, qualquer limite configurado exclusivamente para esse locatário será aplicado. Os limites de API e solicitação de credenciais dessa política ainda são válidos.

Adicionar uma aplicação excluída

Você criou uma aplicação ou obteve um ID de aplicação de outros locatários.

Passo 1 Na página de detalhes da política de limitação de solicitação, clique na guia **Excluded Apps**.

Passo 2 Clique em **Select Excluded App**.

Passo 3 Selecione uma aplicação para excluir. Você pode usar um dos seguintes métodos:

- Para selecionar uma aplicação existente, clique em **Existing**, selecione uma aplicação e insira um limite.
- Para selecionar uma aplicação de outros locatários, clique em **Cross-tenant** e insira o ID da aplicação e um limite.

NOTA

O limite deve ser um número inteiro positivo e não pode exceder o valor de **Max. API Requests**.

----Fim

Adicionar um locatário excluído

Passo 1 Na página de detalhes da política de limitação de solicitações, clique na guia **Excluded Tenants**.

Passo 2 Clique em **Select Excluded Tenant**.

Passo 3 Insira as informações do locatário.

Figura 4-1 Adicionar um locatário excluído

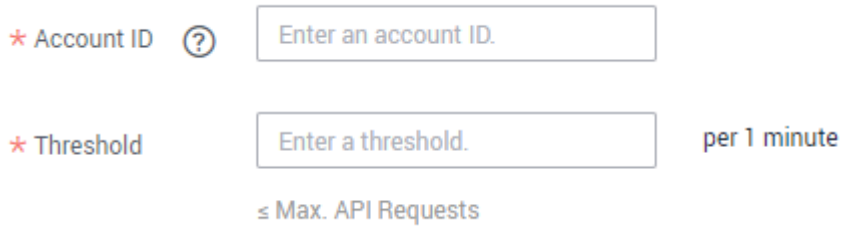


Tabela 4-8 Configuração de locatário excluído

Parâmetro	Descrição
Tenant ID	ID da conta ou ID do projeto. Para obter detalhes, consulte a descrição sobre **Excluded Tenants** em Tabela 4-4.
Threshold	O número máximo de vezes que uma API pode ser chamada pelo locatário dentro de um período especificado. O valor deste parâmetro não pode exceder o de **Max. API Requests**.

Passo 4 Clique em **OK**.

NOTA

Limites de locatários excluídos têm precedência sobre o valor de **Max. User Requests**.

Por exemplo, uma política de limitação de solicitação foi configurada, com **Max. API Requests** sendo **10**, **Max. User Requests** sendo **3**, **Period** sendo 1 minuto e dois locatários excluídos (máximo de **2** solicitações de API para o locatário A e máximo de **4** solicitações de API para o locatário B). Se a política de limitação de solicitações estiver vinculada a uma API, os locatários A e B poderão acessar a API 2 e 4 vezes em 1 minuto, respectivamente.

----Fim

4.8 Controle de acesso

As políticas de controle de acesso são um tipo de medidas de segurança fornecidas pelo APIG. Você pode usá-las para permitir ou negar acesso à API de endereços IP ou contas específicos.

As políticas de controle de acesso terão efeito para uma API somente se elas tiverem sido vinculadas à API.

Diretrizes de uso

Cada API pode ser vinculada a apenas uma política de controle de acesso para um determinado ambiente, mas cada política de controle de acesso pode ser vinculada a várias APIs.

Parâmetros de configuração

Tabela 4-9 Descrição do parâmetro

Parâmetro	Descrição
Name	Nome da política de controle de acesso.
Type	Tipo da origem a partir da qual as chamadas de API devem ser controladas. ● **IP address**: especifique endereços IP e intervalos de endereços IP que têm ou não permissão para acessar uma API. ● **Account name**: especifique os nomes das contas que têm ou não permissão para acessar uma API.
Effect	Opções: **Allow** e **Deny**. Use esse parâmetro junto com **Restriction Type** para controlar o acesso de determinados endereços IP ou contas a uma API.
IP Address	Endereços IP e intervalos de endereços IP que têm ou não permissão para acessar uma API Você precisa definir esse parâmetro somente se tiver definido **Restriction Type** como **IP address**. **NOTA** Você pode definir um máximo de 100 endereços IP, respectivamente, para permitir ou negar acesso.
Account Names	Nomes das contas que têm ou não permissão para acessar uma API. **Este parâmetro se aplica apenas a APIs que são acessadas por meio da autenticação do IAM.** Você precisa definir esse parâmetro apenas se tiver definido **Type** como **Account name**. Você pode inserir vários nomes de conta e separá-los com vírgulas, por exemplo, **aaa,bbb**. **NOTA** O APIG executa o controle de acesso em sua conta, não em usuários do IAM criados usando a conta.

4.9 Chaves de assinatura

As chaves de assinatura são usadas pelos serviços de back-end para verificar a identidade do APIG.

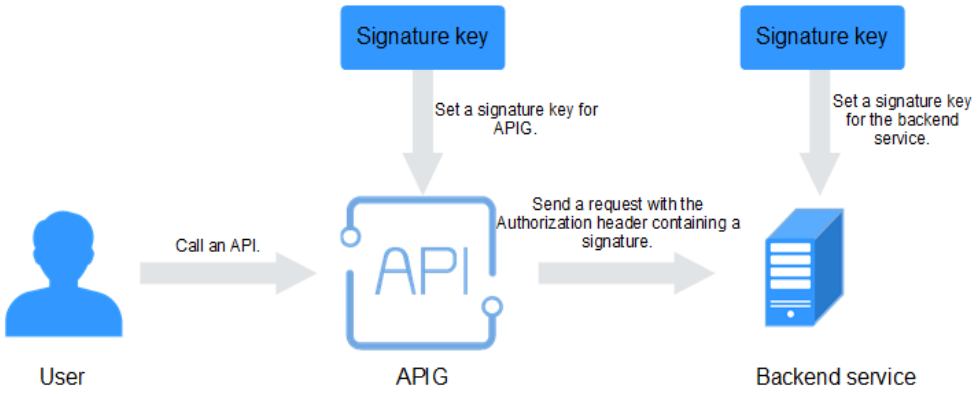
Uma chave de assinatura consiste em uma chave e um segredo e pode ser usada somente depois de vinculada a uma API. Quando uma API vinculada a uma chave de assinatura é chamada, o APIG adiciona detalhes de assinatura à solicitação da API. O serviço de back-end da API assina a solicitação da mesma maneira e verifica a identidade da APIG verificando se a assinatura é consistente com a do cabeçalho de **Authorization** enviado pelo APIG.

Diretrizes de uso

Uma API só pode ser vinculada a uma chave de assinatura em um determinado ambiente, mas cada chave de assinatura pode ser vinculada a várias APIs.

Procedimento

Figura 4-2 Fluxo de processo de chave de assinatura



1. Crie uma chave de assinatura no console do APIG.
2. Vincule a chave de assinatura a uma API.
3. APIG envia solicitações assinadas contendo uma assinatura no cabeçalho **Authorization** para o serviço de back-end. O serviço de back-end pode usar diferentes linguagens de programação (Java, Go, Python, JavaScript, C#, PHP, C++ e C) para assinar cada solicitação e verificar se as duas assinaturas são consistentes.

Parâmetros de configuração

Tabela 4-10 Descrição do parâmetro

Parâmetro	Descrição
Name	Nome da chave de assinatura.
Type	Tipo de autenticação. Opções: **HMAC**, **Basic auth**, **AES** e **Public key**. A **Public key** estará disponível somente se **public_key_enable** tiver sido ativada na **página Parâmetros** do gateway.
Signature Algorithm	Selecione um algoritmo de assinatura AES. Opções: ● aes-128-cfb ● aes-256-cfb

Parâmetro	Descrição
Key	Defina a chave com base no tipo de chave de assinatura selecionada. ● Se **Type** estiver **HMAC**, insira a chave do par de chaves usado para autenticação da aplicação. ● Se **Type** estiver **Basic auth**, incorpore o nome de usuário usado para a autenticação básica. ● Se **Type** estiver definido como **AES**, insira a chave usada para autenticação AES. ● Se **Type** estiver **Public key**, insira a chave pública usada para autenticação.
Secret	Insira as informações de segredos com base no tipo de chave selecionado. ● Se **Type** estiver **HMAC**, insira o segredo do par de chaves usado para autenticação das aplicações. ● Se **Type** estiver **Basic auth**, digite a senha usada para autenticação básica. ● Se **Type** estiver definido como **AES**, insira o vetor usado para autenticação AES. ● Se **Type** estiver **Public key**, digite a chave privada usada para autenticação.
Confirm Secret	Digite o segredo novamente.

Verificar o resultado da assinatura

Assine cada solicitação de back-end seguindo as instruções no **Algoritmo de assinatura** e verifique se a assinatura do back-end é consistente com a assinatura no cabeçalho **Authorization** da solicitação da API.

4.10 Autorizadores personalizados

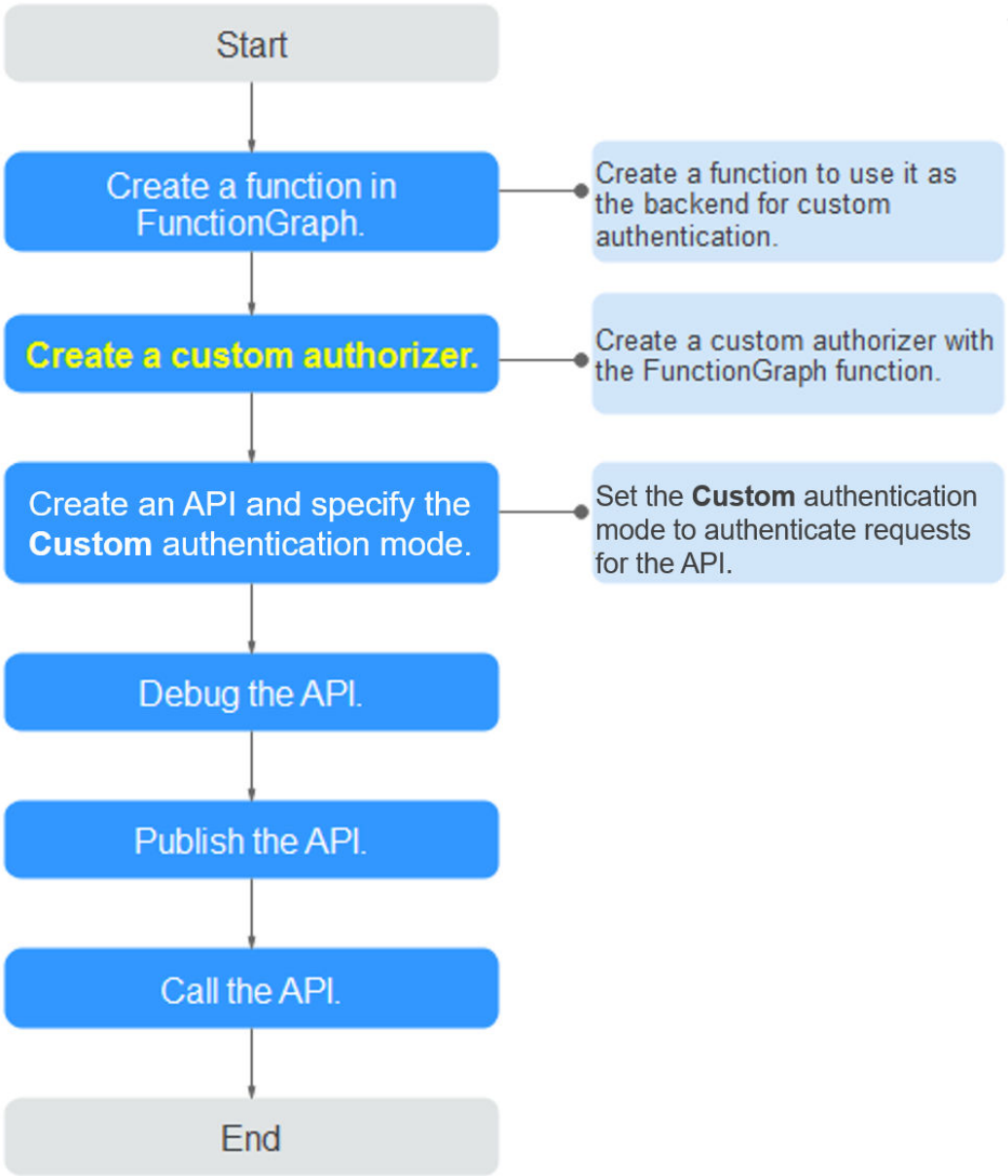
O APIG suporta autenticação personalizada de solicitações de front-end e back-end.

- Autenticação personalizada do front-end: se você já tiver um sistema de autenticação, poderá configurá-lo em uma função e criar um autorizador personalizado usando a função para autenticar solicitações de API.
- Autenticação personalizada de back-end: você pode criar um autorizador personalizado 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 APIG para se conectar ao seu sistema de autenticação de back-end.

> **NOTA**
>
> A autenticação personalizada é implementada usando o FunctionGraph e não é suportada se o FunctionGraph não estiver disponível na região selecionada.
>
> Para obter detalhes sobre a autenticação personalizada, consulte *Guia de desenvolvedor*.

A figura a seguir mostra o processo de chamada de APIs por meio de autenticação personalizada.

Figura 4-3 Chamar APIs por meio de autenticação personalizada



Pré-requisitos

Você criou uma função no FunctionGraph.

Criação de um autorizador personalizado

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Policies**.

Passo 4 Na página **Custom Authorizers**, clique em **Create Custom Authorizer**.

Configurar parâmetros de autorizador personalizados.

Tabela 4-11 Parâmetros para criar um autorizador personalizado

Parâmetro	Descrição
Name	Nome do autorizador.
Type	● **Frontend**: autentica o acesso às APIs. ● **Backend**: autentica o acesso aos serviços de back-end.
Function URN	Selecione uma função do FunctionGraph.
Version/Alias	Selecione uma versão de função ou alias. Para obter detalhes, consulte as seções "Gerenciamento de versões" e "Gerenciamento de aliases" no *Guia de usuário do FunctionGraph*.
Max. Cache Age (s)	O tempo para resultados de autenticação de cache. O valor **0** significa que os resultados da autenticação não serão armazenados em cache. O valor máximo é **3600**.
Identity Sources	Parâmetros de solicitação usados para autenticação. Esse parâmetro é obrigatório somente se você definir **Type** como **Frontend** e **Max. Cache Age (s)** é maior que **0**. Quando o cache é usado, esse parâmetro é usado como um critério de pesquisa para consultar resultados de autenticação.
Send Request Body	Determine se o corpo de cada solicitação de API deve ser enviado para a função de autenticação. Se você habilitar essa opção, o corpo da solicitação será enviado para a função de autenticação da mesma maneira que os cabeçalhos e as cadeias de consulta.
User Data	Parâmetros de solicitação personalizados a serem usados em conjunto com **Identity Sources** quando o APIG invoca uma função.

Passo 5 Clique em **OK**.

----Fim

4.11 Certificados SSL

Os grupos de API que contêm APIs compatíveis com HTTPS devem ter seus nomes de domínio independentes vinculados a certificados SSL.

Pré-requisitos

- Somente certificados SSL no formato PEM são suportados.
- Certificados SSL suportam apenas os algoritmos de criptografia RSA, ECDSA e DSA.

Adição de um certificado SSL

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Policies**.

Passo 4 Na página de guia **SSL Certificates**, clique em **Create SSL Certificate**.

Tabela 4-12 Configuração do certificado SSL

Parâmetro	Descrição
Name	Digite um nome de certificado SSL que esteja em conformidade com regras específicas para facilitar a pesquisa.
Gateways Covered	• **Current**: o certificado será exibido apenas para o gateway atual. • **All**: o certificado será exibido para todos os gateways.
Content	Conteúdo do certificado SSL em formato PEM. Abra o arquivo de certificado PEM de destino usando o Bloco de notas ou outras ferramentas e copie o conteúdo do certificado para **Content**. Se o certificado não estiver no formato PEM, **converta-o para este formato**.
Key	Chave de certificado SSL em formato PEM. Abra o arquivo de chave privada KEY ou PEM usando o Bloco de notas ou outras ferramentas e copie a chave privada para **Key**.

Passo 5 Clique em **OK**. O certificado SSL é adicionado.

----Fim

Converter o formato do certificado em PEM

Formato	Converter com OpenSSL
CER/CRT	Renomeie o arquivo de certificado **cert.crt cert.pem**.

Formato	Converter com OpenSSL
PFX	● Execute o comando de exportação de chave privada. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **key.pem**: openssl pkcs12 -in cert.pfx -nocerts -out key.pem ● Execute o comando de exportação de certificados. Por exemplo, execute o seguinte comando para converter **cert.pfx** em **cert.pem**: openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	1. Execute o comando de conversão de certificado. Por exemplo, execute o seguinte comando para converter **cert.p7b** em **cert.cer**: openssl pkcs7 -print_certs -in cert.p7b -out cert.cer 2. Renomeie o arquivo de certificado **cert.cer cert.pem**.
DER	● Execute o comando de exportação de chave privada. Por exemplo, execute o seguinte comando para converter **privatekey.der** em **privatekey.pem**: openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem ● Execute o comando de exportação de certificados. Por exemplo, execute o seguinte comando para converter **cert.cer** em **cert.pem**: openssl x509 -inform der -in cert.cer -out cert.pem

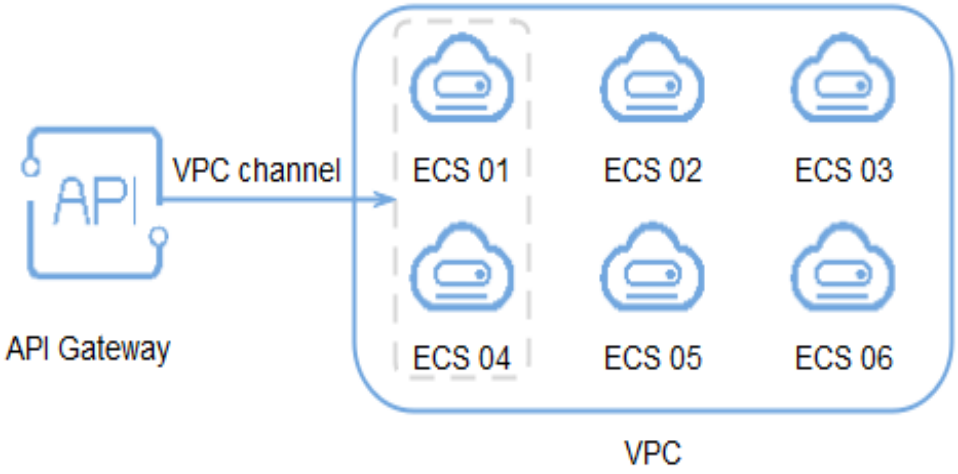
4.12 Canais de balanceamento de carga

Os canais de balanceamento de carga permitem que os serviços sejam acessados por meio de sub-redes em suas VPCs, reduzindo a latência e equilibrando as cargas de serviços de back-end.

Depois de criar um canal de balanceamento de carga, você pode configurá-lo para uma API de um serviço de back-end HTTP/HTTPS.

Por exemplo, seis ECSs foram implementados e um canal de balanceamento de carga foi criado para alcançar o ECS 01 e o ECS 04. Nessa situação, o APIG pode acessar esses dois ECSs pelo canal.

Figura 4-4 Acessar ECSs em um canal de balanceamento de carga por meio do APIG



Pré-requisitos

Você criou servidores em nuvem.

Criar um canal de balanceamento de carga

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Policies**.

Passo 4 Clique na guia **Load Balance Channels**.

Passo 5 Clique em **Create Load Balance Channel** e configure as informações básicas.

Tabela 4-13 Informações básicas

Parâmetro	Descrição
Name	Nome do canal.
Port	A porta do host do canal, ou seja, a porta de seus serviços de back-end. Faixa: 1 – 65535.
Routing Algorithm	O algoritmo a ser usado para encaminhar solicitações para os servidores em nuvem que você selecionar. Os seguintes algoritmos de roteamento estão disponíveis: ● **WRR**: round robin ponderado ● **WLC**: conexão mínima ponderada ● **SH**: hash de origem ● **URI hashing**

Passo 6 Configure servidores.

NOTA

- Para garantir verificações de integridade bem-sucedidas e disponibilidade de serviços, configure grupos de segurança dos servidores em nuvem para permitir o acesso de 100.125.0.0/16.
- Os canais de balanceamento de carga suportam balanceadores de carga de rede privada. Você pode especificar endereços de servidor.

- Selecione servidores em nuvem
  a. Crie um grupo de servidores e defina o nome, o peso e a descrição do grupo.
  b. Adicione servidores em nuvem.
- Especifique endereços IP
  a. Crie um grupo de servidores e defina o nome, o peso e a descrição do grupo.
  b. Clique em **Add Backend Server Addresses**, digite um endereço de servidor back-end e especifique se deseja ativar o nó em espera.

Passo 7 Configure verificações de integridade.

Tabela 4-14 Informações básicas

Parâmetro	Descrição
Protocol	O protocolo usado para executar verificações de integridade em servidores em nuvem associados ao canal. Opções: ● TCP ● HTTP ● HTTPS Valor padrão: **TCP**.
Two-Way Authentication	**Defina este parâmetro apenas quando o protocolo estiver definido como HTTPS.** Determine se deve permitir que o APIG autentique o serviço de back-end da API. Para obter detalhes sobre como configurar o certificado para autenticação bidirecional, consulte **Procedimento**.
Path	**Defina este parâmetro apenas quando o protocolo não estiver definido como TCP.** O caminho de destino para verificações de integridade.
Method	GET HEAD
Check Port	A porta de destino para verificações de integridade. Por padrão, a porta do canal será usada.
Healthy Threshold	O número de verificações consecutivas bem-sucedidas necessárias para que um servidor de nuvem seja considerado saudável. Faixa: 2 – 10. Valor padrão: **2**.

Parâmetro	Descrição
Unhealthy Threshold	O número de verificações consecutivas com falhas necessárias para que um servidor de nuvem seja considerado não íntegro. Faixa: 2 – 10. Valor padrão: **5**.
Timeout (s)	O tempo limite usado para determinar se uma verificação de integridade falhou. Unidade: s. Faixa: 2 – 30. Valor padrão: **5**.
Interval (s)	O intervalo entre verificações consecutivas. Unidade: s. Faixa: 5 – 300. Valor padrão: **10**.
Códigos de resposta	**Defina este parâmetro apenas quando o protocolo não estiver definido como TCP.** Os códigos HTTP usados para verificar uma resposta bem-sucedida de um destino.

Passo 8 Clique em **Finish**.

----Fim

Operações de acompanhamento

Crie uma API para serviços de back-end implementados em uma VPC para balancear cargas.

4.13 Gerenciamento de ambientes

Uma API pode ser chamada em diferentes ambientes, como ambientes de produção, teste e desenvolvimento. RELEASE é o ambiente padrão fornecido pelo APIG.

Criação de um ambiente

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Policies**.

Passo 4 Clique na guia **Environments**.

Passo 5 Clique em **Create Environment** e defina as informações do ambiente.

Tabela 4-15 Informações de ambiente

Parâmetro	Descrição
Name	Nome do ambiente.
Description	Descrição do ambiente.

Passo 6 Clique em **OK**.

Depois que o ambiente é criado, ele é exibido na lista de ambientes.

----Fim

Acessar um ambiente

Você pode chamar uma API no ambiente RELEASE usando uma API RESTful. Para acessar a API em outros ambientes, adicione o cabeçalho **X-Stage** à solicitação para especificar um nome de ambiente. Por exemplo, adicione **X-Stage:DEVELOP** ao cabeçalho da solicitação para acessar uma API no ambiente **DEVELOP**.

NOTA

O APIG não suporta depuração de API com variáveis de ambiente.

Operações de acompanhamento

Depois de criar um ambiente e uma variável, **publique APIs** no ambiente para que possam ser chamadas pelos chamadores da API.

5 Credenciais

5.1 Criar uma credencial e vinculá-la às APIs

Para APIs que usam autenticação de aplicação, crie credenciais para gerar IDs de credenciais e pares de chaves/segredos. Ao chamar essa API, vincule uma credencial à API e use o par de chaves/segredos para substituí-la no SDK para que a APIG possa autenticar sua identidade. Para obter detalhes sobre a autenticação de aplicações, consulte o **Guia de desenvolvedor**.

NOTA

- As APIs que usam autenticação do IAM ou não exigem autenticação não precisam de credenciais.
- Você pode criar um máximo de 50 credenciais para cada gateway.

Criação de uma credencial

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **Credentials**.

Passo 4 Clique em **Create Credential** e defina informações de credencial.

Tabela 5-1 Informações da credencial

Parâmetro	Descrição
Name	Nome da credencial.
Description	Descrição sobre a credencial.

NOTA

Você pode personalizar AppKeys e AppSecrets. Um AppKey é um identificador gerado automaticamente, que é globalmente exclusivo. Não é aconselhável personalizar um, a menos que seja necessário.

Passo 5 Clique em **OK**.

- Depois que a credencial é criada, seu nome e ID são exibidos na página **Credentials**.
- Clique no nome da credencial e visualize a chave e o segredo.

----Fim

Vinculação de uma credencial a APIs

Passo 1 Na página **Credentials**, clique no nome da credencial de destino.

Passo 2 Na área **APIs**, clique em **Bind to APIs**.

Passo 3 Selecione um ambiente, um grupo de APIs e APIs.

Passo 4 Clique em **OK**.

Para desvincular uma API, clique em **Unbind** na linha que contém a API.

NOTA

Uma credencial pode ser vinculada a várias APIs que usam autenticação de aplicação e cada uma dessas API pode ser vinculada a várias credenciais.

----Fim

5.2 Redefinição de segredo

Redefina o segredo de uma credencial conforme necessário. Após a redefinição, o segredo original se torna inválido e as APIs às quais a credencial está vinculada não podem ser chamadas. Para chamar as APIs, atualize o segredo no SDK. A chave é única e não pode ser redefinida.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **Credentials**.

Passo 4 Clique no nome da credencial de destino.

Passo 5 Clique em **Reset Secret**.

Passo 6 Clique em **OK**.

----Fim

5.3 Adição de um AppCode para autenticação simples

AppCodes são credenciais de identidade de uma credencial usada para chamar APIs no modo de autenticação simples. Neste modo, o parâmetro **X-Apig-AppCode** (cujo valor é um AppCode na página de detalhes da credencial) é adicionado ao cabeçalho da solicitação HTTP para uma resposta rápida. O APIG verifica apenas o AppCode e o conteúdo da solicitação não precisa ser assinado.

Quando uma API é chamada usando a autenticação da aplicação e a autenticação simples é ativada para a API, a chave e o segredo podem ser usados para assinar e verificar a solicitação da API. O AppCodes também pode ser usado para autenticação simples.

NOTA

- Por motivos de segurança, a autenticação simples suporta apenas chamadas de API por HTTPS.
- Você pode criar no máximo cinco AppCodes para cada credencial.

Gerenciamento de um AppCode

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **Credentials**.

Passo 4 Clique no nome da credencial de destino.

Passo 5 Em **AppCodes**, clique em **Add AppCode**.

Passo 6 Configure as informações do AppCode e clique em **OK**.

Tabela 5-2 Configuração do AppCode

Parâmetro	Descrição
AppCode Type	Selecione o método para gerar um AppCode. ● **Automatically generated**: um AppCode é gerado pelo sistema. ● **Custom**: especifique um AppCode.
AppCode	Insira um AppCode se você definir **AppCode Type** como **Custom**.

----Fim

Usar o AppCode para autenticação simples de solicitações de API

Passo 1 Ao criar uma API, defina **Authentication Mode** como **App** e ative **Simple Authentication**.

NOTA

Depois de habilitar a autenticação simples para uma API existente, você precisa publicar a API novamente para que a configuração entre em vigor.

Passo 2 Vincule uma credencial à API.

Passo 3 Ao enviar uma solicitação, adicione o parâmetro **X-Apig-AppCode** ao cabeçalho da solicitação e omita a assinatura da solicitação.

Por exemplo, ao usar curl, adicione o parâmetro **X-Apig-AppCode** ao cabeçalho da solicitação e defina o valor do parâmetro como **AppCode gerado**.


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

----Fim

5.4 Vinculação de uma política de cota de credenciais

Uma política de cota de credenciais limita o número de chamadas de API que uma credencial pode fazer durante um período especificado.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **Credentials**.

Passo 4 Clique no nome da credencial de destino.

Passo 5 Na área **Credential Quota Policies**, clique em **Bind**.

Passo 6 Especifique o tipo de política.

- **Existing policy**: selecione uma política.
- **New policy**: configure uma política referindo-se a **Tabela 5-3**.

Tabela 5-3 Configuração da política de cota de credenciais

Parâmetro	Descrição
Name	Digite um nome de política de cota de credencial que esteja em conformidade com regras específicas para facilitar a pesquisa.
Effective On	Momento em que a política de cotas entra em vigor. Por exemplo, se **Effective On** estiver definido como **Aug 8, 2020 05:05:00** e **Period** estiver definido como 1 hora, a política de cotas entrará em vigor em 8 de agosto de 2020 05:05:00. O período do quinto minuto de uma hora ao quinto minuto da hora seguinte é um ciclo, por exemplo, 05:05:00-06:05:00.
Period	Período em que a política de cotas é aplicada. A unidade pode ser segundo, minuto, hora ou dia. Este parâmetro deve ser usado junto com **Max. API Requests** para limitar o número total de vezes que uma API pode ser chamada por um cliente dentro do período especificado.
Max. API Requests	O número máximo de vezes que uma API pode ser chamada por um cliente. Este parâmetro deve ser usado junto com **Period**.
Description	Descrição sobre a política de cota de credencial.

Passo 7 Após a conclusão da configuração, clique em **OK**.

----Fim

5.5 Vinculação de uma política de controle de acesso

Como um mecanismo de proteção para serviços de back-end, as políticas de controle de acesso controlam os endereços IP do cliente (chamador de API) que podem acessar APIs. Você pode configurar uma política de controle de acesso para permitir ou negar o acesso de endereços IP especificados a uma API.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **Credentials**.

Passo 4 Clique no nome da credencial de destino.

Passo 5 Na área **Access Control Policy**, clique em **Bind**.

Passo 6 Configure as informações da política.

Tabela 5-4 Configuração da política de controle de acesso

Parâmetro	Descrição
Effect	Tipo de controle de acesso. Opções: ● **Allow**: somente clientes com endereços IP especificados têm permissão para chamar APIs às quais a credencial está vinculada. ● **Deny**: os clientes com endereços IP especificados não têm permissão para chamar APIs às quais a credencial está vinculada.
IP Addresses	Clique em **Add IP Address** para adicionar endereços IP.

Passo 7 Após a conclusão da configuração, clique em **OK**.

----Fim

6 Monitoramento e análise

6.1 Monitoramento de API

6.1.1 Monitoramento de métricas

Introdução

Esta seção descreve as métricas que o APIG reporta ao serviço Cloud Eye. Você pode visualizar métricas e alarmes usando o console do Cloud Eye.

Namespace

SYS.APIC

Métricas

Tabela 6-1 Descrição de métrica

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto e dimensão monitorados	Período de monitoramento (minuto)
requests	Solicitações	Número de vezes que todas as APIs em um gateway dedicado foram chamadas.	≥0	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto e dimensão monitorados	Período de monitoramento (minuto)
error_4xx	Erros 4xx	Número de vezes que todas as APIs no gateway dedicado retornam um erro 4xx.	≥0	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1
error_5xx	Erros 5xx	Número de vezes que todas as APIs no gateway dedicado retornam um erro 5xx.	≥0	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1
throttled_calls	Chamadas API limitadas	Número de vezes que todas as APIs no gateway dedicado foram limitadas.	≥0	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1
avg_latency	Latência média	Latência média de todas as APIs no gateway.	≥0 Unidade: ms	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1
max_latency	Máxima latência	Máxima latência de todas as APIs no gateway.	≥0 Unidade: ms	Objeto monitorado: um gateway de API dedicado Dimensão: instance_id	1
req_count	Solicitações	Número de vezes que uma API foi chamada.	≥ 0	Objeto monitorado: uma API Dimensão: api_id	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto e dimensão monitorados	Período de monitoramento (minuto)
req_count_2xx	Respostas 2xx	Número de vezes que a API retorna uma resposta 2xx.	≥ 0	Objeto monitorado: uma API Dimensão: api_id	1
req_count_4xx	Erros 4xx	Número de vezes que a API retorna um erro 4xx.	≥ 0	Objeto monitorado: uma API Dimensão: api_id	1
req_count_5xx	Erros 5xx	Número de vezes que a API retorna um erro 5xx.	≥ 0	Objeto monitorado: uma API Dimensão: api_id	1
req_count_error	Erros totais	Número total de erros retornados pela API.	≥ 0	Objeto monitorado: uma API Dimensão: api_id	1
avg_latency	Latência média	Latência média da API.	≥ 0 Unidade: ms	Objeto monitorado: uma API Dimensão: api_id	1
max_latency	Máxima latência	Máxima latência da API.	≥ 0 Unidade: ms	Objeto monitorado: uma API Dimensão: api_id	1
input_throughput	Tráfego de entrada	Tráfego de entrada da API.	≥ 0 Unidade: byte, KB, MB ou GB	Objeto monitorado: uma API Dimensão: api_id	1

ID da métrica	Nome da métrica	Descrição	Intervalo de valores	Objeto e dimensão monitorados	Período de monitoramento (minuto)
output_throughput	Tráfego de saída	Tráfego de saída da API.	≥ 0 Unidade: byte, KB, MB ou GB	Objeto monitorado: uma API Dimensão: api_id	1

Dimensão

Tabela 6-2 Dimensões de monitoramento

Chave	Valor
instance_id	Gateway dedicado
instance_id,api_id	API

6.1.2 Criação de regras de alarme

Cenário

Você pode criar regras de alarme para monitorar o status de suas APIs.

Uma regra de alarme consiste em um nome de regra, objetos monitorados, métricas, limites de alarme, intervalo de monitoramento e notificação.

Pré-requisitos

Uma API foi chamada.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 Na área **Monitoring** da página da guia **APIs**, clique em **More** para acessar o console do Cloud Eye. Em seguida, crie uma regra de alarme. Para obter detalhes, consulte **Criação de uma regra de alarme**.

----Fim

6.1.3 Exibição de métricas

O Cloud Eye monitora o status de suas APIs e permite que você visualize suas métricas.

Exibição das métricas de uma API

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **API Management** > **API Groups**.

Passo 4 Clique em um nome de grupo.

Passo 5 No painel esquerdo da página de guia **APIs**, selecione uma API.

Passo 6 Exiba métricas da API na área **Monitoring**.

Passo 7 Clique em **View Metric** para exibir mais métricas no console do Cloud Eye.

NOTA

Os dados de monitoramento são mantidos por dois dias. Para reter os dados por um período mais longo, salve-os em um bucket do OBS.

----Fim

Exibição de métricas de um grupo de APIs

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **Monitoring & Analysis** > **API Monitoring**.

Passo 4 Selecione o grupo de APIs de destino e visualize suas métricas.

----Fim

6.2 Monitoramento da largura de banda

O APIG fornece métricas de monitoramento sobre a largura de banda de entrada e saída.

Pré-requisitos

O acesso de entrada e saída foi habilitado para o gateway de destino. Visualize os endereços de entrada e saída nas **informações do gateway**.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **Monitoring & Analysis** > **Bandwidth Monitoring**.

Passo 4 Configure as informações de monitoramento de acordo com a tabela a seguir.

Tabela 6-3 Informações de monitoramento

Parâmetro	Descrição
IP Address	Endereço IP de entrada ou saída de um gateway. Veja o endereço nas **informações do gateway**.
Time range	Selecione **1h**, **3h**, **12h**, **24h** ou **7d**, ou clique em  para especificar um intervalo de tempo personalizado. No canto superior direito de cada gráfico de monitoramento mostra dinamicamente os valores de métrica máxima e mínima no intervalo de tempo especificado.
Auto Refresh	Se essa opção estiver ativada, os dados serão atualizados automaticamente a cada minuto.
Period	Um ciclo quando os dados são agregados para calcular o valor máximo, mínimo, médio, total ou variância.

----Fim

6.3 Análise de logs

Esta seção descreve como analisar os logs de chamadas da API de um gateway.

Pré-requisitos

APIs foram chamadas.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 Selecione um gateway na parte superior do painel de navegação.

Passo 3 No painel de navegação, escolha **Monitoring & Analysis** > **Log Analysis**.

Passo 4 Clique em **Configure Log Collection** e altere **Collect Logs** para  para habilitar a coleta de log.

Passo 5 Especifique um grupo de logs e um fluxo de logs e clique em **OK**. Para obter detalhes sobre grupos de logs e fluxos de logs, consulte **Gerenciamento de logs**.

Passo 6 Clique em **Log Fields** para exibir a descrição de cada campo de log. Em seguida, visualize e analise os logs consultando as descrições dos campos de log.

Passo 7 Para exportar logs, consulte **Transferência de log**.

Os campos nos logs de acesso são separados usando espaços. A tabela a seguir descreve cada campo de log.

Tabela 6-4 Descrição do campo de log

Nº	Campo	Descrição
1	remote_addr	Endereço IP do cliente
2	request_id	ID da solicitação
3	api_id	ID da API
4	user_id	ID do projeto fornecido por um solicitante para autenticação do IAM
5	app_id	ID da aplicação fornecido por um solicitante para autenticação baseada em aplicação
6	time_local	Hora em que uma solicitação é recebida
7	request_time	Latência de solicitação.
8	request_method	Método de solicitação HTTP
9	host	Nome de domínio
10	router_uri	URI de solicitação
11	server_protocol	Protocolo de solicitação
12	status	Código do status da resposta
13	bytes_sent	Tamanho da resposta em bytes, incluindo a linha de status, cabeçalho e corpo.
14	request_length	O comprimento da solicitação em bytes, incluindo a linha inicial, o cabeçalho e o corpo.
15	http_user_agent	ID do agente do usuário
16	http_x_forwarded_for	Campo de cabeçalho X-Forwarded-For
17	upstream_addr	Endereço de back-end
18	upstream_uri	URI de back-end
19	upstream_status	Código de resposta do back-end
20	upstream_connect_time	Tempo necessário para estabelecer uma conexão com o back-end
21	upstream_header_time	Duração desde o início do estabelecimento de uma conexão até o recebimento do primeiro byte do back-end
22	upstream_response_time	Duração desde o início do estabelecimento de uma conexão até o recebimento do último byte do back-end

Nº	Campo	Descrição
23	region_id	ID da região

----Fim

7 Gerenciamento de gateway

7.1 Compra de um gateway

Esta seção descreve como comprar um gateway. Você pode criar APIs e usá-las para fornecer serviços somente após a criação de um gateway.

Para saber sobre as diferenças entre os gateways compartilhados e dedicados, consulte **Especificações**.

Informações sobre a compra de um gateway

Existem algumas limitações na compra de um gateway. Se você não conseguir comprar um gateway ou se um gateway falhar ao ser criado, verifique os seguintes itens:

- Cota de gateway

  Por padrão, sua conta pode ser usada para criar cinco gateways em um projeto. Para criar gateways mais dedicados, envie um tíquete de serviço para aumentar a cota.

- Permissões

  Você deve receber os papéis **APIG Administrator** e **VPC Administrator** ou a política **APIG FullAccess** para comprar um gateway.

  Você também pode receber permissões usando políticas personalizadas. Para mais detalhes, consulte **Políticas personalizadas do APIG**.

- Número de endereços IP privados disponíveis na sub-rede

  As edições básica, profissional, empresarial e platina do APIG requerem 3, 5, 6 e 7 endereços IP privados. Uma platina *X* requer mais 4 endereços IP privados do que a edição anterior. Verifique se a sub-rede escolhida tem endereços IP privados suficientes no console da VPC.

Ambiente de rede

- Carga de trabalho

  Os gateways são implementados em VPCs. Os recursos de nuvem, como Elastic Cloud Servers (ECSs), na mesma carga de trabalho podem chamar APIs usando o endereço IP privado do gateway implementado na carga de trabalho.

  Recomendamos que você implemente seus gateways na mesma carga de trabalho que seus outros serviços para facilitar a configuração da rede e o acesso seguro à rede.

> **NOTA**
>
> As VPCs (cargas de trabalho) nas quais os gateways foram implementados não podem ser alteradas.

- EIP

  Para permitir o acesso público de entrada às APIs implementadas em um gateway, compre um Elastic IP (EIP) e vincule-o ao gateway.

  > **NOTA**
  >
  > Para APIs cujos serviços de back-end são implementados em uma rede pública, o APIG gera automaticamente um endereço IP para acesso público de saída, e você não precisa comprar um Elastic IP (EIP).

- Grupo de segurança

  Semelhante a um firewall, um grupo de segurança controla o acesso a um gateway através de uma porta específica e a transmissão de dados de comunicação do gateway para um endereço de destino específico. Para fins de segurança, crie regras de entrada para o grupo de segurança para permitir o acesso apenas em portas específicas.

  O grupo de segurança vinculado a um gateway deve atender aos seguintes requisitos:

  - Acesso de entrada: para permitir que as APIs no gateway sejam acessadas por redes públicas ou de outros grupos de segurança, adicione regras de entrada para o grupo de segurança para permitir o acesso nas portas 80 (HTTP) e 443 (HTTPS).
  - Acesso de saída: se o serviço de back-end de uma API for implementado numa rede pública ou noutro grupo de segurança, adicione regras de saída para o grupo de segurança para permitir o acesso ao endereço do serviço de back-end através da porta de chamada da API.
  - Se os serviços de front-end e back-end de uma API estiverem vinculados ao mesmo grupo de segurança e VPC que o gateway, nenhuma regra de entrada ou saída será necessária para permitir o acesso por meio das portas anteriores.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Gateways**.

Passo 3 Clique em **Buy Dedicated Gateway**.

> **NOTA**
>
> - Por padrão, o balanceamento de carga com ELB está habilitado para **CN East-Shanghai1**, **CN-Hong Kong**, e **CN Southwest-Guiyang1**.
> - O ELB funciona como um balanceador de carga para gateways, que suportam acesso entre VPCs. Os gateways com acesso público de entrada habilitado recebem um EIP aleatoriamente atribuído e não podem usar um EIP existente.

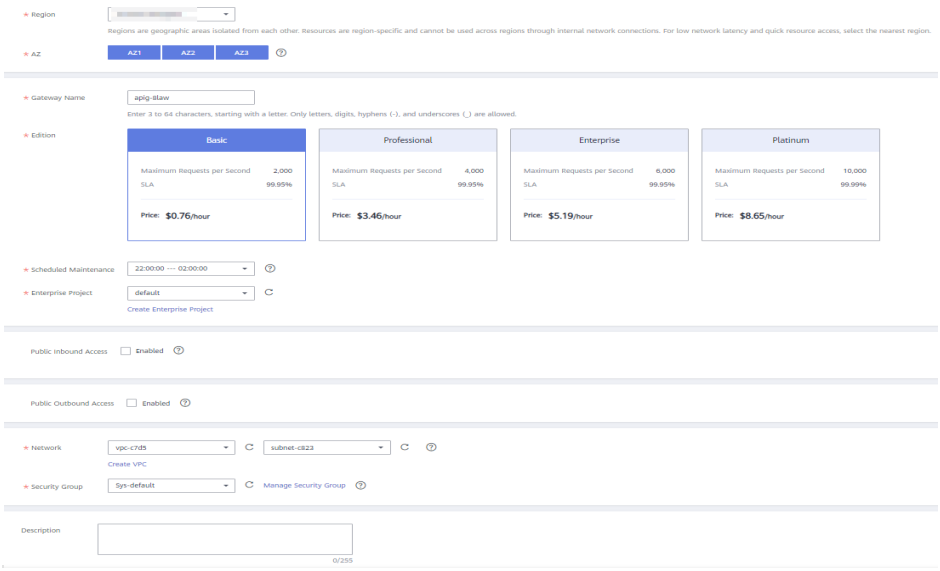


Tabela 7-1 Parâmetros de gateway da API

Parâmetro	Descrição
Billing Mode	Modo de cobrança do gateway dedicado. O pagamento por uso e a cobrança anual/mensal são suportados.
Region	Uma área geográfica onde o gateway será implementado. Implemente o gateway na mesma região que seus outros serviços para permitir que todos os serviços se comuniquem entre si por meio de sub-redes dentro de uma carga de trabalho. Isso reduz os custos de largura de banda pública e a latência da rede.
AZ	Uma região física onde os recursos usam redes e fontes de alimentação independentes. As zonas de disponibilidade (AZs) são fisicamente isoladas, mas interconectadas por meio de uma rede interna. Para aumentar a disponibilidade do gateway, implemente o gateway em várias AZs.
Gateway Name	Nome do gateway.
Edition	As edições básica, profissional, empresarial e platina estão disponíveis. O número de solicitações simultâneas permitidas varia dependendo da edição do gateway. Para obter mais informações, consulte **Especificações** na *Visão geral de serviço do API Gateway*. **NOTA** Atualmente, a edição platina 2 e posterior estão disponíveis apenas em **CN-Hong Kong**.

Parâmetro	Descrição
Scheduled Maintenance	Período de tempo em que o gateway pode ser mantido. O pessoal de suporte técnico entrará em contato com você antes da manutenção. Selecione um período de tempo com baixas demandas de serviço.
Enterprise Project	Selecione um projeto empresarial ao qual o gateway pertence. Este parâmetro só estará disponível se a sua conta for uma conta empresarial. Para obter detalhes sobre o uso de recursos, migração e permissões de usuário de projetos corporativos, consulte **Guia de usuário do Enterprise Management**.
Public Inbound Access	Determine se deve permitir que as APIs criadas no gateway sejam chamadas por serviços externos usando um EIP. Para habilitar essa função, atribua um EIP ao gateway dedicado. Você precisará **pagar** pelo uso do EIP. As APIs no gateway podem ser chamadas usando nomes de domínio independentes ou de depuração. Há uma limitação no número de vezes que as APIs em um grupo de APIs podem ser chamadas por dia usando o nome de domínio de depuração. Para superar a limitação, vincule nomes de domínio independentes ao grupo de APIs e verifique se os nomes de domínio já foram CNAMEd para o EIP do gateway ao qual o grupo de APIs pertence. Por exemplo, você tem uma API HTTPS (caminho: **/apidemo**) com acesso público habilitado. A API pode ser chamada usando "**https://***{domain}*/**apidemo**", onde *domain* indica um nome de domínio independente vinculado ao grupo de APIs ao qual a API pertence. O nome de domínio independente já deve ter sido CNAMEd para o EIP do gateway. A porta padrão é 443.
Public Outbound Access	Determine se os serviços de back-end das APIs criadas no gateway devem ser implementados em redes públicas. Se você ativar essa opção, defina uma largura de banda que atenda aos seus requisitos de serviço. A largura de banda varia de 1 a 2000 Mbit/s e será faturada por hora com base no preço do serviço EIP.
Network	Selecione uma VPC e uma sub-rede para o gateway dedicado. Os recursos de nuvem (como ECSs) dentro da mesma VPC podem chamar APIs usando o endereço IP privado do gateway. Implemente o gateway na mesma VPC que seus outros serviços para facilitar a configuração da rede e proteger o acesso à rede.

Parâmetro	Descrição
Security Group	Selecione um grupo de segurança para controlar o acesso de entrada e saída. Se o serviço de back-end de uma API for implementado em uma rede externa, configure as regras do grupo de segurança para permitir o acesso ao endereço do serviço de back-end por meio da porta de chamada da API. **NOTA** Se o acesso de entrada público estiver habilitado, adicione regras de entrada para o grupo de segurança para permitir o acesso nas portas 80 (HTTP) e 443 (HTTPS).
Required Duration	Defina esse parâmetro somente se você definir **Billing Mode** como **Yearly/Monthly**. A duração mínima é de 1 mês.
Description	Descrição sobre o gateway.

Passo 4 Clique em **Next**.

Passo 5 Se as configurações do gateway estiverem corretas, leia e confirme sua aceitação do contrato de serviço e clique em **Pay Now**.

----Fim

Operações de acompanhamento

Depois que o gateway for criado, você poderá criar e gerenciar APIs nesse gateway. Vá para a página **Gateway Information**. Mostra os detalhes do gateway, as configurações de rede e os parâmetros de configuração.

Você pode modificar o nome do gateway, a descrição, a janela de tempo de manutenção programada, o grupo de segurança e o EIP.

Alterar o modo de cobrança de um gateway

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. O modo de cobrança pode ser alterado de anual/mensal para pagamento por uso somente quando as assinaturas do gateway expirarem.

Passo 1 No painel de navegação, escolha **Gateways**.

Passo 2 Clique em **More** ao lado do gateway de destino e clique em **Change to Yearly/Monthly** ou **Change to Pay-per-Use**.

- Alterar para anual/mensal: selecione uma duração de renovação e clique em **Pay**.
- Alterar para pagamento por uso: clique em **Change to Pay-per-Use** antes que a assinatura do gateway expire ou durante o período congelado após o vencimento. A alteração só entra em vigor depois que a assinatura expirar.

----Fim

7.2 Exibição ou modificação de informações do gateway

Você pode exibir e modificar a configuração de seus gateways no console.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Gateways**.

Passo 3 Clique em **Access Console** ou no nome do gateway de destino.

Passo 4 Na página de guia **Gateway Information**, exiba ou modifique a configuração do gateway.

Tabela 7-2 Informações do gateway

Parâmetro modificável	Descrição
Basic Information	Informações básicas sobre o gateway, incluindo o nome, ID, edição, AZ, descrição, projeto empresarial e janela de tempo de manutenção. ● Modifique as informações básicas conforme necessário. ● Para copiar o ID do gateway, clique em ao lado do ID.
Billing	Modo de cobrança do gateway.
Network	● VPC VPC associado ao gateway. Clique no nome da VPC para exibir a configuração. ● Sub-rede Sub-rede associada ao gateway. Clique no nome da sub-rede para exibir a configuração. ● Grupo de segurança Grupo de segurança associado ao gateway. Clique no nome do grupo de segurança para exibir a configuração ou clique em para vincular um novo.
Inbound Access	● Endereço de acesso da VPC ● EIP EIP vinculado ao gateway. – Para copiar o EIP vinculado, clique em . – Para alterar o EIP vinculado ao gateway, clique em **Change EIP**. – Para desvincular o EIP do gateway, clique em **Unbind EIP**. – Para vincular um EIP ao gateway, clique em **Bind EIP**.

Parâmetro modificável	Descrição
Outbound Access	Determine se os serviços de back-end das APIs criadas no gateway devem ser implementados em redes públicas. Você pode ativar ou desativar o acesso de saída a qualquer momento.
Routes	Segmentos de rede privada. Por padrão, um gateway pode se comunicar com a sub-rede VPC especificada quando o gateway é criado. Se outros segmentos de rede privada precisarem se comunicar com esse gateway, adicione esses segmentos de rede como rotas. Configure rotas em suas instalações se a sub-rede do data center estiver dentro dos três segmentos a seguir: 10.0.0.0/8-24, 172.16.0.0/12-24 e 192.168.0.0/16-24.

----Fim

7.3 Configuração de parâmetros

Esta seção descreve como configurar parâmetros comuns para um gateway para ajustar as funções do componente.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Gateways**.

Passo 3 Clique em **Access Console** ou no nome do gateway de destino.

Passo 4 Clique na guia **Parameters** e clique em **Modify** na linha que contém o parâmetro de destino. Os parâmetros de configuração variam de acordo com a edição do gateway.

Tabela 7-3 Parâmetros de configuração

Parâmetro	Descrição
ratelimit_api_limits	Valor padrão de limitação de solicitação aplicado a todas as APIs. O número total de vezes que uma API pode ser chamada é determinado por esse parâmetro somente se nenhuma política de limitação de solicitações estiver vinculada à API. O **Max. API Requests** de uma política de limitação de solicitações não pode exceder o valor desse parâmetro.
request_body_size	O tamanho máximo do corpo permitido para uma solicitação de API.
backend_timeout	Tempo limite de resposta do back-end. Intervalo de valores: 1 ms para 600.000 ms.

Parâmetro	Descrição
app_token	Determine se a autenticação app_token deve ser ativada. Se você ativar essa função, um access_token poderá ser adicionado à solicitação de autenticação da API. ● **app_token_expire_time**: o período de validade de um access_token. Um novo access_token deve ser obtido antes que o access_token original expire. ● **refresh_token_expire_time**: o período de validade de um refresh_token. Um refresh_token é usado para obter um novo access_token. ● **app_token_uri**: o URI usado para obter um access_token. ● **app_token_key**: a chave de criptografia de um token de acesso.
app_api_key	Determine se a autenticação app_api_key deve ser ativada. Se você habilitar essa função, o parâmetro **apikey** pode ser adicionado à solicitação da API para carregar a chave de uma aplicação (a AppKey de um cliente) para autenticação.
app_basic	Determine se a autenticação app_basic deve ser ativada. Depois que essa opção estiver habilitada, os usuários podem adicionar o parâmetro de cabeçalho **Authorization** e definir o valor do parâmetro como "Basic + base64 (*appkey* + : + *appsecret*)", em que *appkey* e *appsecret* são a chave e o segredo de uma aplicação ou o AppKey e o AppSecret de um cliente.
app_secret	Determine se a autenticação app_secret deve ser ativada. Se você ativar essa função, os parâmetros **X-HW-ID** e **X-HW-AppKey** podem ser adicionados à solicitação da API para transportar a chave e o segredo de uma aplicação (o AppKey e o AppSecret de um cliente) para autenticação. Se você quiser ativar a autenticação app_secret, a autenticação app_api_key deve ser desativada.
app_route	Determine se deve ser compatível com o acesso à API baseado em endereço IP. Se você ativar essa função, as APIs que usam autenticação de aplicação em qualquer grupo, exceto **DEFAULT**, poderão ser chamadas usando endereços IP.
backend_client_certificate	Determine se deve habilitar a autenticação bidirecional de back-end. Se você ativar essa função, poderá configurar a autenticação bidirecional para um back-end ao criar uma API.
ssl_ciphers	Suítes de criptografia HTTPS suportadas. Selecione conjuntos de cifras que atendam aos seus requisitos.

Parâmetro	Descrição
real_ip_from_xff	Determine se os endereços IP devem ser usados no cabeçalho **X-Forwarded-For** para controle de acesso e limitação de solicitação. **xff_index**: número de sequência de um endereço IP no cabeçalho **X-Forwarded-For**. O valor pode ser positivo, negativo ou 0. ● Se o valor for 0 ou positivo, o endereço IP do índice correspondente no cabeçalho **X-Forwarded-For** será obtido. ● Se o valor for negativo, o endereço IP da sequência inversa indicada no cabeçalho **X-Forwarded-For** será obtido. Por exemplo, suponha que o cabeçalho **X-Forwarded-For** de uma solicitação recebida pelo API Gateway contenha três endereços IP: IP1, IP2 e IP3. Se o valor de **xff_index** for 0, IP1 é obtido. Se o valor for 1, IP2 é obtido. Se o valor for -1, IP3 é obtido. Se o valor for -2, IP2 é obtido.
vpc_name_modifiable	Determine se os nomes dos canais de balanceamento de carga podem ser modificados. **AVISO** Se essa opção estiver ativada, os canais de balanceamento de carga do gateway atual não poderão ser gerenciados usando as APIs de gerenciamento de canais de balanceamento de carga no nível do projeto.
api_prom_metrics	Determine se a interface de métricas do Prometheus deve ser ativada. Se esta opção estiver ativada, você pode usar **https://**<*IP do componente de gateway*>**:1026/metrics** para coletar estatísticas de chamadas de API no formato Prometheus.
app_jwt_enable	Determine se a autenticação app_jwt deve ser ativada. Se você ativar essa função, os parâmetros **Authorization** e **Timestamp** podem ser adicionados às solicitações de API para carregar a chave, segredo (o AppKey e AppSecret de um cliente) e carimbo de data/hora de uma aplicação para autenticação. **app_jwt_auth_header** é um cabeçalho incluído nas solicitações de API para autenticação app_jwt. O valor padrão do cabeçalho é **Authorization**.
public_key_enable	Determine se deve habilitar a autenticação public_key. Se você habilitar essa opção, chaves de assinatura do tipo public_key podem ser usadas para autenticação. **public_key_uri_prefix** indica o prefixo do URI usado para obter o segredo de public_key. O formato do URI é o seguinte: **https://***{VPC access address}{public_key_uri_prefix}{public_key name}*.

----Fim

7.4 Gerenciamento de pontos de extremidade da VPC

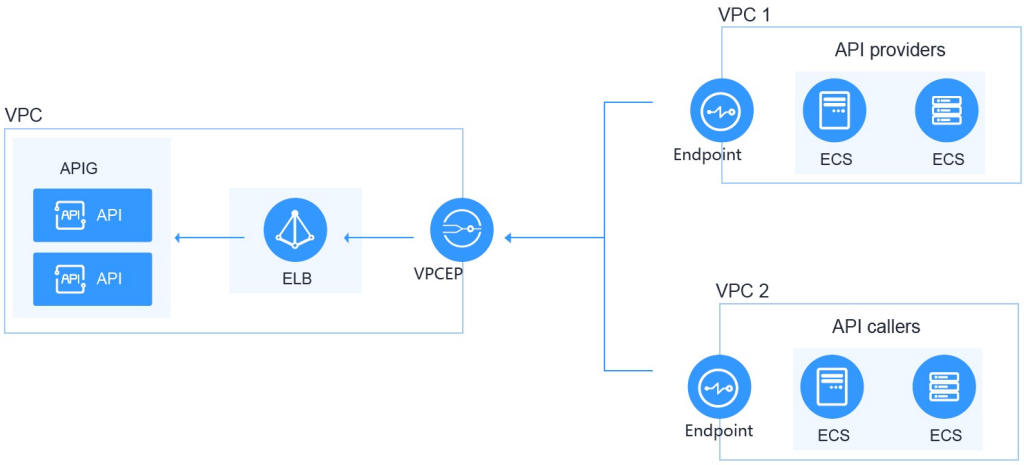
Os pontos de extremidade da VPC são canais seguros e privados para conectar VPCs aos serviços do ponto de extremidade da VPC.

As APIs podem ser expostas e acessadas em VPCs na mesma região da mesma nuvem.

AVISO

Os pontos de extremidade da VPC estão disponíveis apenas nas regiões **CN East-Shanghai1**, **CN-Hong Kong**, e **CN Southwest-Guiyang1**.

Figura 7-1 Acesso entre VPCs na mesma região



Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Gateways**.

Passo 3 Clique em **Access Console** ou no nome do gateway de destino.

Passo 4 Clique em **VPC Endpoints** para exibir os detalhes. Para obter detalhes, consulte **Pontos de extremidade da VPC**.

Tabela 7-4 Informações de ponto de extremidade da VPC

Parâmetro	Descrição
VPC Endpoint Service	Nome do serviço de ponto de extremidade da VPC. Quando você compra um gateway, um serviço de ponto de extremidade da VPC é criado automaticamente e o gateway pode ser acessado usando um ponto de extremidade da VPC.

Parâmetro	Descrição
Connections	Pontos de extremidade da VPC conectados ao gateway. Se você precisar de um novo ponto de extremidade da VPC, clique em **Create VPC Endpoint**. ● **VPC Endpoint ID**: ID de um ponto de extremidade da VPC. ● **Packet ID**: identificador do ID do ponto de extremidade da VPC. ● **Status**: status do ponto de extremidade da VPC. Para obter detalhes sobre os status dos pontos de extremidade da VPC, consulte **Quais são os status dos serviços do ponto de extremidade da VPC e pontos de extremidade da VPC?** ● **Owner**: **ID da conta** do criador do ponto de extremidade da VPC. ● **Created**: hora em que o ponto de extremidade da VPC é criado. ● **Operation**: se permitir que o ponto de extremidade da VPC se conecte ao serviço de ponto de extremidade da VPC. Aceite ou rejeite a conexão do ponto de extremidade da VPC com o serviço do ponto de extremidade da VPC. **AVISO** Depois de rejeitar a conexão, os serviços executados usando a conexão podem ser afetados. Tenha cuidado.
Permissions	Especifique as contas que podem ser acessadas usando os pontos de extremidade da VPC adicionando os IDs de conta à lista branca. Clique em **Add Account** e insira um **ID da conta.** ● **Account ID**: ID de uma conta que pode ser acessada usando os pontos de extremidade da VPC. ● **Created**: hora em que a lista branca é criada. ● **Operation**: gerencie o acesso à conta a partir de pontos de extremidade da VPC. Para proibir o acesso à conta, remova-a da lista branca.

----Fim

7.5 Modificação de especificações

Se as especificações de um gateway não puderem atender aos seus requisitos de serviço, atualize as especificações.

AVISO

- Atualmente, apenas as especificações de gateways com balanceamento de carga baseado em ELB ativado podem ser modificadas nas regiões **CN North-Beijing4**, **CN East-Shanghai1** e **CN South-Guangzhou**.
- As especificações podem ser atualizadas, mas não podem ser reduzidas. As funções de serviço não serão afetadas quando você modificar as especificações.
- Mudar de básica para outra edição altera todos os endereços IP de acesso à rede privada do gateway. Mudar entre outras edições, exceto o básico, gera mais endereços IP de acesso à rede privada para o gateway. Modifique a configuração do firewall ou da lista branca, se necessário, para a continuidade do serviço.

Procedimento

Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Gateways**.

Passo 3 Escolha **More** > **Modify Specifications** à direita do gateway de destino.

Passo 4 Selecione uma edição e clique em **Next**. Para obter detalhes sobre os parâmetros do gateway, consulte **Tabela 7-3**.

Passo 5 Confirme a configuração, leia e confirme a aceitação do contrato de serviço e clique em **Pay Now**. A atualização leva de 15 a 30 minutos para ser concluída.

NOTA

- Para gateways anuais/mensais, pague por taxas extras incorridas pela modificação da especificação.
- Para gateways de pagamento por uso, pague pelo que você usa sem precisar pagar por taxas extras.

----Fim

8 SDKs

O APIG é compatível com autenticação de API baseada em IAM, aplicações e autorizadores personalizados. Você também pode optar por não autenticar solicitações de API. Para obter detalhes sobre as diferenças entre os modos de autenticação, consulte **Como escolher um modo de autenticação**. Esta seção descreve como fazer download de SDKs e visualizar instruções relacionadas.

Cenário

Os SDKs são usados quando você chama APIs por meio da autenticação da aplicação. Faça o download dos SDKs e da documentação relacionada e, em seguida, chame as APIs seguindo as instruções da documentação.

Procedimento

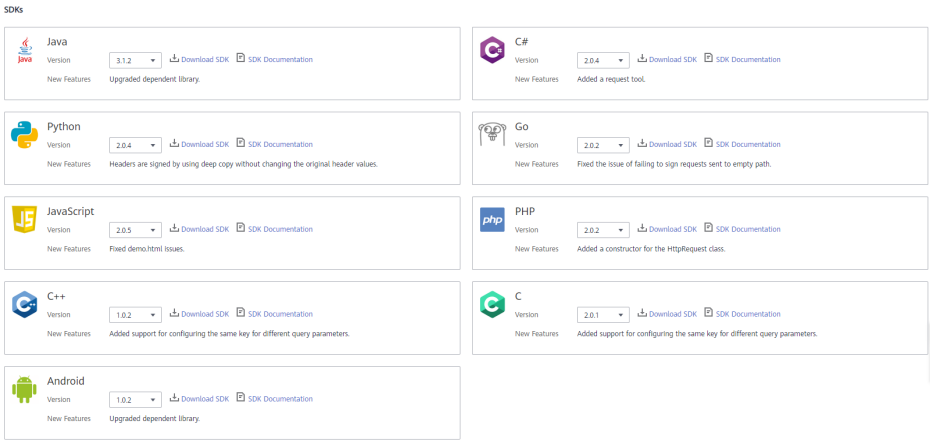
Passo 1 **Faça logon no console do APIG.**

Passo 2 No painel de navegação, escolha **Help Center**.

Passo 3 Clique em **Using SDKs**.

Passo 4 Clique em **Download SDK** ao lado da linguagem desejada. Um SDK contém código SDK e código de exemplo. Os SDKs variam de acordo com a linguagem.

Para ver o guia de suporte, clique em **SDK Documentation**.



----Fim

9 Chamada de API publicada

9.1 Chamada das APIs

Obtenção de APIs e documentação

Antes de chamar as APIs, obtenha as informações de solicitação do provedor da API, incluindo os parâmetros de nome de domínio de acesso, protocolo, método, caminho e solicitação.

Obtenha APIs da sua empresa ou de um parceiro.

Para APIs obtidas da Huawei Cloud, obtenha documentação na **Central de ajuda**.

As informações de autenticação a serem obtidas variam com o modo de autenticação da API.

- Autenticação de aplicação:
  - Autenticação de assinatura: obtenha a chave e o segredo (ou AppKey e AppSecret do cliente) da aplicação autorizada para a API do provedor de API, bem como o SDK para chamar a API.
  - Autenticação simples: obtenha o AppCode da aplicação autorizada para a API do provedor de API.
  - Outros modos de autenticação: obtenha a chave e o segredo (ou AppKey e AppSecret do cliente) da aplicação autorizada para a API do provedor de API.
- Autenticação do IAM: a credencial da conta (token ou AK/SK obtido com a conta e a senha) obtida na plataforma de serviço em nuvem é usada para autenticação. Se o AK/SK for usado para autenticação, você também precisará obter o SDK do provedor da API para chamar a API.
- Autenticação personalizada: obtenha as informações de autenticação personalizadas a serem transportadas nos parâmetros de solicitação do provedor de API.
- Nenhum: nenhuma informação de autenticação é necessária.

Chamar uma API

> **NOTA**
>
> Esta seção descreve somente a configuração do caminho da solicitação e dos parâmetros de autenticação. Para outros parâmetros, como tempo limite e SSL, configure-os conforme necessário. Para evitar perdas de serviço devido a parâmetros incorretos, configure-os consultando os padrões da indústria.

Passo 1 Defina o caminho da solicitação.

Cenário	Configuração de parâmetros de solicitação
Chamar uma API com um nome de domínio	Chame uma API usando o nome de domínio de depuração alocado ao grupo de APIs ou um nome de domínio vinculado ao grupo. Não é necessária configuração adicional.
Chamar uma API no grupo **DEFAULT** com um endereço IP	Chame uma API no grupo **DEFAULT** com um endereço IP. Não é necessária configuração adicional.
Chamar uma API em um grupo personalizado com um endereço IP	● Para chamar APIs usando um endereço IP, verifique se o parâmetro **app_route** foi definido como **on** na página de guia **Parâmetros** do gateway. ● Para usar um endereço IP para chamar uma API que usa autenticação de aplicação em um grupo não-DEFAULT, adicione os parâmetros de cabeçalho **X-HW-ID** e **X-HW-APPKEY** e defina os valores de parâmetro para a chave e o segredo de uma aplicação autorizada para a API ou um AppKey e AppSecret do cliente. ● Para usar um endereço IP para chamar uma API que não usa autenticação de aplicação em um grupo que não é DEFAULT, adicione o parâmetro de cabeçalho **host**.

Passo 2 Defina os parâmetros de autenticação.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação de aplicação (com uma assinatura)	Use o SDK para assinar solicitações de API. Para obter detalhes, consulte **Chamar APIs por meio de autenticação de aplicação**.
Autenticação de aplicação (através de autenticação simples)	Adicione o parâmetro de cabeçalho **X-Apig-AppCode** e defina o valor do parâmetro para o AppCode obtido em **Obtenção de APIs e documentação**. Para obter detalhes, consulte **Primeiros passos**.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação de aplicação (com app_api_key)	● Para ativar a autenticação app_api_key, verifique se o parâmetro **app_api_key** foi definido como **on** na página de guia **Parâmetros** do gateway. ● Adicione o parâmetro **apikey** do cabeçalho ou da cadeia de consulta e defina o valor do parâmetro para a chave ou AppKey obtida em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_secret)	● Na página de guia **Parâmetros** de um gateway, o parâmetro **app_secret** foi definido como **on** para ativar a autenticação app_secret e **app_api_key** como **off** para desativar a autenticação app_api_key. ● Adicione o parâmetro **X-HW-ID** do cabeçalho e defina o valor do parâmetro como a chave da aplicação autorizada para a API ou o AppKey do cliente. ● Adicione o parâmetro de cabeçalho **X-HW-AppKey** e defina o valor do parâmetro para o segredo ou AppSecret obtido em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_basic)	● Para habilitar a autenticação app_basic, verifique se o parâmetro **app_basic** foi definido como **on** na página de guia **Parâmetros** do gateway. ● Adicione o parâmetro de cabeçalho **Authorization** e defina o valor do parâmetro como "Basic + base64 (*appkey* + : + *appsecret*)", em que *appkey* e *appsecret* são a chave e o segredo (ou AppKey e AppSecret) obtidos em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_jwt)	● Para habilitar a autenticação app_jwt, verifique se o parâmetro **app_jwt** foi definido como **on** na página de guia **Parâmetros** do gateway. ● Adicione o parâmetro de cabeçalho **Timestamp** e defina o valor do parâmetro para o carimbo de data/hora Unix da hora atual. ● Adicione o parâmetro de cabeçalho **Authorization** e defina o valor do parâmetro como "sha256 (*appkey* + *appsecret* + *timestamp*)", no qual *appkey* e *appsecret* são a chave e segredo (ou AppKey e AppSecret) obtidos em **Obtenção de APIs e documentação** e *carimbo de data/hora* é o carimbo de data/hora Unix da hora atual.
Autenticação do IAM (com um token)	Obtenha um token da plataforma de nuvem e transporte o token em solicitações de API para autenticação. Para obter detalhes, consulte **Autenticação de token**.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação do IAM (com AK/SK)	Use um SDK para assinar solicitações de API. Para obter detalhes, consulte **Autenticação de AK/SK**.
Autenticação personalizada	Carregue informações de autenticação em parâmetros de solicitação de API para autenticação.
Nenhum	Chamar APIs sem autenticação.

----Fim

9.2 Cabeçalhos de resposta

A tabela a seguir descreve os cabeçalhos de resposta que o APIG adiciona à resposta retornada quando uma API é chamada.

X-Apig-Mode: debug indica informações de depuração da API.

Cabeçalho de resposta	Descrição	Observações
X-Request-Id	ID de solicitação.	Retornado para todos as solicitações válidas.
X-Apig-Latency	Duração desde o momento em que o APIG recebe uma solicitação até o momento em que o back-end retorna um cabeçalho da mensagem.	Retornado somente quando o cabeçalho da requisição contém **X-Apig-Mode: debug**.
X-Apig-Upstream-Latency	Duração desde o momento em que o APIG envia uma solicitação para o back-end até o momento em que o back-end retorna um cabeçalho de mensagem.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e o tipo de back-end não é Mock.
X-Apig-RateLimit-api	Informações de limite de solicitação de API. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada.
X-Apig-RateLimit-user	Informações de limite de solicitação do usuário. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por um usuário.

Cabeçalho de resposta	Descrição	Observações
X-Apig-RateLimit-app	Informações de limite de solicitação de aplicação. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por uma aplicação.
X-Apig-RateLimit-ip	Informações de limite de solicitação de endereço IP. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por um endereço IP.
X-Apig-RateLimit-api-allenv	Informações de limite de solicitação de API padrão. Exemplo: **remain:199,limit:200,time:1 second**.	Retornado somente quando o cabeçalho da requisição contém **X-Apig-Mode: debug**.

9.3 Códigos de erro

A **Tabela 9-1** lista os códigos de erro que você pode encontrar ao chamar APIs. Se um código de erro começando com **APIGW** for retornado após chamar uma API, corrija a falha consultando as instruções fornecidas em **Códigos de erro**.

NOTA

- Para obter detalhes sobre os códigos de erro que podem ocorrer quando você gerencia APIs, consulte **Códigos de erro**.
- Se ocorrer um erro ao usar APIG, localize a mensagem de erro e a descrição na tabela a seguir de acordo com o código de erro, por exemplo, APIG.0101. As mensagens de erro estão sujeitas a alterações sem aviso prévio.

Tabela 9-1 Códigos de erro

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0101	A API não existe ou não foi publicada no ambiente.	404	A API não existe ou não foi publicada no ambiente.	Verifique se o nome de domínio, o método e o caminho são consistentes com os da API registrada. Verifique se a API foi publicada. Se tiver sido publicado em um ambiente que não seja de produção, verifique se o cabeçalho X-Stage na solicitação é o nome do ambiente. Verifique se o nome de domínio usado para chamar a API foi vinculado ao grupo ao qual a API pertence.
APIG.0101	A API não existe.	404	O método de solicitação da API não existe.	Verifique se o método de solicitação da API é o mesmo que o método definido pela API.
APIG.0103	O back-end não existe.	500	O serviço de back-end não foi encontrado.	Entre em contato com o suporte técnico.
APIG.0104	Os plug-ins não existem.	500	Nenhuma configuração de plug-in foi encontrada.	Entre em contato com o suporte técnico.
APIG.0105	As configurações de back-end não existem.	500	Nenhuma configuração de back-end foi encontrada.	Entre em contato com o suporte técnico.
APIG.0106	Erro de orquestração.	400	Ocorreu um erro de orquestração.	Verifique se os parâmetros front-end e back-end da API estão corretos.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0201	Erro de solicitação da API.	400	Parâmetros de solicitação inválidos.	Defina parâmetros de solicitação válidos.
APIG.0201	Entidade de solicitação muito grande.	413	O corpo da solicitação excede 12 MB.	Reduza o tamanho do corpo da solicitação.
APIG.0201	URI de solicitação muito grande.	414	O URI da solicitação excede 32 KB.	Reduza o tamanho do URI da solicitação.
APIG.0201	Cabeçalhos de solicitação muito grandes.	494	Os cabeçalhos de solicitação são muito grandes porque um deles excede 32 KB ou o comprimento total excede 128 KB.	Reduza o tamanho dos cabeçalhos da solicitação.
APIG.0201	Back-end indisponível.	502	O serviço de back-end não está disponível.	Verifique se o endereço de back-end configurado para a API está acessível.
APIG.0201	Tempo limite de back-end.	504	O serviço de back-end expirou o tempo limite.	Aumente a duração do tempo limite do serviço de back-end ou reduza o tempo de processamento.
APIG.0201	Um erro inesperado ocorreu	500	Ocorreu um erro interno.	Entre em contato com o suporte técnico.
APIG.0202	Back-end indisponível	502	O back-end não está disponível.	Verifique se o protocolo de solicitação de back-end configurado para a API é o mesmo que o protocolo de solicitação usado pelo serviço de back-end.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0204	O protocolo SSL não é suportado: TLSv1.1	400	A versão do protocolo SSL não é suportada.	Use uma versão suportada do protocolo SSL.
APIG.0301	Informações incorretas de autenticação do IAM.	401	Os detalhes de autenticação do IAM estão incorretos.	Verifique se o token está correto.
APIG.0302	O usuário do IAM não está autorizado a acessar a API.	403	O usuário do IAM não tem permissão para acessar a API.	Verifique se o usuário é controlado por uma lista negra ou lista branca.
APIG.0303	Informações de autenticação da aplicação incorretas.	401	Os detalhes de autenticação da aplicação estão incorretos.	Verifique se o método de solicitação, caminho, cadeia de consulta e corpo da solicitação são consistentes com os usados para assinatura; verifique se a data e a hora no cliente estão corretas; e verifique se o código de assinatura está correto, referindo-se a **Chamar APIs por meio de autenticação de aplicação**.
APIG.0304	A aplicação não está autorizado a acessar a API.	403	A aplicação não tem permissão para acessar a API.	Verifique se a aplicação foi autorizada a acessar a API.
APIG.0305	Informações de autenticação incorretas.	401	As informações de autenticação estão incorretas.	Verifique se as informações de autenticação estão corretas.
APIG.0306	Acesso à API negado.	403	O acesso à API não é permitido.	Verifique se você foi autorizado a acessar a API.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0307	O token deve ser atualizado.	401	O token precisa ser atualizado.	Obtenha um novo token do IAM.
APIG.0308	O limite de limitação foi atingido.	429	O limite de limitação foi atingido.	Tente novamente depois que a limitação for retomada. Se o número de solicitações de domínio de depuração por dia for atingido, vincule um nome de domínio independente ao serviço ao qual a API pertence.
APIG.0310	O projeto não está disponível.	403	O projeto está indisponível no momento.	Selecione outro projeto e tente novamente.
APIG.0311	Informações de autenticação de depuração incorretas.	401	Os detalhes de autenticação de depuração estão incorretos.	Entre em contato com o suporte técnico.
APIG.0401	Endereço IP do cliente desconhecido.	403	O endereço IP do cliente não pode ser identificado.	Entre em contato com o suporte técnico.
APIG.0402	O endereço IP não está autorizado para acessar a API.	403	O endereço IP não tem permissão para acessar a API.	Verifique se o endereço IP é controlado por uma lista negra ou lista branca.
APIG.0404	O acesso ao endereço IP de back-end foi negado.	403	O endereço IP do back-end não pode ser acessado.	Verifique se o endereço IP do back-end ou o endereço IP correspondente ao nome de domínio do back-end está acessível.
APIG.0501	A cota da aplicação foi usada.	405	A cota da aplicação foi atingida.	Aumentar a cota da aplicação.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0502	A aplicação foi congelada.	405	A aplicação foi congelada.	Verifique se o saldo da sua conta é suficiente.
APIG.0601	Erro de servidor interno.	500	Ocorreu um erro interno.	Entre em contato com o suporte técnico.
APIG.0602	Solicitação inválida.	400	Pedido inválido.	Verifique se a solicitação é válida.
APIG.0605	Falha na resolução do nome de domínio.	500	Falha na resolução do nome de domínio.	Verifique se o nome de domínio está correto e foi vinculado a um endereço de back-end correto.
APIG.0606	Falha ao carregar as configurações da API.	500	As configurações da API não puderam ser carregadas.	Entre em contato com o suporte técnico.
APIG.0607	O seguinte protocolo é suportado: {xxx}	400	O protocolo não é suportado. Somente *xxx* é suportado. *xxx* está sujeito ao valor real na resposta.	Use HTTP ou HTTPS para acessar a API.
APIG.0608	Falha ao obter o token de administrador.	500	Os detalhes da conta de administrador não podem ser obtidos.	Entre em contato com o suporte técnico.
APIG.0609	O back-end da VPC não existe.	500	O serviço de back-end da carga de trabalho não pode ser encontrado.	Entre em contato com o suporte técnico.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0610	Nenhum back-end disponível.	502	Não há serviços de back-end disponíveis.	Verifique se todos os serviços de back-end estão disponíveis. Por exemplo, verifique se as informações de chamada da API são consistentes com a configuração real.
APIG.0611	A porta de back-end não existe.	500	A porta de back-end não foi encontrada.	Entre em contato com o suporte técnico.
APIG.0612	Uma API não pode chamar a si mesma.	500	Uma API não pode chamar a si mesma.	Modifique as configurações de back-end e garanta que o número de camadas que a API é chamada recursivamente não exceda 10.
APIG.0613	O serviço IAM não está disponível no momento.	503	O IAM não está disponível no momento.	Entre em contato com o suporte técnico.
APIG.0705	Falha no cálculo da assinatura de back-end.	500	Falha no cálculo da assinatura de back-end.	Entre em contato com o suporte técnico.
APIG.0802	O usuário do IAM é proibido na região selecionada no momento	403	O usuário do IAM está desativado na região atual.	Entre em contato com o suporte técnico.
APIG.1009	AppKey e AppSecret são inválidos	400	O AppKey e o AppSecret são inválidos.	Verifique se o AppKey e o AppSecret da solicitação estão corretos.

10 Gerenciamento de permissões

10.1 Criação de um usuário e concessão de permissões do APIG

Este tópico descreve como usar **Identity and Access Management** (IAM) para implementar o controle de permissões refinado para seus recursos do APIG. Com o IAM, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos do APIG.
- Conceder somente as permissões necessárias para que os usuários executem uma tarefa específica.
- Confiar outra conta ou serviço de nuvem para executar O&M em seus recursos do APIG.

Se sua conta da HUAWEI CLOUD não exigir usuários individuais do IAM, pule este capítulo.

Esta seção descreve o procedimento para conceder permissões (consulte **Figura 10-1**).

Pré-requisitos

Saiba mais sobre as permissões (consulte **Tabela 10-1**) suportadas pelo APIG e escolha políticas ou funções de acordo com seus requisitos. Para obter as permissões de outros serviços, consulte **Permissões do sistema**.

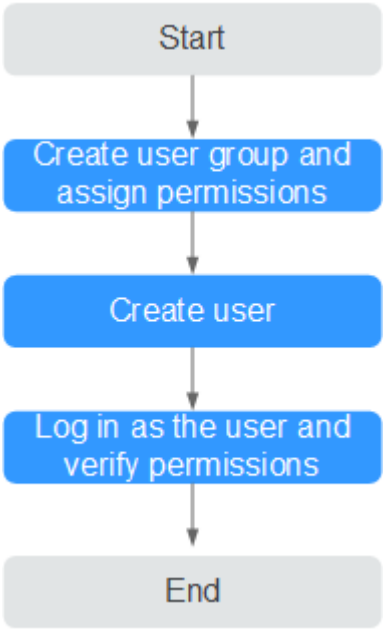
Tabela 10-1 Funções e políticas definidas pelo sistema suportadas pelo APIG

Nome da função/ política	Descrição	Tipo	Dependência
APIG Administrator	Permissões de administrador para APIG. Os usuários com essas permissões podem usar todas as funções do APIG.	Função definida pelo sistema	Nenhuma

Nome da função/ política	Descrição	Tipo	Dependência
APIG FullAccess	Permissões completas para APIG. Os usuários com essas permissões podem usar todas as funções do APIG.	Política definida pelo sistema	Nenhuma
APIG ReadOnlyAccess	Permissões somente leitura para APIG. Os usuários que receberam essas permissões podem apenas visualizar o APIG.	Política definida pelo sistema	Nenhuma

Fluxo do processo

Figura 10-1 Processo para conceder permissões do APIG



1. **Crie um grupo de usuários e atribua permissões** a ele.

   Crie um grupo de usuários no console do IAM e anexe o papel de **APIG Administrator** ou a política de **APIG FullAccess** ao grupo.

2. **Crie um usuário do IAM**.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.

3. **Faça logon** e verifique as permissões.

   Faça logon no console do APIG como o usuário criado e verifique se o usuário tem permissões de administrador para o APIG.

10.2 Políticas personalizadas do APIG

As políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema do APIG. Para as ações que podem ser adicionadas às políticas personalizadas, consulte **Políticas de permissões e ações suportadas**.

Você pode criar políticas personalizadas usando um dos seguintes métodos:

- Editor visual: selecione serviços em nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe de política.
- JSON: edite políticas de JSON do rascunho ou com base em uma política existente.

Para obter detalhes, consulte **Criação de uma política personalizada**. A seção a seguir contém exemplos de políticas customizadas APIG comuns.

Exemplo de políticas personalizadas

- Exemplo 1: permitir que os usuários criem e depurem APIs

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    apig:apis:create
                    apig:apis:debug
                 "
            ]
        }
    ]
}
```

- Exemplo 2: negar criação de grupo de API

  Uma política com apenas permissões "Deny" deve ser usada em conjunto com outras políticas para entrar em vigor. Se as permissões atribuídas a um usuário contiverem "Allow" e "Deny", as permissões "Deny" terão precedência sobre as permissões "Allow".

  O método a seguir pode ser usado se você precisar atribuir permissões da política **APIG FullAccess** a um usuário, mas quiser impedir que o usuário crie grupos de API. Crie uma política personalizada para negar a criação de grupo de API e anexe ambas as políticas ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações em gateways de API, exceto a criação de grupos de API. O seguinte é um exemplo de uma política de negação:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    apig:apis:create
                    apig:apis:debug
                 "
            ]
        }
    ]
}
```


11 Auditoria

11.1 Operações do APIG registradas pelo CTS

Ativação de CTS

Se você quiser coletar, registrar ou consultar logs de operação para APIG em cenários comuns, como análise de segurança, auditoria e localização de problemas, **habilite o Cloud Trace Service (CTS)**.

O CTS fornece as seguintes funções:

- Gravação de logs de auditoria
- Consulta de logs de auditoria
- Despejo de logs de auditoria
- Criptografia de arquivos de rastreamento
- Ativação de notificações de operações-chave

Exibição de operações principais

Com o CTS, você pode registrar operações associadas ao APIG para consultas futuras, auditorias e rastreamento inverso.

Tabela 11-1 Operações do APIG registradas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criação de um grupo de API	ApiGroup	createApiGroup
Exclusão de um grupo de API	ApiGroup	deleteApiGroup
Atualização de um grupo de API	ApiGroup	updateApiGroup
Vinculação de um nome de domínio	ApiGroup	createDomainBinding

Operação	Tipo de recurso	Nome do rastreamento
Alteração da versão mínima do TLS	ApiGroup	modifySecureTransmission
Desvinculação de um nome de domínio	ApiGroup	relieveDomainBinding
Adição de um certificado de domínio	ApiGroup	addDomainCertificate
Exclusão de um certificado de domínio	ApiGroup	deleteDomainCertificate
Criação de uma API	Api	createApi
Exclusão de uma API	Api	deleteApi
Exclusão de várias APIs	Api	batchDeleteApi
Atualização de uma API	Api	updateApi
Publicação de uma API	Api	publishApi
Deixar uma API off-line	Api	offlineApi
Publicar várias APIs ou deixar APIs off-line	Api	batchPublishOrOfflineApi
Alternação de versões da API	Api	switchApiVersion
Deixar uma versão da API off-line	Api	offlineApiByVersion
Depuração de uma API	Api	debugApi
Criação de um ambiente	Environment	createEnvironment
Exclusão de um ambiente	Environment	deleteEnvironment
Atualização de um ambiente	Environment	updateEnvironment
Criação de uma variável de ambiente	EnvVariable	createEnvVariable
Atualização de uma variável de ambiente	EnvVariable	updateEnvVariable
Exclusão de uma variável de ambiente	EnvVariable	deleteEnvVariable
Criação de uma aplicação	App	createApp
Exclusão de uma aplicação	App	deleteApp
Atualização de uma aplicação	App	updateApp

Operação	Tipo de recurso	Nome do rastreamento
Redefinição do AppSecret	App	resetAppSecret
Vinculação de um cliente a uma API	AppAuth	grantAuth
Desvinculação de um cliente de uma API	AppAuth	relieveAuth
Criação de uma chave de assinatura	Signature	createSignature
Exclusão de uma chave de assinatura	Signature	deleteSignature
Atualização de uma chave de assinatura	Signature	updateSignature
Vinculação de uma chave de assinatura	SignatureBinding	createSignatureBinding
Desvinculação de uma chave de assinatura	SignatureBinding	relieveSignatureBinding
Criação de uma política de controle de acesso	Acl	createAcl
Exclusão de uma política de controle de acesso	Acl	deleteAcl
Exclusão de políticas de controle de acesso	Acl	batchDeleteAcl
Atualização de uma política de controle de acesso	Acl	updateAcl
Criação de uma lista negra de controle de acesso	Acl	addAclValue
Exclusão de uma lista negra de controle de acesso	Acl	deleteAclValue
Vinculação de uma política de controle de acesso a uma API	AclBinding	createAclBinding
Desvinculação de uma política de controle de acesso de uma API	AclBinding	relieveAclBinding
Desvinculação de várias políticas de controle de acesso de APIs	AclBinding	batchRelieveAclBinding
Criação de uma política de limitação de solicitações	Throttle	createThrottle

Operação	Tipo de recurso	Nome do rastreamento
Exclusão de uma política de limitação de solicitações	Throttle	deleteThrottle
Exclusão de várias políticas de limitação de solicitações	Throttle	batchDeleteThrottle
Atualização de uma política de limitação de solicitações	Throttle	updateThrottle
Vinculação de uma política de limitação de solicitações	ThrottleBinding	createThrottleBinding
Desvinculação de uma política de limitação de solicitações	ThrottleBinding	relieveThrottleBinding
Desvinculação de várias políticas de limitação de solicitações	ThrottleBinding	batchRelieveThrottleBinding
Criação de uma configuração de limitação de solicitação excluída	ThrottleSpecial	createSpecialThrottle
Exclusão de uma configuração de limitação de solicitação excluída	ThrottleSpecial	deleteSpecialThrottle
Atualização de uma configuração de limitação de solicitação excluída	ThrottleSpecial	updateSpecialThrottle
Criação de um canal de balanceamento de carga	Vpc	createVpc
Exclusão de um canal de balanceamento de carga	Vpc	deleteVpc
Atualização de um canal de balanceamento de carga	Vpc	updateVpc
Adição de membros a um canal de balanceamento de carga	Vpc	addVpcMember
Exclusão de membros de um canal de balanceamento de carga	Vpc	deleteVpcMember
Exportação de uma API	Swagger	swaggerExportApi
Exportação de várias APIs	Swagger	swaggerExportApiList
Exportação de todas as APIs em um grupo	Swagger	swaggerExportApiByGroup

Operação	Tipo de recurso	Nome do rastreamento
Importação de APIs para um novo grupo	Swagger	swaggerImportApiTo-NewGroup
Importação de APIs para um grupo existente	Swagger	swaggerImportApiToEx-istGroup
Exportação de todos os back-ends personalizados	Swagger	SwaggerExportLdApi
Importação de back-ends personalizados	Swagger	SwaggerImportLdApi
Criação de um autorizador personalizado	Authorizer	createAuthorizer
Exclusão de um autorizador personalizado	Authorizer	deleteAuthorizer
Atualização de um autorizador personalizado	Authorizer	updateAuthorizer
Criação de um plug-in	Plugin	createPlugin
Atualização de um plug-in	Plugin	updatePlugin
Exclusão de um plug-in	Plugin	deletePlugin
Vinculação de um plug-in a uma API	Plugin	pluginAttachApi
Desvinculação de uma API de um plug-in	Plugin	pluginDetachApi
Vinculação de um plug-in a uma API	Plugin	apiAttachPlugin
Desvinculação de um plug-in de uma API	Plugin	apiDetachPlugin

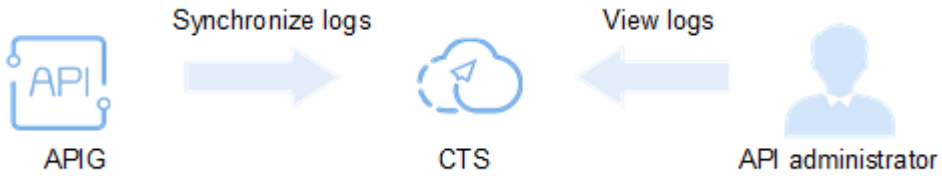
Desativação de CTS

Desabilite o CTS seguindo o procedimento em **Exclusão de um rastreador**.

11.2 Consulta de logs de auditoria

Consultar logs de auditoria seguindo o procedimento em **Consulta de rastreamentos em tempo real**.

Figura 11-1 Visualização de logs



12 Console antigo

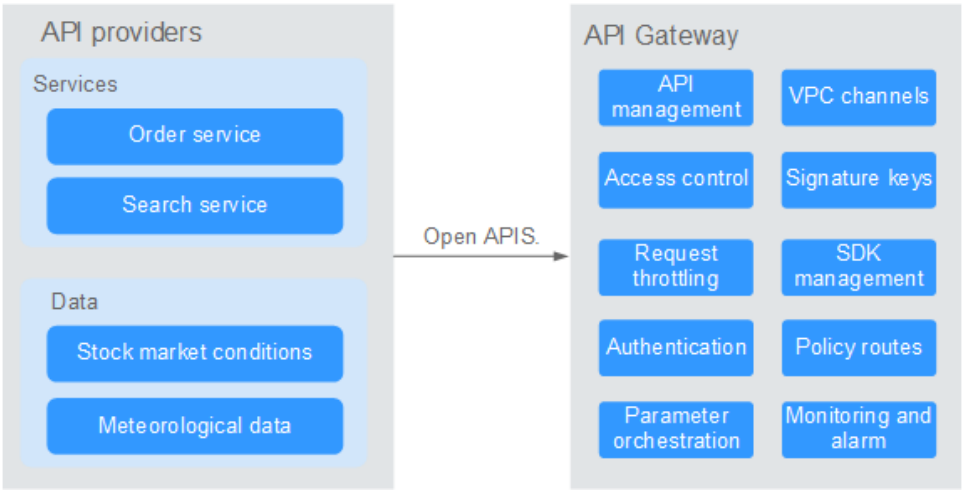
12.1 Visão geral

O API Gateway (APIG) é um serviço totalmente gerenciado que permite criar, gerenciar e implementar APIs com segurança em qualquer escala com alto desempenho e disponibilidade. Com o APIG, você pode facilmente integrar seus sistemas de serviços internos e expor seletivamente seus recursos de serviço por meio de suas funções de abertura e chamada de API.

- **Abertura da API**

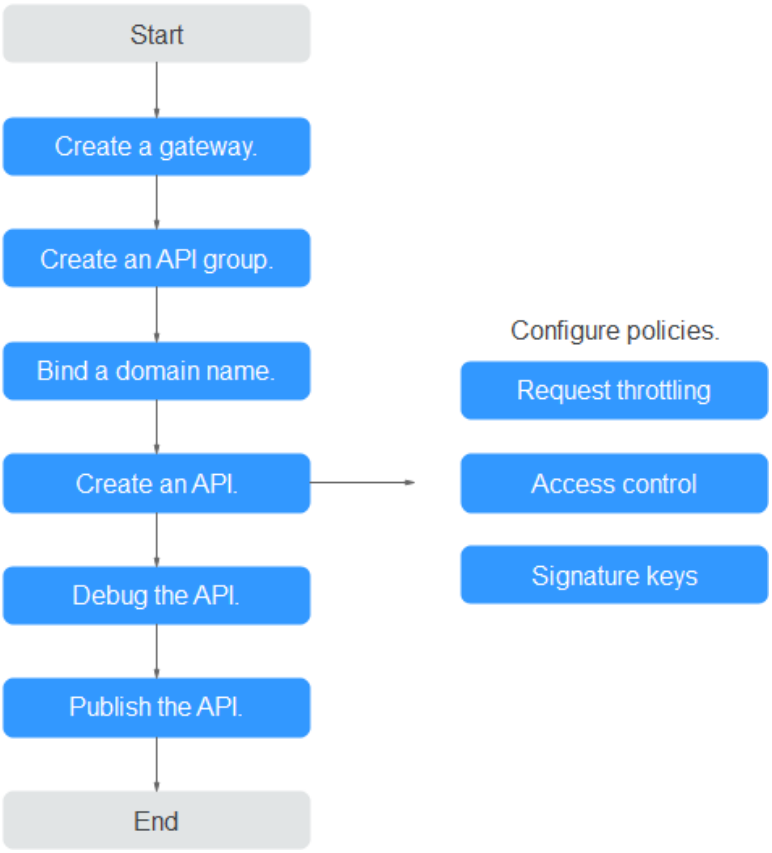
  Empresas e desenvolvedores expõem seletivamente seus serviços e dados através do APIG.

  Figura 12-1 Abertura da API



A figura a seguir mostra o processo de abertura da API.

Figura 12-2 Processo de abertura da API



a. Crie um gateway.

Compre um gateway dedicado.

Como alternativa, use o **gateway compartilhado**.

b. **Crie um grupo de APIs**.

Cada API pertence a um grupo de APIs. Crie um grupo antes de criar uma API.

c. **Vincule um nome de domínio**.

Antes de expor uma API, associe um nome de domínio independente ao grupo para que os usuários possam acessar a API.

Você pode depurar a API usando o nome de subdomínio padrão alocado ao grupo ao qual a API pertence. O nome do subdomínio pode ser chamado no máximo 1.000 vezes por dia.

d. **Crie uma API**.

Encapsule os serviços de back-end existentes em APIs RESTful padrão e os exponha a sistemas externos.

Depois de criar uma API, defina as seguintes configurações para controlar o acesso à API:

- **Limitação de solicitação**

  Defina o número máximo de vezes que a API pode ser chamada dentro de um período de tempo para proteger serviços de back-end.

- **Controle de acesso**

Defina uma lista negra ou lista branca para negar ou permitir acesso à API de endereços IP ou contas específicas.

- **Chaves de assinatura**

  As chaves de assinatura são usadas pelos serviços de back-end para verificar a identidade do APIG e garantir o acesso seguro.

e. **Depure a API**.

Verifique se a API está funcionando normalmente.

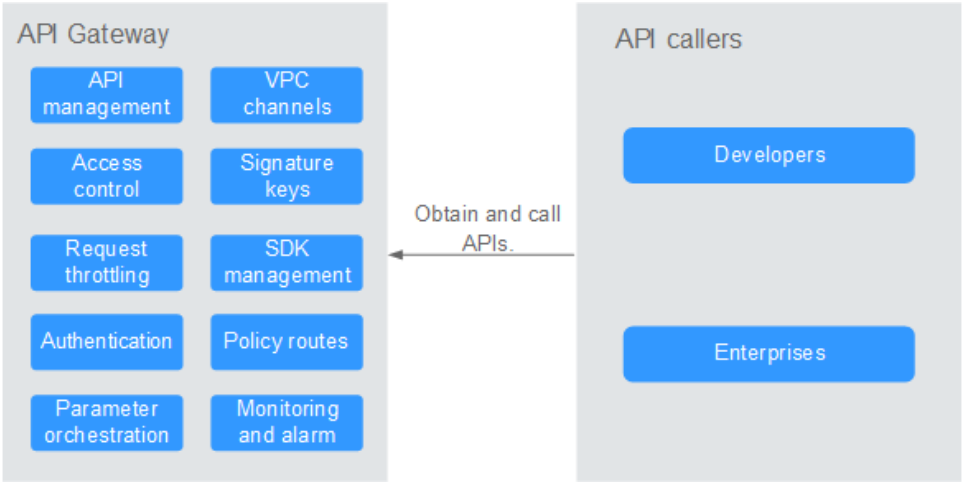
f. **Publique a API**.

A API só pode ser chamada depois de ter sido publicada em um ambiente.

- **Chamada da API**

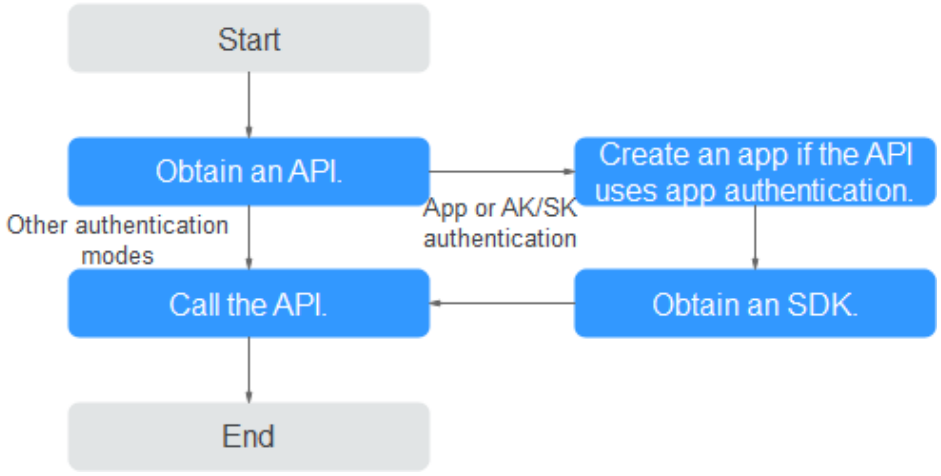
Empresas e desenvolvedores obtêm e chamam APIs de outros provedores, reduzindo assim o tempo e os custos de desenvolvimento.

Figura 12-3 Chamada de API



A figura a seguir mostra o processo de chamada da API.

Figura 12-4 Processo de chamada da API



a. **Obtenha uma API**.

Obtenha as informações de solicitação da API, incluindo o nome de domínio, o protocolo, o método, o caminho e o modo de autenticação.

b. **Crie uma aplicação**.

   Para uma API que usa autenticação de aplicação, crie uma aplicação para gerar um AppKey e um AppSecret. Vincule a aplicação à API para que você possa chamar a API por meio da autenticação da aplicação.

c. **Obtenha um SDK**.

   Use o SDK para gerar uma assinatura para a AK/SK e chamar a API.

d. **Chame a API**.

   Obtenha a API usando seu endereço de acesso e execute a autenticação com base em seu modo de autenticação.

12.2 Gerenciamento de gateway

12.2.1 Compra de um gateway dedicado

Esta seção descreve como comprar um gateway dedicado. Você pode criar APIs e usá-las para fornecer serviços somente após a criação de um gateway dedicado. Se você não tiver requisitos de alto desempenho, pule esta seção e use o gateway compartilhado para **criar e gerenciar APIs**.

Para saber sobre as diferenças entre os gateways compartilhados e dedicados, consulte **Especificações**.

Informações sobre como comprar um gateway dedicado

Existem algumas limitações na compra de um gateway dedicado. Se você não conseguir comprar um gateway dedicado ou não conseguir criar um gateway, verifique os seguintes itens:

- Cota de gateway

  Por padrão, sua conta pode ser usada para criar cinco gateways dedicados em um projeto. Para criar gateways mais dedicados, envie um tíquete de serviço para aumentar a cota.

- Permissões

  Você deve receber as funções **APIG Administrator** e **VPC Administrator**.

  Você também pode receber permissões usando a política de **APIG FullAccess** ou políticas personalizadas. Para obter detalhes, consulte **Políticas personalizadas do APIG**.

- Número de endereços IP privados disponíveis na sub-rede

  As edições básica, profissional, empresarial e platina do APIG exigem 3, 5, 6 e 7 endereços IP privados em uma sub-rede, respectivamente. Certifique-se de que a sub-rede escolhida tenha endereços IP privados suficientes no console da Virtual Private Cloud (VPC).

Ambiente de rede

- VPC

Gateways dedicados são implementados em VPCs. Recursos em nuvem, como Elastic Cloud Servers (ECSs), na mesma VPC podem chamar APIs usando o endereço IP privado do gateway dedicado implementado na VPC.

É recomendável implementar seus gateways dedicados na mesma VPC que seus outros serviços para facilitar a configuração de rede e proteger o acesso à rede.

NOTA

VPCs de gateways dedicados não podem ser modificados.

- EIP

  Para permitir o acesso público de entrada às APIs implementadas em um gateway dedicado, compre um Elastic IP (EIP) e vincule-o ao gateway dedicado.

  NOTA

  Para APIs cujos serviços de back-end são implementados em uma rede pública, o APIG gera automaticamente um endereço IP para acesso público de saída e você não precisa comprar um EIP.

- Grupo de segurança

  Semelhante a um firewall, um grupo de segurança controla o acesso a um gateway através de uma porta específica e a transmissão de dados de comunicação do gateway para um endereço de destino específico. Para fins de segurança, crie regras de entrada para o grupo de segurança para permitir o acesso apenas em portas específicas.

  O grupo de segurança vinculado a um gateway dedicado deve atender aos seguintes requisitos:

  - Acesso de entrada: para permitir que as APIs no gateway dedicado sejam acessadas por redes públicas ou de outros grupos de segurança, adicione regras de entrada para o grupo de segurança para permitir o acesso nas portas 80 (HTTP) e 443 (HTTPS).
  - Acesso de saída: se o serviço de back-end de uma API for implementado numa rede pública ou noutro grupo de segurança, adicione regras de saída para o grupo de segurança para permitir o acesso ao endereço do serviço de back-end através da porta de chamada da API.
  - Se os serviços de front-end e back-end de uma API estiverem vinculados ao mesmo grupo de segurança e VPC do gateway dedicado, nenhuma regra de entrada ou saída será necessária para permitir o acesso pelas portas anteriores.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**.

Passo 5 Clique em **Buy Dedicated Gateway**.

Tabela 12-1 Parâmetros para criar um gateway dedicado

Parâmetro	Descrição
Billing Mode	Modo de cobrança do gateway dedicado. Atualmente, apenas o faturamento pagamento por uso é suportado.
Region	Uma área geográfica onde o gateway será implementado. Implemente o gateway na mesma região que seus outros serviços para permitir que todos os serviços se comuniquem por meio de sub-redes em uma VPC. Isso reduz os custos de largura de banda pública e a latência da rede.
AZ	Uma região física onde os recursos usam redes e fontes de alimentação independentes. As zonas de disponibilidade (AZs) são fisicamente isoladas, mas interconectadas por meio de uma rede interna. Para aumentar a disponibilidade do gateway, implemente o gateway em várias AZs.
Gateway Name	Nome do gateway.
Edition	As edições básica, profissional, empresarial e platina estão disponíveis. O número de solicitações simultâneas permitidas varia dependendo da edição do gateway. Para obter mais informações, consulte **Especificações**.
Scheduled Maintenance	Período de tempo em que o gateway pode ser mantido. O pessoal de suporte técnico entrará em contato com você antes da manutenção. Selecione um período de tempo com baixas demandas de serviço.
Enterprise Project	Selecione um projeto empresarial ao qual o gateway dedicado pertence. Este parâmetro só estará disponível se a sua conta for uma conta empresarial. Para obter detalhes sobre uso de recursos, migração e permissões de usuário de projetos empresariais, consulte **Guia de usuário do Enterprise Management**.
Public Inbound Access	Determine se deve permitir que as APIs criadas no gateway dedicado sejam chamadas por serviços externos usando um EIP. Para habilitar essa função, atribua um EIP ao gateway dedicado. Você precisará **pagar** pelo uso do EIP. APIs no gateway dedicado podem ser chamadas usando nomes de domínio independentes ou nomes de subdomínio. Há uma limitação no número de vezes que as APIs em um grupo de APIs podem ser chamadas por dia usando o nome do subdomínio. Para superar a limitação, vincule nomes de domínio independentes ao grupo de API e certifique-se de que os nomes de domínio independentes já tenham sido CNAMEd para o EIP do gateway dedicado ao qual o grupo de API pertence. Por exemplo, você tem uma API HTTPS (caminho: **/apidemo**) com acesso público habilitado. A API pode ser chamada usando "**https://***{domain}*/**apidemo**", onde *domain* indica um nome de domínio independente vinculado ao grupo de APIs ao qual a API pertence. O nome de domínio independente já deve ter sido CNAMEd para o EIP do gateway dedicado. A porta padrão é 443.

Parâmetro	Descrição
Public Outbound Access	Determine se os serviços de back-end das APIs criadas no gateway dedicado devem ser implementados em redes públicas. Se você ativar essa opção, defina uma largura de banda que atenda aos seus requisitos de serviço. A largura de banda varia de 1 a 2000 Mbit/s e será faturada por hora com base no preço do serviço EIP.
IPv6	**Este parâmetro está disponível apenas quando você define o modo de cobrança como pagamento por uso.** Se o serviço de back-end de uma API for implementado em uma rede pública e puder ser acessado apenas usando um endereço IPv6, selecione **IPv6 Access**. **NOTA** Esta função está disponível apenas em determinadas regiões.
Network	Selecione uma VPC e uma sub-rede para o gateway dedicado. Recursos em nuvem (como ECSs) na mesma VPC podem chamar APIs usando o endereço IP privado do gateway dedicado. Implemente o gateway dedicado na mesma VPC de seus outros serviços para facilitar a configuração de rede e proteger o acesso à rede.
Security Group	Selecione um grupo de segurança para controlar o acesso de entrada e saída. Se o serviço de back-end de uma API for implementado em uma rede externa, configure as regras do grupo de segurança para permitir o acesso ao endereço do serviço de back-end por meio da porta de chamada da API. **NOTA** Se o acesso de entrada público estiver habilitado, adicione regras de entrada para o grupo de segurança para permitir o acesso nas portas 80 (HTTP) e 443 (HTTPS).
Description	Descrição do gateway.

Passo 6 Clique em **Next**.

Passo 7 Verifique as configurações do gateway, leia e confirme a aceitação do contrato do cliente e a declaração de privacidade e clique em **Pay Now**. O progresso da criação do gateway é exibido na tela.

Se você definir o modo de cobrança como **Yearly/monthly**, o gateway dedicado será criado somente após você efetuar o pagamento.

----Fim

Operações de acompanhamento

Depois que o gateway for criado, você poderá criar e gerenciar APIs no console do gateway. A página **Gateway Information** mostra os detalhes do gateway, as configurações de rede, os recursos da API e as métricas.

Você pode modificar o nome do gateway, a descrição, a janela de tempo de manutenção programada, o grupo de segurança e o EIP.

Alteração do modo de cobrança de um gateway dedicado

Você pode alterar o modo de cobrança de gateways dedicados de **yearly/monthly** para **pay-per-use** ou de **pay-per-use** para **yearly/monthly**. O modo de cobrança pode ser alterado de anual/mensal para pagamento por uso somente quando as assinaturas do gateway expirarem.

Passo 1 No painel de navegação, escolha **Dedicated Gateways**.

Passo 2 Clique em **More** ao lado do gateway de destino e clique em **Change to Yearly/Monthly** ou **Change to Pay-per-Use**.

- Alterar para anual/mensal: selecione uma duração de renovação e clique em **Pay**.
- Alterar para pagamento por uso: clique em **Change to Pay-per-Use** antes que a assinatura do gateway expire ou durante o período congelado após o vencimento. A alteração só entra em vigor depois que a assinatura expirar.

----Fim

12.2.2 Modificação de um gateway dedicado

Você pode modificar as informações básicas e os parâmetros de configuração de gateways dedicados.

Modificar informações básicas

Para modificar as informações básicas sobre um gateway dedicado, faça o seguinte:

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**.

Passo 5 Clique em **Access Console** no canto superior direito do gateway dedicado que você deseja modificar.

Passo 6 Na página de guia **Basic Information**, modifique as informações básicas.

Tabela 12-2 Informações básicas sobre um gateway dedicado

Parâmetro	Descrição
Gateway Name	Nome do gateway.
Description	Descrição do gateway.
Scheduled Maintenance	Período de tempo em que o gateway pode ser mantido pelo pessoal de suporte técnico. O pessoal de suporte técnico entrará em contato com você se alguma atividade de manutenção ocorrer durante a janela. Selecione um período de tempo com baixas demandas de serviço.

Parâmetro	Descrição
Security Group	Selecione um grupo de segurança para controlar o acesso de entrada e saída. Se o serviço de back-end de uma API for implementado em uma rede externa, configure as regras do grupo de segurança para permitir o acesso ao endereço do serviço de back-end por meio da porta de chamada da API. **NOTA** ● Se você alterar o grupo de segurança, o novo grupo de segurança deverá atender aos requisitos para chamar APIs incluídas no gateway dedicado e acessar os serviços de back-end dessas APIs. ● Se o acesso de entrada público estiver habilitado, adicione regras de entrada para o grupo de segurança para permitir o acesso nas portas 80 (HTTP) e 443 (HTTPS).
EIP	Determine se deve permitir que as APIs criadas no gateway dedicado sejam chamadas por serviços externos usando um EIP. Para habilitar essa função, atribua um EIP ao gateway dedicado. Você precisará **pagar** pelo uso do EIP. APIs no gateway dedicado podem ser chamadas usando nomes de domínio independentes ou nomes de subdomínio. Há uma limitação no número de vezes que as APIs em um grupo de APIs podem ser chamadas por dia usando o nome do subdomínio. Para superar a limitação, vincule nomes de domínio independentes ao grupo de API e certifique-se de que os nomes de domínio independentes já tenham sido CNAMEd para o EIP do gateway dedicado ao qual o grupo de API pertence.
Outbound Access	Determine se deve permitir que os serviços de back-end da API sejam implementados em redes públicas e acessados usando o endereço IP gerado automaticamente pelo APIG. Você pode ativar ou desativar o acesso de saída a qualquer momento.
Bandwidth	A largura de banda é faturada por hora com base na taxa do serviço EIP.
Routes	Configure rotas em suas instalações se a sub-rede do data center estiver dentro dos três segmentos a seguir: 10.0.0.0/8-24, 172.16.0.0/12-24 e 192.168.0.0/16-24.

----Fim

Modificação dos parâmetros de configuração

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**.

Passo 5 Clique em **Access Console** no canto superior direito do gateway dedicado que você deseja modificar.

Passo 6 Clique na guia **Configuration Parameters** e clique em **Edit** na linha que contém o parâmetro que deseja modificar.

Tabela 12-3 Parâmetros de configuração

Nome do parâmetro	Descrição
ratelimit_api_limits	Valor padrão de limitação de solicitação aplicado a todas as APIs. O número total de vezes que uma API pode ser chamada é determinado por esse parâmetro somente se nenhuma política de limitação de solicitações estiver vinculada à API. O **Max. API Requests** de uma política de limitação de solicitações não pode exceder o valor desse parâmetro.
request_body_size	O tamanho máximo do corpo permitido para uma solicitação de API.
backend_timeout	Tempo limite de resposta do back-end. Intervalo de valores: 1 ms para 600.000 ms.
app_token	Determine se a autenticação app_token deve ser ativada. Se você ativar essa função, um access_token poderá ser adicionado à solicitação de autenticação da API. ● **app_token_expire_time**: o período de validade de um access_token. Um novo access_token deve ser obtido antes que o access_token original expire. ● **refresh_token_expire_time**: o período de validade de um refresh_token. Um refresh_token é usado para obter um novo access_token. ● **app_token_uri**: o URI usado para obter um access_token. ● **app_token_key**: a chave de criptografia de um token de acesso.
app_basic	Determine se a autenticação app_basic deve ser ativada. Depois que essa opção estiver habilitada, os usuários podem adicionar o parâmetro de cabeçalho **Authorization** e definir o valor do parâmetro como "Basic + base64 (*appkey* + : + *appsecret*)", em que *appkey* e *appsecret* são a chave e o segredo de uma aplicação ou o AppKey e o AppSecret de um cliente.

Nome do parâmetro	Descrição
app_secret	Determine se a autenticação app_secret deve ser ativada. Se você ativar essa função, os parâmetros **X-HW-ID** e **X-HW-AppKey** podem ser adicionados à solicitação da API para transportar a chave e o segredo de uma aplicação (o AppKey e o AppSecret de um cliente) para autenticação. Se você quiser ativar a autenticação app_secret, a autenticação app_api_key deve ser desativada.
app_route	Determine se deve ser compatível com o acesso à API baseado em endereço IP. Se você ativar essa função, as APIs que usam autenticação de aplicação em qualquer grupo, exceto **DEFAULT**, poderão ser chamadas usando endereços IP.
backend_client_certificate	Determine se deve habilitar a autenticação bidirecional de back-end. Se você ativar essa função, poderá configurar a autenticação bidirecional para um back-end ao criar uma API.
ssl_ciphers	Suítes de criptografia HTTPS suportadas. Selecione conjuntos de cifras que atendam aos seus requisitos.
real_ip_from_xff	Determine se os endereços IP devem ser usados no cabeçalho **X-Forwarded-For** para controle de acesso e limitação de solicitação. **xff_index**: número de sequência de um endereço IP no cabeçalho **X-Forwarded-For**. O valor pode ser positivo, negativo ou 0. ● Se o valor for 0 ou positivo, o endereço IP do índice correspondente no cabeçalho **X-Forwarded-For** será obtido. ● Se o valor for negativo, o endereço IP da sequência inversa indicada no cabeçalho **X-Forwarded-For** será obtido. Por exemplo, suponha que o cabeçalho **X-Forwarded-For** de uma solicitação recebida pelo API Gateway contenha três endereços IP: IP1, IP2 e IP3. Se o valor de **xff_index** for 0, IP1 é obtido. Se o valor for 1, IP2 é obtido. Se o valor for –1, IP3 é obtido. Se o valor for –2, IP2 é obtido.
vpc_name_modifiable	Determine se os nomes dos canais de balanceamento de carga podem ser modificados. **AVISO** Se essa opção estiver ativada, os canais de balanceamento de carga do gateway atual não poderão ser gerenciados usando as APIs de gerenciamento de canais de balanceamento de carga no nível do projeto.

Nome do parâmetro	Descrição
api_prom_metrics	Determine se a interface de métricas do Prometheus deve ser ativada. Se esta opção estiver ativada, você pode usar **https://**<*IP do componente de gateway*>**:1026/metrics** para coletar estatísticas de chamadas de API no formato Prometheus.
app_jwt_enable	Determine se a autenticação app_jwt deve ser ativada. Se esta opção estiver ativada, os parâmetros **Authorization** e **Timestamp** podem ser adicionados às solicitações da API para transportar a chave e o segredo (ou AppKey e AppSecret de um cliente) e um carimbo de data/hora para autenticação. **app_jwt_auth_header** é um cabeçalho incluído nas solicitações de API para autenticação app_jwt. O valor padrão do cabeçalho é **Authorization**.
public_key_enable	Determine se deve habilitar a autenticação public_key. **public_key_uri_prefix** indica o prefixo do URI usado para obter o segredo de public_key. O formato do URI é o seguinte: **https://***{VPC access address}{public_key_uri_prefix}{public_key name}*.

----Fim

12.2.3 Acessar o gateway compartilhado

O gateway compartilhado está disponível fora da caixa e pode ser usado diretamente.

NOTA

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

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Shared Gateway**.

----Fim

12.3 Abertura da API

12.3.1 Gerenciamento do grupo de API

12.3.1.1 Criação de um grupo de API

Cenário

Antes de criar uma API, você deve criar um grupo de APIs. Um grupo de APIs contém APIs diferentes usadas para o mesmo serviço.

NOTA

Cada API só pode pertencer a um grupo de APIs.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **API Groups**.

Passo 6 Clique em **Create API Group** e defina os parâmetros descritos em **Tabela 12-4**.

Tabela 12-4 Parâmetros para criar um grupo de APIs

Parâmetro	Descrição
Name	Nome do grupo de APIs.
Description	Descrição do grupo de APIs.

Passo 7 Clique em **OK**.

Depois que o grupo de APIs é criado, ele é exibido na lista de grupos de APIs.

NOTA

- O sistema aloca automaticamente um nome de subdomínio para o grupo de API para teste interno. O nome do subdomínio pode ser acessado 1000 vezes por dia.
- Um grupo de API padrão é gerado automaticamente para cada gateway dedicado. As APIs no grupo padrão podem ser chamadas usando o endereço IP da VPC onde o gateway dedicado é implementado.
- As APIs criadas no gateway compartilhado podem ser acessadas em redes públicas usando o nome do subdomínio do grupo ao qual as APIs pertencem. Em um gateway dedicado, o nome do subdomínio de cada grupo de APIs deve ser resolvido para um servidor na mesma VPC que o gateway. Se você deseja resolver o nome do subdomínio para uma rede pública, vincule um EIP ao gateway.
- Para disponibilizar suas APIs para acesso dos usuários, vincule nomes de domínio independentes ao grupo de APIs ao qual as APIs pertencem.

----Fim

Criação de um grupo de APIs chamando uma API

Você também pode criar um grupo de API chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Criação de um grupo de API**.

Operações de acompanhamento

Depois que o grupo de APIs for criado, vincule nomes de domínio independentes a ele para que os chamadores da API possam usar os nomes de domínio para chamar APIs no grupo. Para obter mais informações, consulte **Vinculação de um nome de domínio**.

12.3.1.2 Vinculação de um nome de domínio

Cenário

Antes de abrir uma API, você deve vincular um ou mais nomes de domínio independentes ao grupo ao qual a API pertence. Se nenhum nome de domínio estiver vinculado ao grupo, a API será chamada usando o nome de subdomínio padrão do grupo e poderá ser chamada apenas 1000 vezes por dia.

NOTA

- Em um gateway dedicado ou no gateway compartilhado, você não pode vincular o mesmo nome de domínio independente a diferentes grupos de API.

Observe os seguintes pontos antes de vincular um nome de domínio:

- Nome do subdomínio: depois que um grupo de APIs é criado, o sistema aloca automaticamente um nome de subdomínio exclusivo a ele para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia, mas não pode ser modificado.
- Nome de domínio independente: um nome de domínio independente é um nome de domínio personalizado usado para chamadores de API para chamar APIs abertas no grupo ao qual o nome de domínio está vinculado.

Pré-requisitos

1. Existe um nome de domínio independente disponível.

2. Gateway compartilhado: um registro CNAME aponta o nome de domínio independente para o nome do subdomínio do grupo de API. Para obter detalhes, consulte **Adição de um conjunto de registros CNAME**.

   Gateway dedicado: um registro A aponta o nome de domínio independente para o endereço do gateway. Para obter detalhes, consulte **Adição de um conjunto de registros A**.

3. Se o grupo de APIs contiver APIs que são chamadas por meio de HTTPS, é necessário que haja **certificados SSL** configurados para o nome de domínio independente. Certificados SSL só podem ser adicionados manualmente com um nome personalizado, conteúdo e uma chave.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **API Groups**.

Passo 6 Vá para a página de guia **Domain Names** usando um dos seguintes métodos:

- Clique no nome do grupo de API de destino e clique na guia **Domain Names** na página de detalhes do grupo de API exibida.
- Na coluna **Operation** do grupo de API de destino, escolha **More** > **Manage Domain Name**.

Passo 7 Clique em **Bind Independent Domain Name** e insira um nome de domínio.

Para grupos de API criados em gateways dedicados, especifique a versão mínima do TLS (TLS 1.1 ou TLS 1.2) compatível com os nomes de domínio vinculados aos grupos de API. O TLS 1.2 é recomendado.

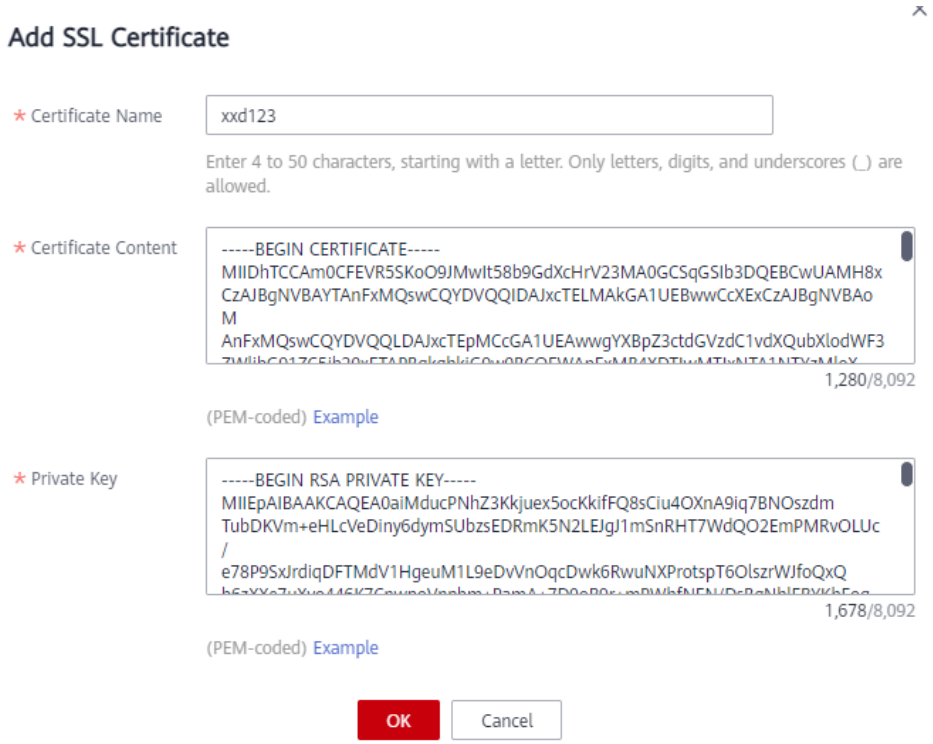
Passo 8 Clique em **OK**.

Se o nome de domínio não for necessário, clique em **Unbind** para desvinculá-lo do grupo de API.

Passo 9 (Opcional) Se o grupo de APIs contiver APIs acessadas por HTTPS, adicione um certificado SSL.

1. Clique em **Add SSL Certificate**.
2. Digite o nome, o conteúdo e a chave do **certificado SSL obtido** e clique em **OK**.

Figura 12-5 Adição de um certificado SSL



NOTA

- Atualmente, você só pode adicionar certificados SSL no formato PEM. Para adicionar certificados SSL de outros formatos, converta os certificados para o formato PEM primeiro.
- Para substituir ou editar um certificado SSL, clique em ao lado do nome do certificado. O conteúdo e a chave do certificado não estarão visíveis depois que você clicar em **OK** para adicionar o certificado. Se o conteúdo tiver sido atualizado, adicione todo o conteúdo ou a chave novamente.
- Se você não precisar de um certificado SSL, clique em **Delete SSL Certificate** na linha que contém o certificado para excluí-lo.

----Fim

Vinculação de um nome de domínio chamando uma API

Você também pode vincular um nome de domínio independente a um grupo de APIs chamando uma API fornecida pelo APIG. Para detalhes, consulte as seguintes referências:

Vinculação de um nome de domínio

Adição de um certificado a um nome de domínio

Solução de problemas

- Falha na vinculação de um nome de domínio independente: o nome de domínio independente não é CNAMEd para o nome de subdomínio do grupo de API ou o nome de domínio independente já existe.
- Falha ao adicionar um certificado SSL: o nome de domínio do certificado SSL é diferente do nome de domínio para o qual você adiciona o certificado SSL.

Operações de acompanhamento

Depois de vincular nomes de domínio independentes ao grupo de APIs, crie APIs no grupo para expor seletivamente os recursos de back-end. Para mais detalhes, consulte **Criação de uma API**.

12.3.1.3 Exclusão de um grupo de API

Cenário

Você pode excluir um grupo de APIs se não precisar dele.

NOTA

Os grupos de API que contêm APIs não podem ser excluídos.

Pré-requisitos

Você criou um grupo de APIs.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **API Groups**.

Passo 6 Excluir um grupo de APIs. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** do grupo de API de destino, escolha **More** > **Delete**.
- Clique no nome do grupo de API de destino e clique em **Delete Group** no canto superior direito da página de detalhes do grupo de API exibida.

Passo 7 Digite **DELETE** e clique em **Yes**.

----Fim

Exclusão de um grupo de API chamando uma API

Você também pode excluir um grupo de APIs chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de um grupo de API**.

12.3.1.4 Adição de uma resposta de gateway

Cenário

Uma resposta de gateway é exibida se o APIG falhar ao processar uma solicitação de API. O APIG fornece um conjunto de respostas padrão e também permite criar respostas de gateway com códigos de status e conteúdo personalizados na página **API Groups**. O conteúdo da resposta deve estar no formato JSON.

Por exemplo, o conteúdo de uma resposta de gateway padrão é o seguinte:

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

Você pode adicionar uma resposta com o seguinte conteúdo:

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

Você pode adicionar mais campos ou excluir campos existentes do corpo JSON.

NOTA

- As respostas de gateway padrão fornecidas pelo APIG podem ser editadas.
- Você pode criar respostas de gateway e configurar respostas diferentes para APIs no mesmo grupo de APIs.
- O tipo de resposta de gateway não pode ser alterado. Para mais detalhes, consulte **Tipos de respostas**.
- As respostas do gateway podem conter as variáveis de contexto do gateway da API (começando com **$context**). Para mais detalhes, consulte **Variáveis de contexto do APIG**.

Pré-requisitos

Você criou um grupo de APIs.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

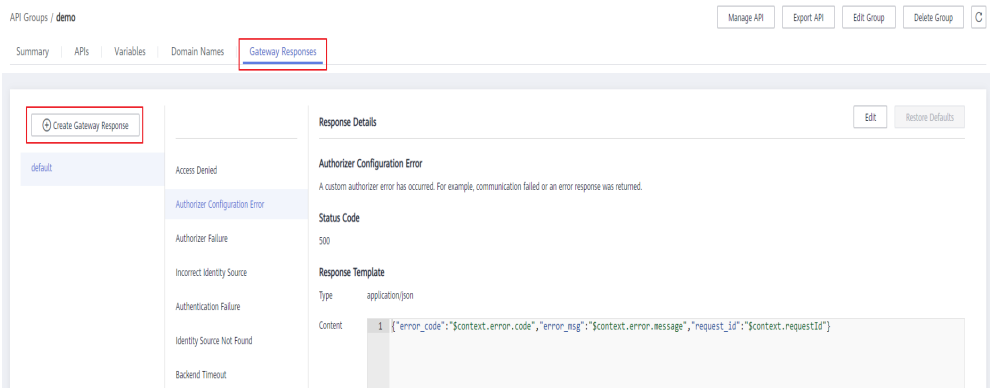
Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **API Groups**.

Passo 6 Localize o grupo de APIs para o qual você deseja criar ou modificar uma resposta de gateway e clique no nome do grupo para ir para a página de detalhes do grupo de APIs.

Passo 7 Clique na guia **Gateway Responses** e crie uma resposta de gateway.



NOTA

- Para editar uma resposta, clique no botão **Edit** no canto superior direito e modifique o código de status e o conteúdo da resposta.
- Você pode modificar apenas o código de status e o conteúdo de uma resposta de gateway padrão ou personalizada e não pode alterar o tipo de resposta.
- Informações de erro e outros detalhes de resposta podem ser obtidos usando variáveis. Para obter detalhes sobre as variáveis suportadas, consulte **Tabela 12-6**.

----Fim

Tipos de respostas

Tabela 12-5 lista os tipos de resposta suportados pelo APIG. Você pode definir códigos de status de respostas para atender aos seus requisitos de serviço.

Tabela 12-5 Tipos de resposta de erro suportados pelo APIG

Nome da resposta	Código de status padrão	Descrição
Acesso negado	403	Acesso negado. Por exemplo, a política de controle de acesso é acionada ou um ataque é detectado.
Erro de configuração do autorizador	500	Ocorreu um erro de autorizador personalizado. Por exemplo, a comunicação falhou ou uma resposta de erro foi retornada.
Autorizador falhou	500	Falha na autorização personalizada.
Fonte de identidade incorreta	401	A origem de identidade do autorizador personalizado está ausente ou é inválida.
Falha de autenticação	401	Falha na autenticação do IAM ou da aplicação.
Fonte de identidade não encontrada	401	Nenhuma fonte de identidade foi especificada.
Tempo limite de back-end	504	A comunicação com o serviço de back-end expirou.

Nome da resposta	Código de status padrão	Descrição
Back-end indisponível	502	O serviço de back-end não está disponível devido a um erro de comunicação.
Padrão 4XX	-	Outro erro 4XX ocorreu.
Padrão 5XX	-	Outro erro 5XX ocorreu.
Nenhuma API encontrada	404	Nenhuma API foi encontrada.
Parâmetros de solicitação incorretos	400	Os parâmetros de solicitação estão incorretos ou o método HTTP não é suportado.
Solicitação limitada	429	A solicitação foi rejeitada devido à limitação de solicitação.
Aplicação não autorizada	401	A aplicação que você está usando não foi autorizada a chamar a API.

Variáveis de contexto do APIG

Tabela 12-6 Variáveis que podem ser usadas no corpo da mensagem de resposta

Variável	Descrição
$context.apiId	ID da API.
$context.appId	ID da aplicação que chama a API.
$context.requestId	ID da solicitação gerada quando a API é chamada.
$context.stage	Ambiente de implementação no qual a API é chamada.
$context.sourceIp	Endereço IP de origem do chamador da API.
$context.authorizer.frontend.property	Valores dos pares de valor do atributo especificados mapeados para o contexto na resposta do autorizador personalizado do front-end
$context.authorizer.backend.property	Valores dos pares de valor do atributo especificados mapeados para o contexto na resposta do autorizador personalizado de back-end
$context.error.message	Mensagem de erro.
$context.error.code	Código de erro.
$context.error.type	Tipo de erro.

12.3.2 Gerenciamento de API

12.3.2.1 Criação de uma API

Cenário

Você pode expor seletivamente seus serviços configurando suas APIs no APIG.

Para criar uma API, defina as informações básicas e defina a solicitação da API, o serviço de back-end e as respostas.

NOTA

O APIG usa uma arquitetura de API baseada em REST, portanto, a abertura e a chamada da API devem estar em conformidade com as especificações da API RESTful relacionadas.

Pré-requisitos

- Você criou um grupo de APIs. Se nenhum grupo de API estiver disponível, crie um durante a criação da API.
- Se o serviço de back-end da API for implementado em uma VPC, você criou um canal da VPC para acessar o serviço seguindo o procedimento em **Criação de um canal da VPC**. Você também pode criar um canal da VPC durante a criação da API.

Configuração de informações básicas

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Clique em **Create API** e defina os parâmetros listados em **Tabela 12-7**.

Tabela 12-7 Informações básicas

Parâmetro	Descrição
Name	Nome da API. É recomendável inserir um nome com base nas regras de nomenclatura para facilitar a pesquisa.

Parâmetro	Descrição
API Group	O grupo ao qual a API pertence. Se nenhum grupo de APIs estiver disponível, clique em **Create API Group** para criar um.
Gateway Response	Exibido se o APIG falhar ao processar uma solicitação de API. O APIG fornece um conjunto de respostas padrão e também permite que você **crie respostas de gateway** com códigos de status e conteúdo personalizados, na página **API Groups**. O conteúdo da resposta deve estar no formato JSON.
Visibility	Determine se a API está disponível para o público. Opções: ● **Public**
Security Authentication	Os seguintes modos de autenticação estão disponíveis: ● **App**: as solicitações para a API serão autenticadas pelo APIG. ● **IAM**: as solicitações para a API serão autenticadas pelo Identity and Access Management (IAM). ● **Custom**: as solicitações para a API serão autenticadas usando seu próprio sistema ou serviço de autenticação (por exemplo, um sistema de autenticação baseado em OAuth). ● **None**: nenhuma autenticação será necessária. O método de chamada da API varia dependendo do modo de autenticação. Para obter detalhes, consulte **Guia de desenvolvedor**. A autenticação da aplicação é recomendada. **AVISO** ● Se você definir o modo de autenticação de uma API como **IAM**, qualquer usuário do APIG poderá acessar a API, o que pode resultar em cobranças excessivas se a API for bombardeada com solicitações maliciosas. ● Se você definir o modo de autenticação de uma API como **None**, qualquer usuário poderá acessar a API em redes públicas, o que pode resultar em cobranças excessivas se a API for bombardeada com solicitações maliciosas. ● Se você definir o modo de autenticação de uma API como **Custom**, poderá criar uma função no FunctionGraph para interconectar com seu próprio sistema ou serviço de autenticação. Este modo de autenticação não é suportado em regiões onde o FunctionGraph não está disponível.
Simple Authentication	Esse parâmetro está disponível somente se você definir **Security Authentication** como **App**. Se você selecionar autenticação de aplicação, poderá configurar se deseja ativar a autenticação simples. Na autenticação simples, o parâmetro **X-Apig-AppCode** é adicionado ao cabeçalho da solicitação HTTP para uma resposta rápida. O APIG verifica apenas o AppCode e o conteúdo da solicitação não precisa ser assinado. A autenticação simples suporta apenas solicitações HTTPS e não suporta solicitações HTTP. Para mais detalhes, consulte **Adição de um AppCode para autenticação simples**. **NOTA** Depois de ativar a autenticação simples para uma API existente, você precisa publicar a API novamente. Para mais detalhes, consulte **Publicação de uma API**.

Parâmetro	Descrição
Custom Authorizer	Este parâmetro é obrigatório se a **Security Authentication** estiver definida como **Custom**. Selecione um autorizador personalizado se você definir a **Security Authentication** como **Custom**. Se nenhum autorizador personalizado estiver disponível, clique em **Create Custom Authorizer** para criar um.
Tag Name	Atributo de classificação usado para identificar rapidamente a API de outras APIs.
Description	Descrição da API.

Passo 7 Clique em **Next**.

----Fim

Definição de solicitação de API

Passo 1 Na página **Define API Request**, defina os parâmetros listados em **Tabela 12-8**.

Figura 12-6 Definir solicitação de API

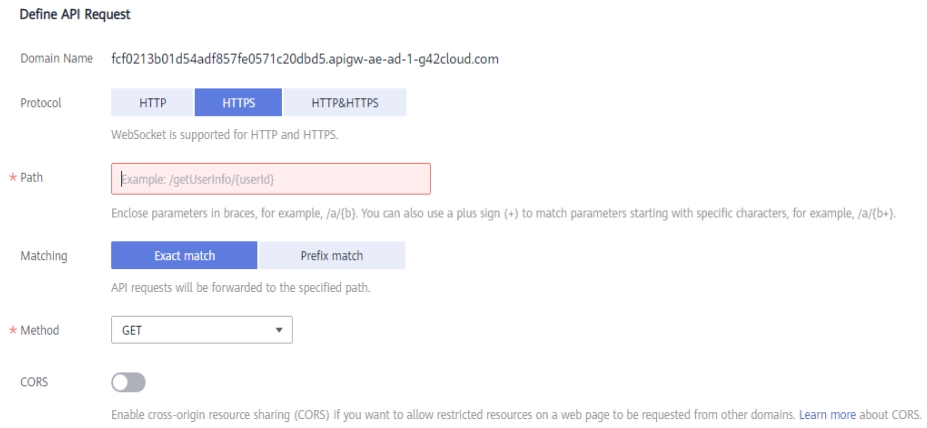


Tabela 12-8 Parâmetros para definição de solicitações de API

Parâmetro	Descrição
Domain Name	O subdomínio alocado automaticamente ao grupo de APIs.
Protocol	O protocolo usado para chamar a API. Opções: ● HTTP ● HTTPS ● HTTP&HTTPS HTTPS é recomendado para transmitir dados importantes ou confidenciais.

Parâmetro	Descrição
Path	O caminho para solicitar a API. Insira um caminho no formato "/users/*{userId}*/projects". ● A variável em chaves ({}) é um parâmetro de solicitação. Certifique-se de que é um segmento inteiro entre um par de barras (/). Um segmento que não é marcado por um par de barras, por exemplo, **/abc{userId}**, não é suportado. Se você definir o modo de correspondência como **Exact match**, poderá adicionar um sinal de adição (+) ao final do parâmetro de requisição, por exemplo, **/users/{*p*+}**. A variável *p* corresponde aos segmentos entre um ou vários pares de barras (/). ● Certifique-se de definir os parâmetros contidos no caminho da solicitação como parâmetros de entrada. ● O conteúdo é sensível a maiúsculas e minúsculas.
Matching	Opções: ● **Exact match**: a API pode ser chamada apenas usando o caminho de solicitação especificado. ● **Prefix match**: a API pode ser chamada usando caminhos começando com os caracteres correspondentes. Por exemplo, se você definir o caminho da solicitação como **/test/AA** e o modo de correspondência como **Prefix match**, a API poderá ser chamada usando **/test/AA/CC**, mas não poderá ser chamada usando **/test/AACC**. **NOTA** ● A correspondência exata tem precedência sobre a correspondência de prefixo. A correspondência de prefixo com um prefixo curto tem uma prioridade mais baixa. Por exemplo, para o caminho de solicitação **/a/b/c** (correspondência exata), **/a** (correspondência de prefixo) e **/a/b** (correspondência de prefixo), a ordem de correspondência é **/a/b/c** > **/a/b** > **/a**. ● Se você definir o modo de correspondência como **Prefix match**, os caracteres do caminho de solicitação da API, excluindo o prefixo, serão transmitidos de forma transparente ao serviço de back-end. Por exemplo, se você definir os caminhos de solicitação de front-end e back-end de uma API como **/test/** e **/test2/**, respectivamente, e a API for chamada usando **/test/AA/CC**, os caracteres **AA/CC** serão transmitidos de forma transparente para o serviço de back-end. A URL de solicitação recebida pelo serviço de back-end é **/test2/AA/CC/**.
Method	O método de chamada da API. As opções são **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS** e **ANY**. ● **ANY** indica que a API pode ser chamada usando qualquer método de solicitação. ● Se você definir **Method** como **POST**, **PUT**, **PATCH** ou **ANY**, defina o corpo da solicitação.

Parâmetro	Descrição
CORS	Determine se deve ativar o compartilhamento de recursos de origem cruzada (CORS). O CORS permite que navegadores enviem XMLHttpRequest para servidores em outros domínios, superando a limitação de que Asynchronous JavaScript and XML (AJAX) podem ser usados apenas no mesmo domínio. Existem dois tipos de solicitações CORS: ● Solicitações simples: solicitações que possuem o campo **Origin** no cabeçalho. ● Solicitações não tão simples: solicitações HTTP enviadas antes da solicitação real. Se você ativar o CORS, precisará criar outra API que use o método OPTIONS. Para mais detalhes, consulte **CORS**.

Passo 2 (Opcional) Defina os parâmetros de entrada.

Os parâmetros de entrada são transmitidos juntamente com a solicitação quando a API é chamada.

1. Clique em **Add Input Parameter**.
2. Defina os parâmetros listados em **Tabela 12-9**.

Tabela 12-9 Definição do parâmetro de entrada

Parâmetro	Descrição
Name	Nome do parâmetro de entrada. Se você definir o local do parâmetro como **PATH**, certifique-se de que o nome do parâmetro seja o mesmo definido no caminho da solicitação. **NOTA** – O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**. – O nome do parâmetro não pode ser **x-stage**. – Se você definir a localização do parâmetro como **HEADER**, verifique se o nome do parâmetro não é **Authorization** ou **X-Auth-Token** e não contém sublinhados (_).
Location	Posição do parâmetro nas solicitações. As opções são **PATH**, **HEADER** e **QUERY**. **NOTA** Se você definir o local do parâmetro como **PATH**, deverá incluir o parâmetro no caminho da solicitação.
Type	Tipo do valor do parâmetro. Opções: **STRING** e **NUMBER**. **NOTA** Defina o tipo de parâmetros Boolean como **STRING**.

Parâmetro	Descrição
Mandatory	Determine se o parâmetro de entrada é necessário em cada solicitação enviada para chamar a API. Se você selecionar **Yes**, as solicitações de API que não contêm o parâmetro de entrada serão rejeitadas.
Passthrough	Determine se deseja transmitir de forma transparente o parâmetro de entrada para o serviço de back-end.
Default Value	O valor que será usado se nenhum valor for especificado para o parâmetro de entrada quando a API for chamada. Se o parâmetro de entrada não for especificado em uma solicitação, o APIG enviará automaticamente o valor padrão para o serviço de back-end.
Enumerated Value	Valor enumerado do parâmetro de entrada. Use vírgulas (,) para separar vários valores enumerados. O valor desse parâmetro de entrada pode ser apenas um dos valores enumerados.
Minimum Length	O comprimento mínimo do valor do parâmetro. Apenas números são permitidos.
Maximum Length	O comprimento máximo do valor do parâmetro. Apenas números são permitidos.
Example	Exemplo de valor para o parâmetro.
Description	Descrição do parâmetro.

3. Clique em **OK**.

Passo 3 Clique em **Next**.

----Fim

Definição do serviço de back-end

O APIG permite que você defina várias políticas de back-end para diferentes cenários. As solicitações que atendam às condições especificadas serão encaminhadas para o back-end correspondente. Por exemplo, você pode fazer com que certas solicitações para uma API sejam encaminhadas para um back-end específico especificando o endereço IP de origem nas condições de política do back-end.

Você pode definir no máximo cinco políticas de back-end para uma API, além do back-end padrão.

Passo 1 Defina o back-end padrão.

As solicitações de API que não atenderem às condições de qualquer back-end serão encaminhadas para o back-end padrão.

Na página **Define Backend Request**, selecione um tipo de back-end.

Tabela 12-10, **Tabela 12-11** e **Tabela 12-12** descreva os parâmetros do serviço de back-end.

Tabela 12-10 Parâmetros para definir um serviço de back-end HTTP/HTTPS

Parâmetro	Descrição
Protocol	HTTP ou HTTPS. Este protocolo deve ser o utilizado pelo serviço de back-end. **NOTA** ● O WebSocket é compatível com HTTP e HTTPS. ● HTTPS é recomendado para transmitir dados importantes ou confidenciais.
Method	O método de chamada da API. As opções são **GET**, **POST**, **DELETE**, **PUT**, **PATCH**, **HEAD**, **OPTIONS** e **ANY**. **ANY** indica que a API pode ser chamada usando qualquer método de solicitação.
VPC Channel	Determine se o serviço de back-end será acessado usando um canal da VPC. ● **Se sim, selecione um canal da VPC.** **NOTA** – Para garantir uma verificação de integridade bem-sucedida e a disponibilidade do serviço, configure os grupos de segurança dos servidores de nuvem em cada canal da VPC para permitir o acesso de 100.125.0.0/16. ● **Se não, configure o endereço do serviço de back-end.** Digite um endereço de back-end no formato de "endereço IP do host ou nome de domínio": "número da porta". A porta padrão (80 para HTTP e 443 para HTTPS) será usada se você não especificar uma porta. Portas disponíveis: 1 a 65535. Se você quiser usar uma variável, coloque o nome da variável em sinais numéricos (#), por exemplo, **#ipaddress#**. Você pode usar múltiplas variáveis, por exemplo, **#ipaddress##test#**.
Host Header (if applicable)	Esse parâmetro só estará disponível se você definir o **VPC Channel** como **Configure**. Defina um cabeçalho de host para solicitações a serem enviadas para servidores em nuvem associados ao canal da VPC. Por padrão, o cabeçalho do host original em cada solicitação será usado.
Path	O caminho de solicitação (URI) do serviço de back-end. Certifique-se de que todos os parâmetros no caminho estejam entre chaves ({}). Por exemplo, **/getUserInfo/{userId}**. Se o caminho contiver uma variável de ambiente, coloque a variável de ambiente em sinais numéricos (#), por exemplo, **/#path#**. Você pode usar várias variáveis de ambiente, por exemplo, **/#path##request#**.

Parâmetro	Descrição
Timeout (ms)	Tempo limite de solicitação de back-end. Se ocorrer um erro de tempo limite de back-end durante a depuração da API, aumente o tempo limite para localizar o motivo. **NOTA** Para gateways dedicados, você pode modificar o tempo limite máximo consultando **Parâmetros de configuração**. O intervalo de valores é de 1 ms a 600.000 ms.
Two-way Authentication	Determine se deve permitir que o APIG autentique o serviço de back-end da API por meio de HTTPS. Para obter detalhes sobre como configurar o certificado para autenticação bidirecional, consulte **Parâmetros de configuração**. **NOTA** A autenticação bidirecional está disponível apenas para gateways dedicados em determinadas regiões.
Backend Authentication	Determine se seu serviço de back-end precisa autenticar solicitações de API. Se você habilitar essa opção, selecione um autorizador personalizado para autenticação de back-end. **Autorizadores personalizados** são funções criadas no FunctionGraph para implementar uma lógica de autenticação ou invocar um serviço de autenticação. **NOTA** A autenticação de back-end depende do FunctionGraph e só está disponível em determinadas regiões.

Tabela 12-11 Parâmetros para definir um serviço de back-end do FunctionGraph

Parâmetro	Descrição
FunctionURN	Identificador da função solicitada. Clique em **Select Function URN** para especificar uma função URN.
Version/Alias	Selecione uma versão de função ou alias. Para obter detalhes, consulte as seções "Gerenciamento de versões" e "Gerenciamento de aliases" no *Guia de usuário do FunctionGraph*.
Invocation Mode	● **Synchronous**: invocação síncrona. Ao receber uma solicitação de invocação, o FunctionGraph processa imediatamente a solicitação e retorna um resultado. O cliente fecha a conexão uma vez que recebeu uma resposta do back-end. ● **Asynchronous**: invocação assíncrona. Os resultados de invocação de função de solicitações de clientes não importam para os clientes. Quando recebe uma solicitação, o FunctionGraph a enfileira, retorna uma resposta e processa uma a uma no estado ocioso.
Timeout (ms)	Tempo limite de solicitação de back-end. Para mais detalhes, consulte **Tabela 12-10**.

Parâmetro	Descrição
Backend Authentication	Para obter detalhes, consulte a descrição sobre autenticação de back-end em **Tabela 12-10**.

Tabela 12-12 Parâmetros para definição de um serviço de back-end Mock

Parâmetro	Descrição
Status Code	Este parâmetro só está disponível depois de actualizar o componente Shubao.
Response	Você pode usar o Mock para desenvolvimento, depuração e verificação de APIs. Ele permite que o APIG retorne uma resposta sem enviar a solicitação para o back-end. Isso é útil se você precisar testar APIs quando o back-end não estiver disponível.
Backend Authentication	Para obter detalhes, consulte a descrição sobre autenticação de back-end em **Tabela 12-10**.
Header Parameters	Cabeçalhos de resposta da API. Clique em **Add Header** e insira o nome do parâmetro, o valor e a descrição.

NOTA

- Se você tiver definido uma variável de ambiente no caminho de solicitação de back-end, a API não poderá ser depurada na página de depuração da API.
- Para variáveis definidas no caminho de solicitação de back-end de uma API, as variáveis de ambiente correspondentes e seus valores devem ser configurados. Caso contrário, a API não poderá ser publicada porque não haverá valores que possam ser atribuídos às variáveis.
- Os nomes das variáveis de ambiente diferenciam maiúsculas de minúsculas.

Passo 2 (Opcional) Adicione uma política de back-end.

Você pode adicionar políticas de back-end para encaminhar solicitações para diferentes serviços de back-end.

1. Clique em **Add Backend Policy**.
2. Defina parâmetros referindo-se a **Tabela 12-13** e **Tabela 12-10**.

Figura 12-7 Adição de uma política de back-end

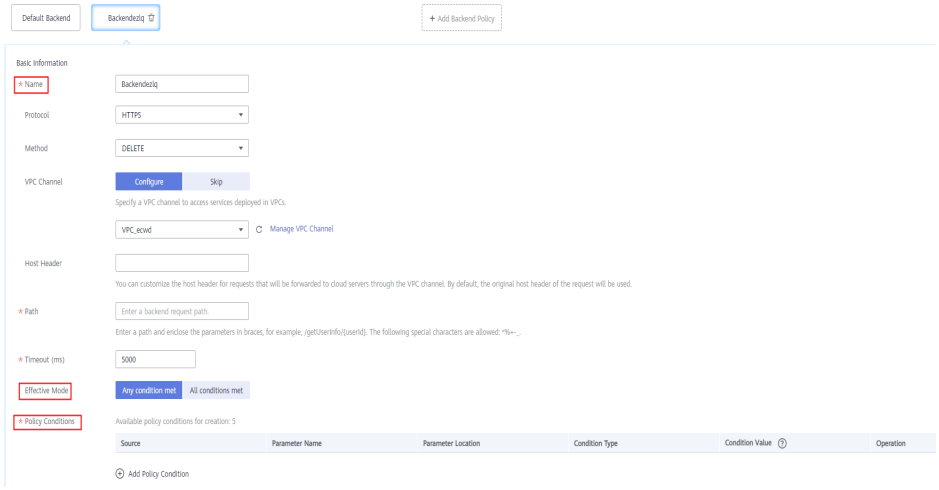


Tabela 12-13 Parâmetros de política de back-end

Parâmetro	Descrição
Name	O nome da política de back-end.
Effective Mode	- **Any condition met**: a política de back-end entra em vigor se alguma das condições da política tiver sido cumprida. - **All conditions met**: a política de back-end entra em vigor somente quando todas as condições da política forem atendidas.
Policy Conditions	Condições que devem ser atendidas para que a política de back-end entre em vigor. Estabeleça condições referindo-se a **Tabela 12-14**.

Tabela 12-14 Condições de políticas

Parâmetro	Descrição
Source	- Endereço IP de origem - Parâmetro de entrada - Parâmetros do sistema: parâmetros de tempo de execução usados pelo APIG para processar solicitações de API **AVISO** Os parâmetros de entrada (por exemplo, cabeçalhos) definidos como condições de política já devem ter sido definidos nas configurações de solicitação da API. Somente gateways dedicados suportam o uso de parâmetros do sistema como condições de política. Se **System parameter** não for exibido, entre em contato com o suporte técnico para atualizar seu gateway.

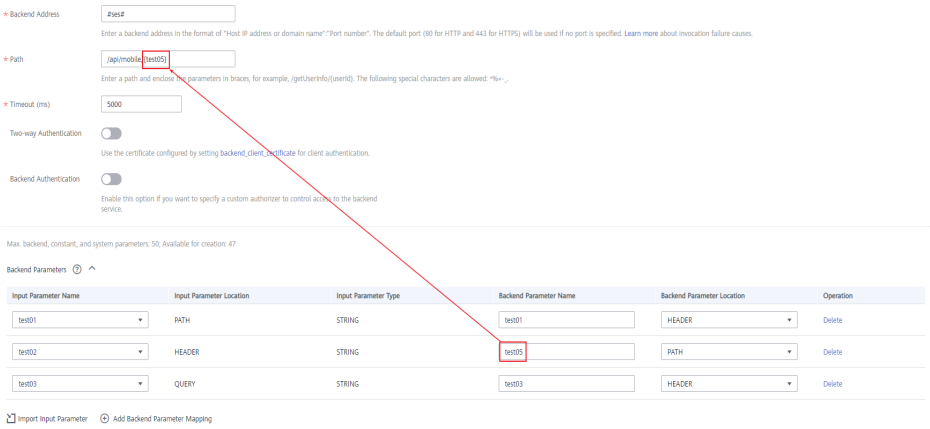
Parâmetro	Descrição
Parameter Name	- Ao definir **Source** como **Input parameter**, selecione um parâmetro de entrada. - Ao definir o **Source** para **System parameter**, selecione um parâmetro do sistema. ■ **reqPath**: solicitar URI, por exemplo, **/a/b/c**. ■ **reqMethod**: método de requisição, por exemplo, **GET**.
Parameter Location	A localização do parâmetro é exibida apenas se você definir **Source** como **Input parameter**.
Condition Type	Este parâmetro é necessário somente se você definir **Source** para **Input parameter** ou **System parameter**. - **Equal**: o parâmetro de solicitação deve ser igual ao valor especificado. - **Enumerated**: o parâmetro de solicitação deve ser igual a qualquer um dos valores enumerados. - **Matching**: o parâmetro de solicitação deve ser igual a qualquer valor da expressão regular. **NOTA** Ao definir o **Source** para **System parameter** e selecionar um parâmetro chamado **reqMethod**, você pode definir o tipo de condição apenas como **Equal** ou **Enumerated**.
Condition Value	Defina um valor de condição de acordo com o tipo de condição. - **Equal**: insira um valor. - **Enumerated**: insira vários valores e separe-os usando vírgulas. - **Matching**: insira um intervalo, por exemplo, **[0-5]**. Se você tiver definido **Source** para **Source IP address**, insira um ou mais endereços IP e separe-os usando vírgulas.

Passo 3 (Opcional) Defina parâmetros de back-end.

Os parâmetros de entrada da API são mapeados para os parâmetros de back-end correspondentes nas solicitações de back-end.

1. Clique em ⌄ ao lado de **Backend Parameters** e defina os parâmetros de back-end. Você pode usar um dos seguintes métodos:
   - Clique em **Import Input Parameter**. Todos os parâmetros de entrada definidos são exibidos automaticamente.
   - Clique em **Add Backend Parameter Mapping** e adicione os parâmetros de back-end necessários.
2. Modifique os mapeamentos com base nos parâmetros e seus locais nas solicitações de back-end. **Figura 12-8** destaca os parâmetros de back-end.

Figura 12-8 Configurar parâmetros de back-end



a. Se você definir o local do parâmetro como **PATH**, verifique se o nome do parâmetro é o mesmo que o definido no caminho da solicitação de back-end.

b. O nome e o local de um parâmetro de entrada podem ser diferentes daqueles do parâmetro de solicitação de back-end mapeado.

   NOTA

   - O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**.
   - O nome do parâmetro não pode ser **x-stage**.
   - Se você definir o local do parâmetro como **HEADER**, certifique-se de que o nome do parâmetro não contenha sublinhados (_).

c. Na figura anterior, os parâmetros **test01** e **test03** estão localizados nas posições de caminho e consulta das solicitações da API e seus valores serão recebidos no cabeçalho das solicitações de back-end. O **test02** está localizado no cabeçalho das solicitações da API, e seu valor será recebido através do **test05** no caminho das solicitações de back-end.

   Por exemplo, **test01** é **abc**, **test02** é **def** e **test03** é **xyz**.

   Solicitações de API:

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

   Solicitação de back-end:

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

Passo 4 (Opcional) Defina parâmetros constantes.

Você pode definir parâmetros constantes para o serviço de back-end para receber constantes que são invisíveis para os chamadores da API. O APIG adiciona parâmetros constantes às posições especificadas na solicitação enviada ao serviço de back-end.

1. Clique em ⌄ ao lado de **Constant Parameters**.
2. Clique em **Add Constant Parameter** e defina os parâmetros listados em **Tabela 12-15**.

Figura 12-9 Adição de parâmetros constantes

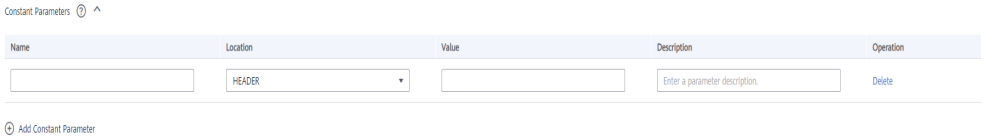


Tabela 12-15 Configuração de parâmetros constantes

Parâmetro	Descrição
Name	Nome do parâmetro constante. Se você definir o local do parâmetro como **PATH**, verifique se o nome do parâmetro é o mesmo que o definido no caminho da solicitação de back-end. **NOTA** – O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**. – O nome do parâmetro não pode ser **x-stage**. – Se você definir o local do parâmetro como **HEADER**, certifique-se de que o nome do parâmetro não contenha sublinhados (_).
Location	Posição do parâmetro nas solicitações. As opções são **PATH**, **QUERY** e **HEADER**.
Value	Valor do parâmetro.
Description	Descrição do parâmetro constante.

NOTA

- O APIG envia solicitações contendo parâmetros constantes para serviços de back-end após a codificação percentual de valores de parâmetros especiais. Certifique-se de que os serviços de back-end ofereçam suporte à codificação de porcentagem. Por exemplo, o valor do parâmetro **[apig]** torna-se **%5Bapig%5D** após a codificação percentual.
- Para valores de parâmetros de caminho, os seguintes caracteres serão codificados por porcentagem: códigos ASCII 0–31, símbolos em branco, códigos ASCII 127–255 e caracteres especial ?></%#"[\]^` {|}
- Para valores de cadeias de consulta, os seguintes caracteres serão codificados por porcentagem: códigos ASCII 0–31, símbolos em branco, códigos ASCII 127–255 e caracteres especiais >=<+&%#"[\]^` {|}

Passo 5 (Opcional) Defina os parâmetros do sistema.

Os parâmetros do sistema referem-se aos parâmetros de tempo de execução relativos à execução do gateway e às autenticações de front-end e back-end. Os parâmetros são transferidos para o serviço de back-end da API para controle de acesso e autenticação personalizada.

1. Clique em ⌄ ao lado de **System Parameters**.
2. Clique em **Add System Parameter** e defina os parâmetros listados em **Tabela 12-16**.

Figura 12-10 Adição de um parâmetro do sistema

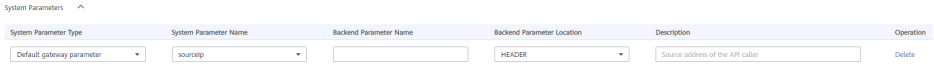


Tabela 12-16 Parâmetros do sistema

Parâmetro	Descrição
System Parameter Type	- **Default gateway parameter**: parâmetros padrão suportados pelo APIG. - **Frontend authentication parameter**: parâmetros a serem exibidos no resultado de autenticação personalizada do front-end. Essa opção estará disponível somente se você selecionar **Custom** para **Security Authentication** na página **Set Basic Information**. - **Backend authentication parameter**: parâmetros a serem exibidos no resultado de autenticação personalizada do back-end. Essa opção estará disponível somente se você ativar **Backend Authentication** na página **Define Backend Request**.
System Parameter Name	- Se **System Parameter Type** for **Default gateway parameter**, selecione qualquer um dos seguintes parâmetros. ■ **sourceIp**: endereço IP de origem do chamador da API ■ **stage**: ambiente no qual a API é chamada ■ **apiId**: ID da API ■ **appId**: ID da aplicação que chama a API ■ **requestId**: ID da solicitação gerada quando a API é chamada ■ **serverAddr**: endereço IP do servidor de gateway ■ **serverName**: nome do servidor de gateway ■ **handleTime**: tempo de processamento da solicitação da API ■ **providerAppId**: ID da aplicação do provedor de API - Certifique-se de que os parâmetros de autenticação de front-end e back-end sejam consistentes com os parâmetros de resultado de retorno definidos para a função de autorizador personalizada correspondente. Para obter detalhes sobre como criar uma função de autorizador personalizada e obter parâmetros de resultado retornados, consulte **Guia de desenvolvedor do API Gateway**.
Backend Parameter Name	Nome do parâmetro de back-end para o qual o parâmetro de sistema será mapeado. **NOTA** – O nome do parâmetro não diferencia maiúsculas de minúsculas. Não pode começar com **x-apig-** ou **x-sdk-**. – O nome do parâmetro não pode ser **x-stage**. – Se você definir o local do parâmetro como **HEADER**, certifique-se de que o nome do parâmetro não contenha sublinhados (_).
Backend Parameter Location	Posição do parâmetro back-end nas solicitações.
Description	Descrição do parâmetro do sistema.

Passo 6 Clique em **Next**.

----Fim

Definição de respostas

Passo 1 Na página **Define Response**, defina os parâmetros listados em **Tabela 12-17**.

Tabela 12-17 Definição de respostas

Parâmetro	Descrição
Example Success Response	Um exemplo de uma resposta retornada quando a API é chamada com sucesso.
Example Failure Response	Um exemplo de uma resposta retornada quando a API falha ao ser chamada.

Passo 2 Clique em **Finish**.

Depois que a API for criada, clique em seu nome na lista de APIs para exibir os detalhes.

----Fim

Criação de uma API chamando uma API

Você também pode criar uma API chamando uma API fornecida pelo APIG.

Para obter detalhes, consulte **Registração de uma API**.

Perguntas frequentes sobre a criação de APIs

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

Qual modo de autenticação dever escolher?

Quais são as possíveis causas se um serviço de back-end falhar ao ser chamado ou se a chamada expirar?

Por que estar vendo a mensagem "Nenhum back-end disponível"?

Operações de acompanhamento

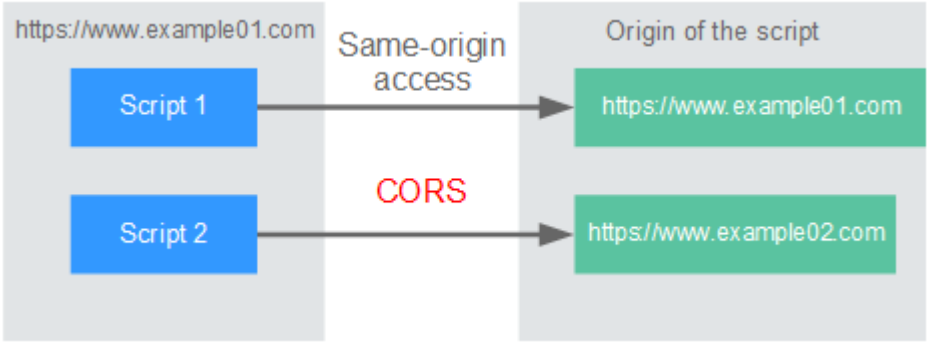
Depois de criar uma API, verifique-a seguindo o procedimento em **Depuração de uma API**.

12.3.2.2 CORS

O que é o CORS?

Por motivos de segurança, os navegadores restringem as solicitações de origem cruzada iniciadas a partir de scripts. Isso significa que uma aplicação Web só pode solicitar recursos de sua origem. O mecanismo CORS permite que os navegadores enviem XMLHttpRequest para servidores em outros domínios e solicitem acesso aos recursos lá.

Figura 12-11 Fluxo de processo do mecanismo CORS



Existem dois tipos de solicitações CORS:

- **Solicitações simples**

  As solicitações simples devem atender às seguintes condições:

  a. O método de requisição é HEAD, GET ou POST.

  b. O cabeçalho da solicitação contém apenas os seguintes campos:

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

  No cabeçalho de uma solicitação simples, os navegadores adicionam automaticamente o campo **Origin** para especificar a origem (incluindo o protocolo, o domínio e a porta) da solicitação. Depois de receber tal solicitação, o servidor de destino determina se a solicitação é segura e pode ser aceita com base na origem. Se o servidor enviar uma resposta contendo o campo **Access-Control-Allow-Origin**, o servidor aceitará a solicitação.

- **Solicitações não tão simples**

  Solicitações que não atendem às condições para solicitações simples são solicitações não tão simples.

  Antes de enviar uma solicitação não tão simples, os navegadores enviam uma solicitação de simulação HTTP ao servidor de destino para confirmar se a origem da página da Web está na lista de origem permitida e para confirmar quais métodos de solicitação HTTP e campos de cabeçalho podem ser usados. Se a solicitação de simulação for bem-sucedida, os navegadores enviam solicitações simples para o servidor.

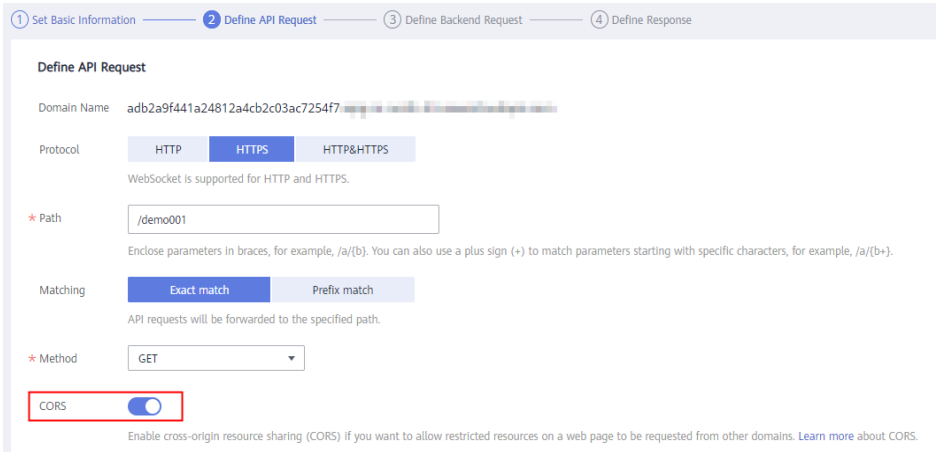
Configurar o CORS

O CORS está desativado por padrão. Para habilitar o CORS para uma API, execute as operações descritas nesta seção. Para personalizar cabeçalhos de solicitação, métodos de solicitação e origens permitidos para acesso entre domínios, crie um **plug-in CORS**.

- **Solicitações CORS simples**

  Ao criar uma API, ative o CORS na página de configuração da solicitação da API. Para obter mais informações, consulte **Solicitação simples**.

Figura 12-12 CORS



- **Solicitações CORS não tão simples**

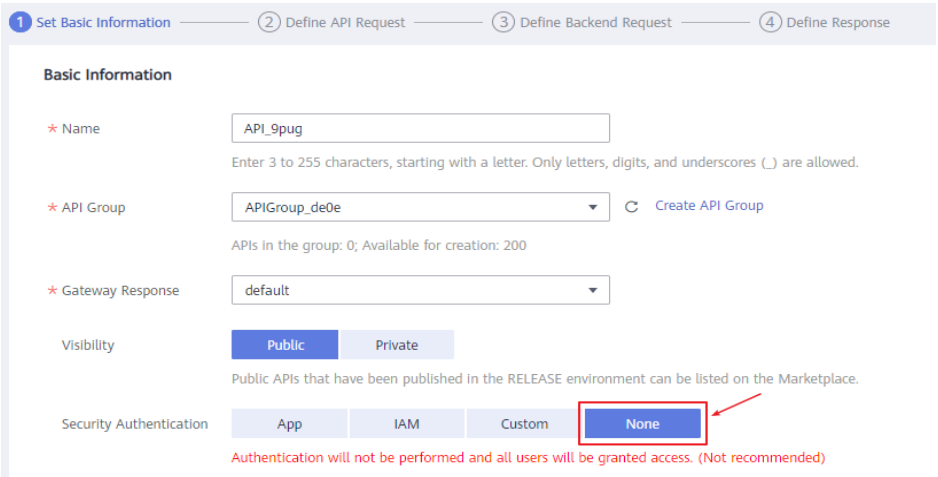
AVISO

Se sua API receber solicitações não tão simples, **crie outra API que será acessada usando o método OPTIONS** no mesmo grupo da API de destino para receber solicitações de simulação.

Siga este procedimento para definir a API de solicitação de simulação. Para obter mais informações, consulte **Solicitações não tão simples**.

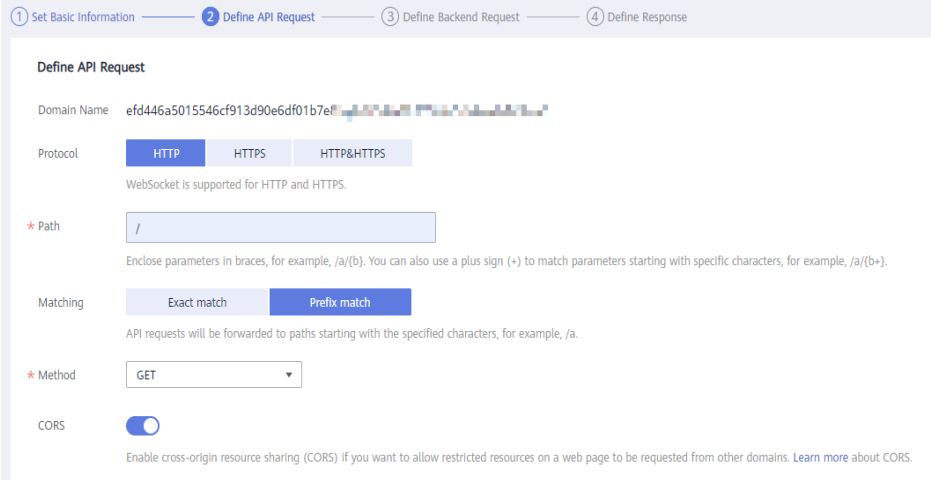
a. Na página **Set Basic Information**, selecione **None** para ignorar a autenticação de segurança.

Figura 12-13 Nenhuma autenticação



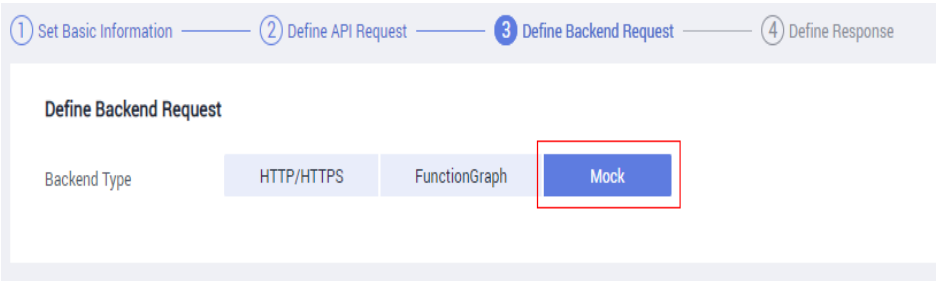
b. Na página **Define API Request**, execute as seguintes configurações:
   - **Protocol**: o mesmo protocolo usado pela API com o CORS ativado.
   - **Path**: insira uma barra (/).
   - **Method**: selecione **OPTIONS**.
   - **CORS**: ativado.

Figura 12-14 Definição da solicitação da API



c. Selecione o tipo de back-end **Mock**.

Figura 12-15 Serviço de back-end Mock



Solicitação simples

Ao criar uma API que receberá solicitações simples, **ative o CORS** para a API.

Cenário 1: se o CORS estiver habilitado e a resposta do back-end não contiver um cabeçalho CORS, o APIG tratará solicitações de qualquer domínio e retornará o cabeçalho **Access-Control-Allow-Origin**. Por exemplo:

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origem:

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

Origin: este campo é necessário para especificar a origem (**http://www.cors.com** neste exemplo) da solicitação. O APIG e o serviço de back-end determinam, com base na origem, se a solicitação é segura e pode ser aceita.

Resposta enviada pelo serviço de back-end:

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



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

Resposta enviada pelo APIG:

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

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

Access-Control-Allow-Origin: este campo é obrigatório. O asterisco (*) significa que o APIG lida com solicitações enviadas de qualquer domínio.

Cenário 2: se o CORS estiver habilitado e a resposta do back-end contiver um cabeçalho CORS, o cabeçalho substituirá o adicionado pelo APIG. As seguintes mensagens são usadas como exemplos:

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origem:

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

Origin: este campo é necessário para especificar a origem (**http://www.cors.com** neste exemplo) da solicitação. O APIG e o serviço de back-end determinam, com base na origem, se a solicitação é segura e pode ser aceita.

Resposta enviada pelo serviço de back-end:

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

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

Access-Control-Allow-Origin: indica que o serviço de back-end aceita solicitações enviadas do **http://www.cors.com**.

Resposta enviada pelo APIG:

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

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

O cabeçalho CORS na resposta de back-end substitui o da resposta do APIG.

Solicitações não tão simples

Ao criar uma API que receberá solicitações não tão simples, habilite o CORS para a API seguindo as instruções em **Configurar o CORS** e crie outra API que será acessada usando o método OPTIONS.

> **NOTA**
>
> Se você usar o plug-in CORS para uma API, não precisará criar outra API que use o método OPTIONS.

Os parâmetros de solicitação de uma API acessada usando o método OPTIONS devem ser definidos da seguinte forma:

- **API Group**: o mesmo grupo ao qual a API com CORS habilitado pertence.
- **Security Authentication**: selecione **None**. Nenhuma autenticação é necessária para solicitações recebidas pela nova API, independentemente do modo de autenticação de segurança selecionado.
- **Protocol**: o mesmo protocolo usado pela API com o CORS ativado.
- **Path**: insira uma barra (/) ou selecione o caminho que foi definido ou corresponda à API com CORS ativado.
- **Method**: selecione **OPTIONS**.
- **CORS**: ativado.

A seguir estão exemplos de solicitações e respostas enviadas para ou de um back-end mock.

Solicitação enviada de um navegador para uma API que é acessada usando o método OPTIONS:

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

- **Origin**: esse campo é necessário para especificar a origem da qual a solicitação foi enviada.
- **Access-Control-Request-Method**: este campo é necessário para especificar os métodos HTTP a serem usados pelas solicitações simples subsequentes.
- **Access-Control-Request-Headers**: esse campo é opcional e usado para especificar os campos de cabeçalho adicionais nas solicitações simples subsequentes.

Resposta enviada pelo back-end: nenhuma

Resposta enviada pelo APIG:

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



```
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Max-Age: 172800
```

- **Access-Control-Allow-Origin**: este campo é obrigatório. O asterisco (*) significa que o APIG lida com solicitações enviadas de qualquer domínio.
- **Access-Control-Allow-Headers**: este campo é obrigatório se estiver contido na solicitação. Indica todos os campos de cabeçalho que podem ser usados durante o acesso entre origens.
- **Access-Control-Expose-Headers**: estes são os campos de cabeçalho de resposta que podem ser visualizados durante o acesso entre regiões.
- **Access-Control-Allow-Methods**: este campo é necessário para especificar quais métodos de solicitação HTTP o APIG suporta.
- **Access-Control-Max-Age**: este campo é opcional e usado para especificar o período de tempo (em segundos) durante o qual o resultado da comprovação permanece válido. Não serão enviadas mais solicitações de simulação dentro do período especificado.

Solicitação enviada por um navegador e contendo o campo de cabeçalho Origin:

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

Resposta enviada pelo back-end:

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

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

Resposta enviada pelo APIG:

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

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

12.3.2.3 Depuração de uma API

Cenário

Depois de criar uma API, depure-a no console do APIG definindo cabeçalhos HTTP e parâmetros de corpo para verificar se a API está sendo executada normalmente.

NOTA

- As APIs com caminhos de solicitação de back-end contendo variáveis não podem ser depuradas.
- Se uma API tiver sido vinculada a uma política de limitação de solicitações, a política não funcionará durante a depuração da API.

Pré-requisitos

- Você criou um grupo de API e uma API.
- Você configurou o serviço de back-end da API.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

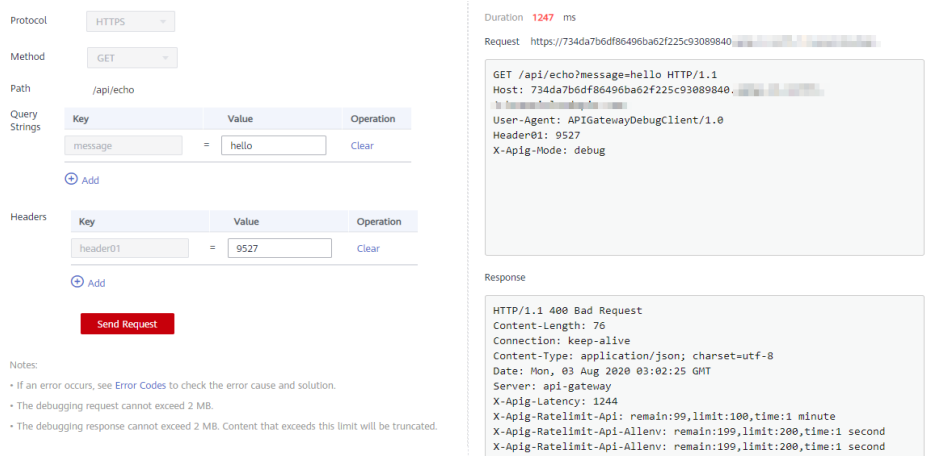
- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Depure uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da API que você deseja depurar, escolha **More** > **Debug**.
- Clique no nome da API de destino e clique em **Debug** no canto superior direito da página de detalhes da API exibida.

Figura 12-16 Depuração de uma API



No lado esquerdo, defina os parâmetros de solicitação da API listados em **Tabela 12-18**. No lado direito, veja as informações de solicitação e resposta da API depois de clicar em **Send Request**.

Tabela 12-18 Parâmetros para depurar uma API

Parâmetro	Descrição
Protocol	Esse parâmetro só pode ser modificado se você definir **Protocol** para **HTTP&HTTPS** para a API.
Method	Esse parâmetro só pode ser modificado se você definir **Method** como **ANY** para a API.
Suffix	Você só pode definir um caminho se tiver definido **Matching** ao **Prefix match** para a API.
Path	Caminho de solicitação da API.
Path Parameters	Esse parâmetro só pode ser modificado se você tiver definido parâmetros de caminho (como **{test}**) para a API.
Headers	Cabeçalhos e valores HTTP.
Query Strings	Consultar parâmetros e valores de cadeia.
Body	Esse parâmetro só pode ser modificado se você definir **Method** como **PATCH**, **POST** ou **PUT** para a API.

NOTA

Os campos exibidos na página de depuração variam de acordo com o tipo de solicitação.

Passo 7 Depois de definir os parâmetros da solicitação, clique em **Send Request**.

A caixa no canto inferior direito exibe a resposta da solicitação da API.

- Se a depuração for bem-sucedida, o código de status HTTP **200** e os detalhes da resposta serão exibidos.
- Se a solicitação não for enviada, um código de status HTTP **4xx** ou **5xx** será exibido. Para mais detalhes, consulte **Códigos de erro**.

Passo 8 Você pode enviar mais solicitações com diferentes parâmetros e valores para verificar a API.

NOTA

Para modificar as configurações da API, clique em **Edit** no canto superior direito e modifique os parâmetros na página **Edit API**.

----Fim

Operações de acompanhamento

Depois que a API for depurada com sucesso, **publique** a API em um ambiente específico para que ela possa ser chamada pelos usuários. Para garantir a segurança da API, crie políticas de limitação de solicitações (consulte **Criação de uma política de limitação de solicitações**), políticas de controle de acesso (**Criação de uma política de controle de acesso**) e chaves de assinatura (**Criação e uso de uma chave de assinatura**) para a API.

12.3.2.4 Autorização de aplicações a chamar uma API

Cenário

As APIs que usam autenticação de aplicações só podem ser chamadas por aplicações autorizadas a chamá-las.

NOTA

- Você só pode autorizar aplicações a chamar APIs publicadas.
- Você pode autorizar aplicações apenas para chamar APIs que usam autenticação de aplicação.

Pré-requisitos

- Você criou um grupo de API e uma API.
- (Opcional) Você criou um ambiente.
- Você criou uma aplicação.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

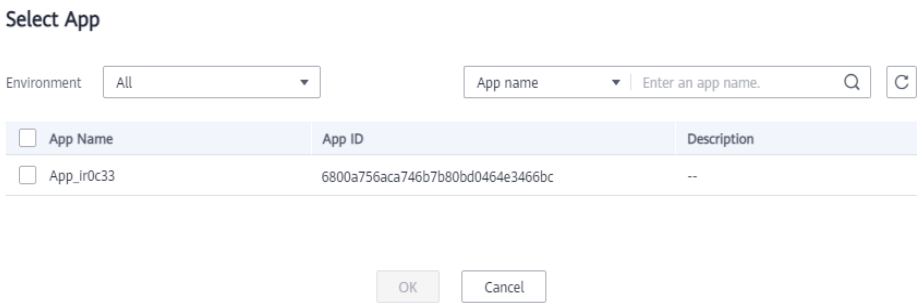
Passo 6 Autorize as aplicações a chamar uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da API de destino, escolha **More** > **Authorize App** e, em seguida, clique em **Select App**.
- Selecione a API de destino, clique em **Authorize App** na lista de APIs e, em seguida, clique em **Select App**.
- Autorize aplicações por meio da página de detalhes da API.
  a. Clique no nome da API de destino.
  b. Clique na guia **Authorization**.
  c. Clique em **Select App**.

NOTA

Para autorizar uma aplicação a acessar várias APIs, selecione as APIs e clique em **Authorize App**. Clique em **Select App**, selecione a aplicação que você deseja autorizar e clique em **OK**. Você pode conceder acesso a um máximo de 1000 APIs por vez.

Passo 7 Selecione um ambiente, procure e selecione as aplicações desejadas e clique em **OK**.



Passo 8 Após a conclusão da autorização, visualize as aplicações autorizadas na página da guia **Authorization** ou na página **Authorize App**.

NOTA

Se uma aplicação não precisar chamar a API, clique em **Cancel Authorization** na linha que contém a aplicação para desvinculá-la.

----Fim

Autorização de uma aplicação chamando uma API

Você também pode autorizar uma aplicação chamando uma API fornecida pelo APIG. Para detalhes, consulte as seguintes referências:

Autorização de aplicações

Cancelamento de autorização

Operações de acompanhamento

Depois que você autoriza uma aplicação a chamar uma API, ela pode ser chamada usando SDKs de diferentes linguagens de programação.

12.3.2.5 Publicação de uma API

Cenário

As APIs só podem ser chamadas depois de terem sido publicadas em um ambiente. Você pode publicar APIs em diferentes ambientes. O APIG permite que você visualize o histórico de publicações (como a versão, a descrição, a hora e o ambiente) de cada API e suporta a reversão de APIs para diferentes versões históricas.

NOTA

- Se você modificar uma API publicada, deverá publicá-la novamente para que as modificações entrem em vigor no ambiente em que a API foi publicada.
- Um máximo de 10 registros de publicação de uma API são retidos em um ambiente.

Pré-requisitos

- Você criou um grupo de API e uma API.
- Você criou um ambiente.

Publicação de uma API

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Publique uma API. Você pode usar um dos seguintes métodos:

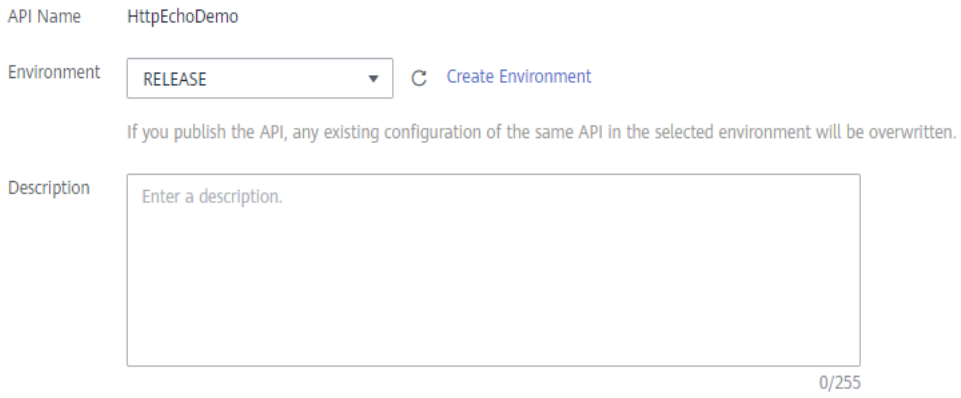
- Clique em **Publish** na linha que contém a API que você deseja publicar.
- Clique no nome da API de destino e clique em **Publish** no canto superior direito da página de detalhes da API exibida.

NOTA

Para publicar várias APIs, selecione as APIs e clique em **Publish**. Você pode publicar no máximo 1.000 APIs por vez.

Passo 7 Selecione o ambiente onde a API será publicada e insira uma descrição.

Figura 12-17 Publicação de uma API



NOTA

- Se a API já tiver sido publicada no ambiente, publicá-la novamente substituirá sua definição nesse ambiente.
- Se não houver um ambiente que atenda aos seus requisitos, crie um novo.

Passo 8 Clique em **Publish**.

----Fim

Visualizar o histórico de publicações

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

Shared Gateway: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.

Dedicated Gateways: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

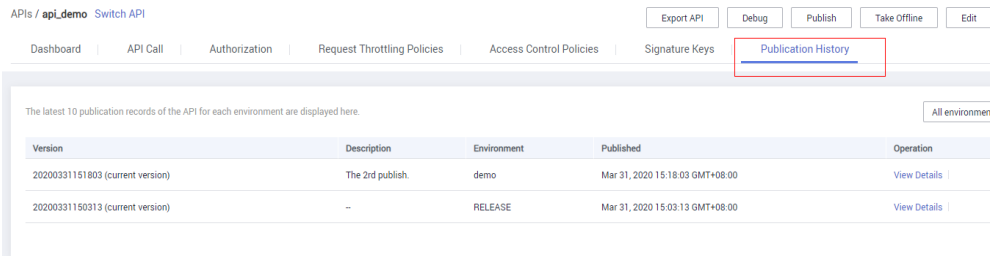
Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Clique no nome da API de destino.

Passo 7 Clique na guia **Publication History**.

O histórico de publicações da API é exibido.

Figura 12-18 Visualizar o histórico de publicações



Passo 8 Clique em **View Details** na coluna **Operation** de uma versão.

A caixa de diálogo **View Details** exibe as informações básicas, informações de solicitação de front-end e back-end, parâmetros de entrada e constantes, mapeamentos de parâmetros e respostas de exemplo da API.

Passo 9 Para reverter a API para uma versão histórica, clique em **Switch Version** na linha que contém a versão de destino e clique em **Yes**.

Se a "versão atual" for exibida ao lado da versão de destino, a reversão foi bem-sucedida.

Quando a API é chamada, a configuração da versão atual é usada em vez da configuração salva anteriormente.

Por exemplo, uma API foi publicada no ambiente RELEASE em 1º de agosto de 2018. Em 20 de agosto de 2018, a API foi publicada no mesmo ambiente após modificação. Se a versão publicada em 1º de agosto for definida como a versão atual, a configuração dessa versão será usada quando a API for chamada.

----Fim

Publicar uma API chamando uma API

Você também pode publicar uma API chamando uma API fornecida pelo APIG. Para obter detalhes, consulte a seguinte referência:

Publicação de uma API

Perguntas frequentes sobre a publicação de APIs

Precisar publicar uma API novamente após a modificação?

Por que as APIs publicadas em um ambiente não RELEASE não podem ser acessadas?

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

12.3.2.6 Deixar uma API off-line

Cenário

Você pode remover APIs que não são necessárias dos ambientes em que as APIs foram publicadas.

AVISO

Essa operação fará com que as APIs fiquem inacessíveis nos ambientes. Certifique-se de que notificou os usuários antes desta operação.

Pré-requisitos

- Você criou um grupo de API e uma API.
- Você publicou a API.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Coloque a API off-line. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da API de destino, escolha **More** > **Take Offline**.
- Clique no nome da API de destino e clique em **Take Offline** no canto superior direito da página de detalhes da API.

NOTA

Para colocar várias APIs off-line, selecione as APIs e clique em **Take Offline**. Você pode colocar no máximo 1000 APIs off-line por vez.

Passo 7 Selecione o ambiente do qual você deseja colocar a API off-line e clique em **Yes**.

----Fim

Colocar uma API off-line chamando uma API

Você também pode colocar uma API off-line chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Deixar uma API off-line**.

Operações de acompanhamento

Depois de colocar uma API off-line, exclua-a com base nas instruções fornecidas em **Exclusão de uma API**.

12.3.2.7 Exclusão de uma API

Cenário

Você pode excluir as APIs publicadas que não são mais necessárias.

AVISO

- As APIs excluídas não podem ser acessadas por aplicações ou usuários que estavam usando as APIs, portanto, certifique-se de notificar os usuários antes da exclusão.
- As APIs publicadas devem primeiro ser colocadas off-line e depois excluídas.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Exclua a API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da API que você deseja excluir, escolha **More** > **Delete**.
- Clique no nome da API de destino e clique em **Delete** no canto superior direito da página de detalhes da API exibida.

NOTA

Para excluir várias APIs, selecione as APIs e clique em **Delete**. Você pode excluir no máximo 1.000 APIs por vez.

Passo 7 Digite **DELETE** e clique em **Yes**.

----Fim

Excluir uma API chamando uma API

Você também pode excluir uma API chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de uma API**.

12.3.2.8 Importação de APIs

Cenário

O APIG permite importar APIs do Swagger 2.0 para grupos de APIs existentes ou novos. Swagger é uma ferramenta de código aberto construída com base nas especificações OpenAPI para projetar, construir, gravar e usar APIs REST.

Você pode importar APIs individualmente ou em lotes, dependendo do número de APIs contidas em um arquivo Swagger.

Pré-requisitos

- O arquivo API Swagger a ser importado está disponível e já tem definições de API estendidas suplementadas. Para obter mais informações, consulte **Definição estendida**.
- Você tem cotas suficientes de grupos de APIs e APIs.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Clique em **Import API**.

Passo 7 Defina os parâmetros listados em **Tabela 12-19**.

Figura 12-19 Importação de APIs

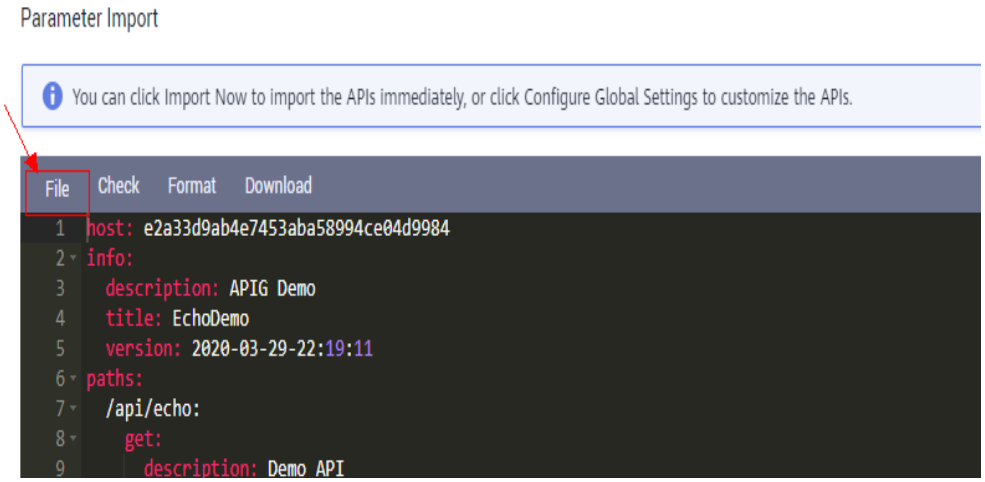
Tabela 12-19 Parâmetros para importar APIs

Parâmetro	Descrição
Import	Opções: ● **New group**: importar APIs para um novo grupo de APIs. Se você selecionar essa opção, o sistema criará automaticamente um grupo de APIs e importará as APIs para esse grupo. ● **Existing group**: importar APIs para um grupo de APIs existente. Se você selecionar essa opção, o sistema adicionará as APIs ao grupo de APIs selecionado, mantendo as APIs existentes no grupo de APIs.
API group	Selecione um grupo de API se você definir **Import** para **Existing group**.
Basic Definition Overwrite	Determine se deve substituir uma API existente se o nome da API for o mesmo de uma API importada. Este parâmetro está disponível somente se você definir **Import** para **Existing group**.
Extended Definition Overwrite	Se essa opção estiver selecionada, os itens de definição estendida (controle de acesso e políticas de limitação de solicitações) de uma API importada substituirão as políticas existentes com o mesmo nome.

Passo 8 Na área **Parameter Import**, clique em **File** e selecione um arquivo a ser importado.

Arquivos YAML e JSON são suportados. Você pode visualizar o conteúdo da API a ser importado na página **Import API**.

Figura 12-20 Importação de parâmetro



Passo 9 (Opcional) Defina configurações globais para as APIs a serem importadas.

Você pode definir as configurações globais das APIs, como solicitações de front-end e back-end ou modificar outros parâmetros das APIs.

Figura 12-21 Configuração de configurações globais

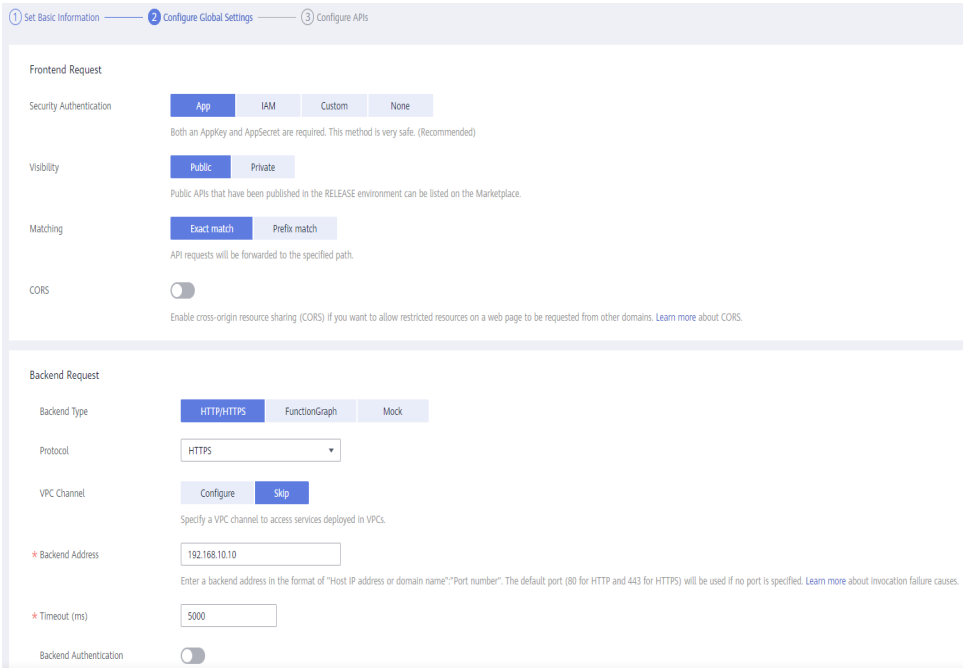
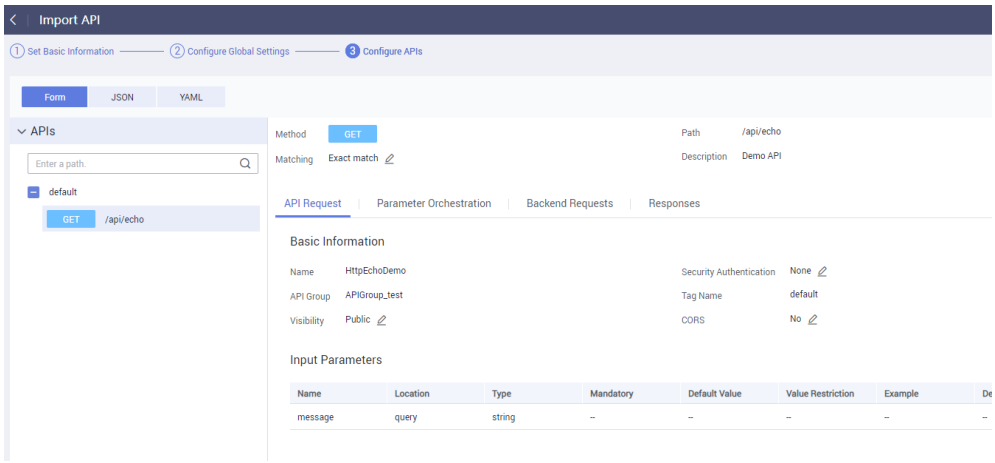


Figura 12-22 Modificação de APIs



Passo 10 Clique em **Import Now** para importar as APIs.

NOTA

As APIs importadas devem ser publicadas manualmente para que fiquem disponíveis para acesso dos usuários.

----Fim

Operações de acompanhamento

Publique a API importada em um ambiente para que possa ser chamada pelos usuários.

12.3.2.9 Exportação de APIs

Cenário

Você pode exportar APIs uma a uma ou em lotes como arquivos JSON ou YAML.

Pré-requisitos

Você criou um grupo de API e uma API.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 Clique em **Export API**.

Passo 6 Defina os parâmetros listados em **Tabela 12-20**.

Figura 12-23 Exportação de APIs

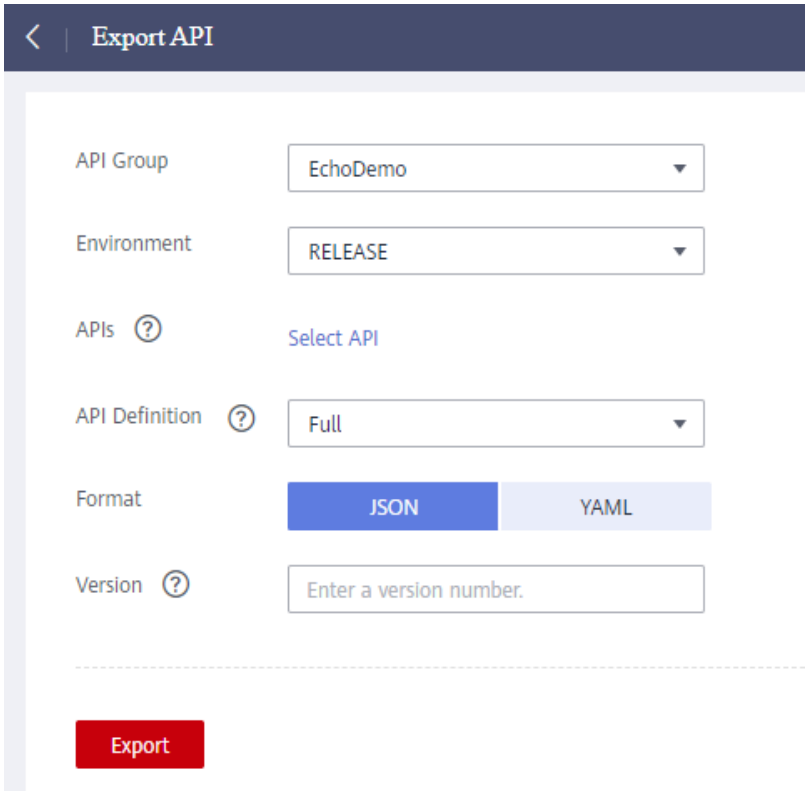


Tabela 12-20 Parâmetros para exportação de APIs

Parâmetro	Descrição
API Group	Selecione o grupo de APIs do qual as APIs serão exportadas.
Environment	Selecione o ambiente onde as APIs a serem exportadas foram publicadas.
APIs	Por padrão, todas as APIs do grupo de APIs publicadas no ambiente selecionado são exportadas. Para exportar apenas APIs específicas, clique em **Select API** e especifique as APIs que deseja exportar.

Parâmetro	Descrição
API Definition	● **Basic**: a definição básica de uma API é composta pelas definições de solicitação e resposta. Não inclui a definição de back-end. A definição de solicitação inclui campos Swagger padrão e estendido. ● **Full**: a definição completa de uma API é composta pelas definições de solicitação, back-end e resposta. ● **Extended**: a definição estendida de uma API é composta pelas definições de solicitação, back-end e resposta, bem como pela política de limitação de solicitações, política de controle de acesso e outras configurações da API.
Format	Exporte APIs em formato **JSON** ou **YAML**.
Version	Defina a versão das APIs a serem exportadas. Se você não especificar uma versão, a versão será definida como a data e a hora atuais.

Passo 7 Clique em **Export**.

O resultado da exportação é exibido à direita.

----Fim

12.3.3 Limitação de solicitação

12.3.3.1 Criação de uma política de limitação de solicitações

Cenário

A limitação de solicitações controla o número de vezes que uma API pode ser chamada dentro de um período de tempo para proteger os serviços de back-end.

Para fornecer serviços estáveis e ininterruptos, você pode criar políticas de limitação de solicitações para controlar o número de chamadas feitas às suas APIs.

As políticas de limitação de solicitação entram em vigor para uma API somente se tiverem sido vinculadas à API.

NOTA

- Uma API pode ser vinculada a apenas uma política de limitação de solicitações para um determinado ambiente, mas cada política de limitação de solicitações pode ser vinculada a várias APIs.
- Para o gateway compartilhado, o limite de solicitação padrão é de 200 chamadas por segundo. Para um gateway dedicado, o limite é o valor de **ratelimit_api_limits** que você configurou na página **Configuration Parameters**.

Pré-requisitos

Você **publicou a API** à qual deseja vincular uma política de limitação de solicitações.

Criação de uma política de limitação de solicitações

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

Passo 6 Clique em **Create Request Throttling Policy** e defina os parâmetros listados em **Tabela 12-21**.

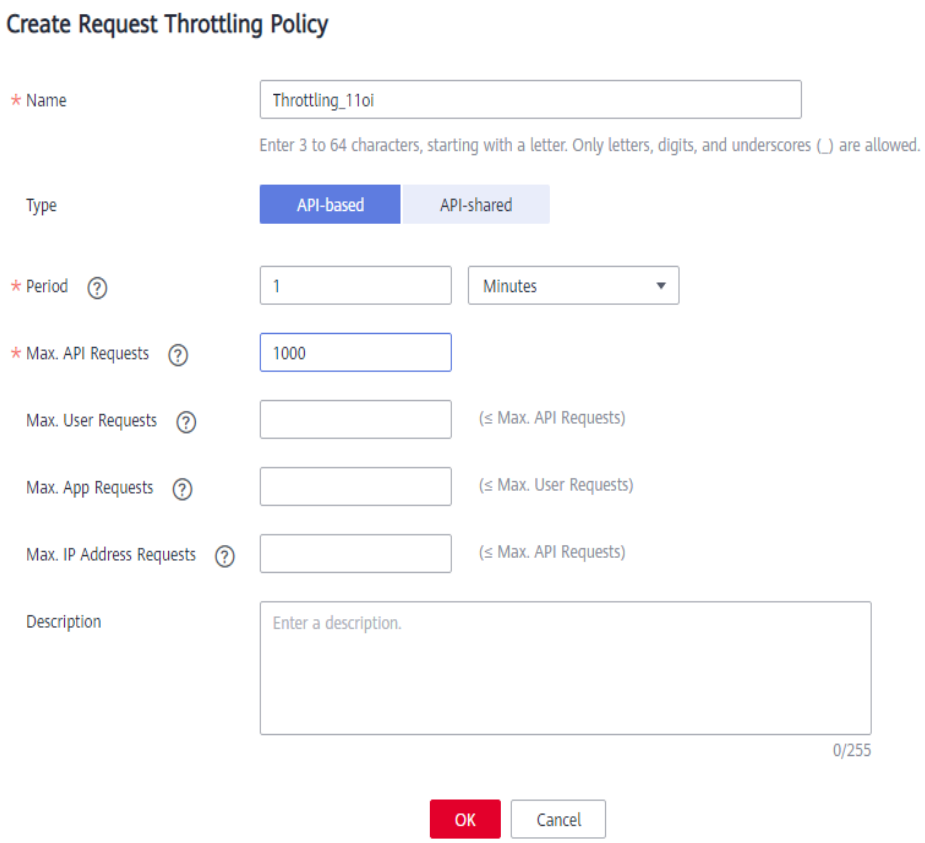


Tabela 12-21 Parâmetros para criar uma política de limitação de solicitações

Parâmetro	Descrição
Name	Nome da política de limitação de solicitação.

Parâmetro	Descrição
Type	Limitação de solicitação baseada em API ou compartilhada por API. ● **API-based**: a limitação de solicitações é baseada em todas as APIs às quais a política está vinculada. ● **API-shared**: a limitação de solicitações baseia-se em todas as APIs como um todo às quais a política está vinculada.
Period	Por quanto tempo você deseja limitar o número de chamadas de API. Este parâmetro pode ser usado em conjunto com os seguintes parâmetros: ● **Max. API Requests**: limite o número máximo de vezes que uma API pode ser chamada em um período específico. ● **Max. User Requests**: limite o número máximo de vezes que uma API pode ser chamada por um usuário dentro de um período específico. ● **Max. App Requests**: limite o número máximo de vezes que uma API pode ser chamada por uma aplicação em um período específico. ● **Max. IP Address Requests**: limite o número máximo de vezes que uma API pode ser chamada por um endereço IP dentro de um período específico.
Max. API Requests	O número máximo de vezes que cada API vinculada pode ser chamada dentro do período especificado. Este parâmetro deve ser utilizado em conjunto com o **Period**.
Max. User Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um usuário dentro do período especificado. **Esse limite se aplica apenas às APIs acessadas por meio da autenticação do IAM.** ● O valor deste parâmetro não pode exceder o de **Máximo de solicitações de API**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**. ● Se houver muitos usuários na sua conta que acessam uma API, os limites de limitação de solicitações da API serão aplicados a todos esses usuários.
Max. App Requests	O número máximo de vezes que cada API vinculada pode ser chamada por uma aplicação dentro do período especificado. **Esse limite só se aplica a APIs acessadas por meio da autenticação da aplicação.** ● O valor deste parâmetro não pode exceder o de **Max. User Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Max. IP Address Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um endereço IP dentro do período especificado. ● O valor deste parâmetro não pode exceder o de **Máximo de solicitações de API**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Description	Descrição da política de limitação de solicitação.

Passo 7 Clique em **OK**.

Depois que a política é criada, ela é exibida na página **Request Throttling**. Você pode vincular essa política a APIs para limitar as solicitações de API.

----Fim

Vinculação de uma política de limitação de solicitações a uma API

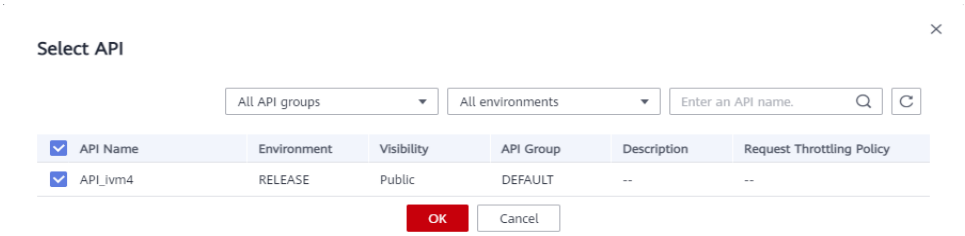
Passo 1 Acesse a página para vincular uma política de limitação de solicitações a uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da política de limitação de solicitação a ser vinculada, clique em **Bind to API** e, em seguida, clique em **Select API**.
- Clique no nome da política de limitação de solicitações de destino e clique em **Select API** na página de guia **APIs**.

Passo 2 Especifique um grupo de APIs, um ambiente e uma palavra-chave de nome de API para pesquisar a API desejada.

Passo 3 Selecione a API e clique em **OK**.

Figura 12-24 Vinculação de uma política de limitação de solicitações a uma API



NOTA

Se uma política de limitação de solicitações não for mais necessária para uma API, você poderá desvinculá-la. Para desvincular uma política de limitação de solicitação de várias APIs, selecione as APIs e clique em **Unbind**. Você pode desvincular uma política de limitação de solicitações de no máximo 1000 APIs por vez.

----Fim

Criação, vinculação e desvinculação de uma política de limitação de solicitações chamando uma API

Você também pode criar uma política de limitação de solicitações, vinculá-la a APIs ou desvinculá-la de APIs chamando uma API fornecida pelo APIG. Para detalhes, consulte as seguintes referências:

Criação de uma política de limitação de solicitações

Vinculação de uma política de limitação de solicitações

Desvinculação de uma política de limitação de solicitações

Operações de acompanhamento

Para controlar o número máximo de chamadas de API recebidas de uma aplicação ou locatário específico, especifique a aplicação ou locatário a ser excluído referindo-se a **Adição de uma aplicação ou locatário excluído**. Se uma aplicação for excluída em uma política de limitação de solicitações, qualquer limite configurado para essa aplicação terá precedência sobre a política de limitação de solicitações. A API e os limites de solicitação do usuário dessa política ainda são válidos. Se um locatário for excluído em uma política de limitação de solicitação, qualquer limite configurado para esse locatário será aplicado. Os limites de solicitação de API e aplicação desta política ainda são válidos.

12.3.3.2 Exclusão de uma política de limitação de solicitações

Cenário

Você pode excluir as políticas de limitação de solicitações que não são mais necessárias.

Pré-requisitos

Você criou uma política de limitação de solicitações.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

Passo 6 Exclua uma política de limitação de solicitações. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da política de limitação de solicitações que você deseja excluir, clique em **Delete**.
- Clique no nome da política de limitação de solicitações de destino e clique em **Delete** no canto superior direito da página de detalhes da política de limitação de solicitações exibida.

NOTA

- Se uma política de limitação de solicitações tiver sido vinculada a uma API, desvincule a política e exclua-a. Para desvincular uma política de limitação de solicitações, vá para a página de detalhes da política, clique em **Unbind** na linha que contém a API da qual você deseja desvincular a política e clique em **Yes**.
- Para excluir várias políticas de limitação de solicitações, selecione as políticas e clique em **Delete**. Você pode excluir no máximo 1000 políticas de limitação de solicitações por vez.

Passo 7 Clique em **Yes**.

----Fim

Excluir uma política de limitação de solicitações chamando uma API

Você também pode excluir uma política de limitação de solicitações chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de uma política de limitação de solicitações**.

12.3.3.3 Adição de uma aplicação ou locatário excluído

Cenário

Se você quiser controlar o número de chamadas de API recebidas de uma aplicação ou locatário específico, adicione uma aplicação ou locatário excluído a uma política de limitação de solicitações.

Pré-requisitos

Você criou uma aplicação ou obteve um ID de aplicação de outra conta ou um ID de conta.

Adicionar uma aplicação excluída

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

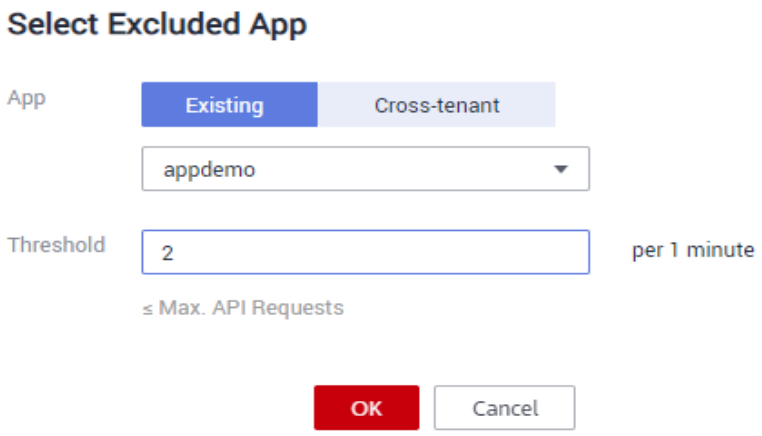
Passo 6 Clique no nome da política de limitação de solicitações de destino.

Passo 7 Na página de detalhes da política de limitação de solicitação exibida, clique na guia **Excluded Apps**.

Passo 8 Clique em **Select Excluded App**.

Passo 9 Selecione uma aplicação para excluir. Você pode usar um dos seguintes métodos:

Figura 12-25 Adicionar uma aplicação excluída



- Para selecionar uma aplicação existente, clique em **Existing**, selecione uma aplicação e insira um limite.
- Para selecionar uma aplicação de outros locatários, clique em **Cross-tenant** e insira o ID da aplicação e um limite.

NOTA

O limite deve ser um número inteiro positivo e não pode exceder o valor de **Max. API Requests**.

----Fim

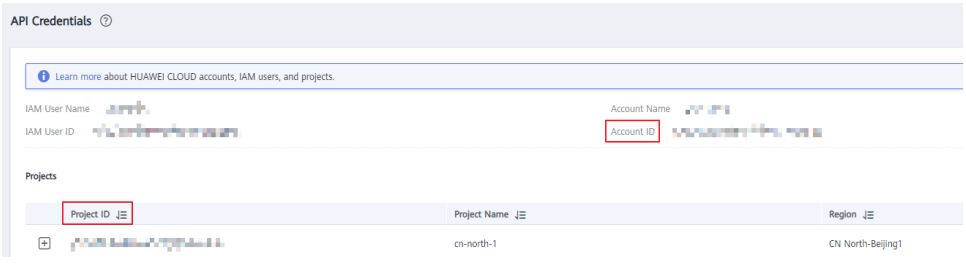
Adicionar um locatário excluído

Passo 1 Acesse o console de gerenciamento.

Passo 2 Passe o ponteiro do mouse sobre o nome de usuário e escolha **My Credentials** na lista suspensa.

Passo 3 Na página **API Credentials**, visualize o ID da conta e o ID do projeto.

Figura 12-26 Exibição do ID da conta e o ID do projeto



Passo 4 Clique em no canto superior esquerdo e selecione uma região.

Passo 5 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 6 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.

- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 7 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

Passo 8 Clique no nome da política de limitação de solicitações de destino.

Passo 9 Clique na guia **Excluded Tenants**.

Passo 10 Clique em **Select Excluded Tenant**.

Passo 11 Na caixa de diálogo **Select Excluded Tenant**, defina os parâmetros listados em **Tabela 12-22**.

Figura 12-27 Adicionar um locatário excluído

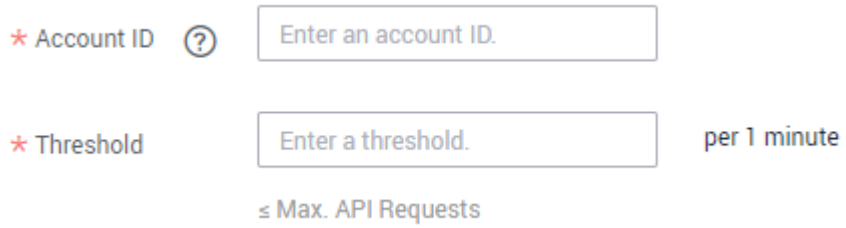


Tabela 12-22 Configuração de locatário excluído

Parâmetro	Descrição
Account ID	ID da conta ou ID do projeto obtido em **Passo 3**. ● Insira um ID de projeto se você vincular ou tiver vinculado esta política a uma API que usa autenticação de aplicação. ● Insira um ID de conta se for vincular ou tiver vinculado esta política a uma API que usa autenticação do IAM.
Threshold	O número máximo de vezes que uma API pode ser chamada pelo locatário dentro de um período especificado. O valor deste parâmetro não pode exceder o de **Max. API Requests**.

Passo 12 Clique em **OK**.

NOTA

Limites de locatários excluídos têm precedência sobre o valor de **Max. User Requests**.

Por exemplo, suponha que uma política de limitação de solicitação esteja configurada, com **Max. API Requests** sendo **10**, **Max. User Requests** sendo **3**, **Period** sendo 1 minuto e dois locatários excluídos (máximo de **2** solicitações de API para o locatário A e máximo de **4** solicitações de API para o locatário B). Se a política de limitação de solicitações estiver vinculada a uma API, os locatários A e B poderão acessar a API 2 e 4 vezes em 1 minuto, respectivamente.

----Fim

Adição de uma aplicação ou locatário excluído chamando uma API

Você também pode adicionar uma aplicação ou locatário excluído a uma política de limitação de solicitações chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Criação de uma configuração de limitação de solicitação excluída**.

12.3.3.4 Remoção de uma aplicação ou locatário excluído

Cenário

Você pode remover aplicações ou locatários excluídos de uma política de limitação de solicitação. Esta seção usa uma aplicação excluída como exemplo.

Pré-requisitos

- Você criou uma política de limitação de solicitações.
- Você já adicionou uma aplicação ou locatário excluído à política de limitação de solicitações.

Remoção de uma aplicação excluída

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

Passo 6 Clique no nome da política de limitação de solicitações de destino.

Passo 7 Clique na guia **Excluded Apps** na página de detalhes da política de limitação de solicitação exibida.

Passo 8 Na coluna **Operation** da aplicação que você deseja remover, clique em **Remove**.

Passo 9 Clique em **Yes**.

----Fim

Remoção de um locatário excluído

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Request Throttling**.

Passo 6 Clique no nome da política de limitação de solicitações de destino.

Passo 7 Clique na guia **Excluded Tenants**.

Passo 8 Na coluna **Operation** do locatário que deseja remover, clique em **Remove**.

Passo 9 Clique em **Yes**.

----Fim

Remoção de uma aplicação ou locatário excluído chamando uma API

Você também pode remover uma aplicação ou locatário excluído de uma política de limitação de solicitação chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de uma configuração de limitação de solicitação excluída**.

12.3.4 Controle de acesso

12.3.4.1 Criação de uma política de controle de acesso

Cenário

As políticas de controle de acesso são um tipo de medidas de segurança fornecidas pelo APIG. Você pode usá-los para permitir ou negar acesso à API de endereços IP ou contas específicos.

As políticas de controle de acesso terão efeito para uma API somente se elas tiverem sido vinculadas à API.

NOTA

Cada API pode ser vinculada a apenas uma política de controle de acesso para um determinado ambiente, mas cada política de controle de acesso pode ser vinculada a várias APIs.

Criação de uma política de controle de acesso

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.

- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Access Control**.

Passo 6 Clique em **Create Access Control Policy**.

Passo 7 Na caixa de diálogo **Create Access Control Policy**, defina os parâmetros listados em **Tabela 12-23**.

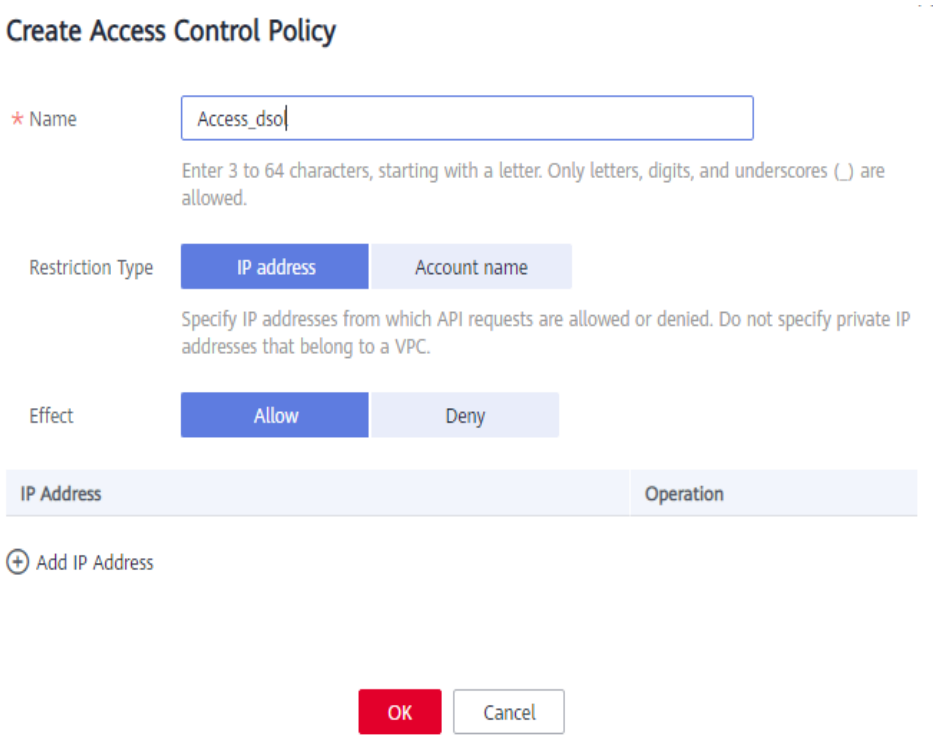


Tabela 12-23 Parâmetros para criação de uma política de controle de acesso

Parâmetro	Descrição
Name	Nome da política de controle de acesso.
Restriction Type	Tipo da origem a partir da qual as chamadas de API devem ser controladas. ● **IP address**: especifique endereços IP e intervalos de endereços IP que têm ou não permissão para acessar uma API. ● **Account name**: especifique os nomes das contas que têm ou não permissão para acessar uma API.
Effect	Opções: **Allow** e **Deny**. Use esse parâmetro junto com **Restriction Type** para controlar o acesso de determinados endereços IP ou contas a uma API.

Parâmetro	Descrição
IP Address	Endereços IP e intervalos de endereços IP que têm ou não permissão para acessar uma API Você precisa definir esse parâmetro somente se tiver definido **Restriction Type** como **IP address**. **NOTA** Você pode definir um máximo de 100 endereços IP, respectivamente, para permitir ou negar acesso.
Account Names	Nomes das contas que têm ou não permissão para acessar uma API. **Este parâmetro se aplica apenas a APIs que são acessadas por meio da autenticação do IAM.** Você precisa definir esse parâmetro apenas se tiver definido **Restriction Type** como **Account name**. Você pode inserir vários nomes de conta e separá-los com vírgulas, por exemplo, **aaa,bbb**. **NOTA** O APIG executa o controle de acesso em contas, não em usuários do IAM criados usando contas.

Passo 8 Clique em **OK**. Você pode vincular a política a APIs para controlar o acesso à API.

----Fim

Vinculação de uma política de controle de acesso a uma API

Passo 1 Acesse a página para vincular uma política de controle de acesso a uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da política de controle de acesso a ser vinculada, clique em **Bind to API** e, em seguida, clique em **Select API**.
- Clique no nome da política de controle de acesso de destino e clique em **Select API**.

Passo 2 Especifique um grupo de APIs, um ambiente e uma palavra-chave de nome de API para pesquisar a API desejada.

Passo 3 Selecione a API e clique em **OK**.

NOTA

Se uma política de controle de acesso não for mais necessária para uma API, você poderá desvinculá-la dessa API. Para desvincular uma política de controle de acesso de várias APIs, selecione as APIs e clique em **Unbind**. Você pode desvincular uma política de limitação de solicitações de no máximo 1000 APIs por vez.

----Fim

12.3.4.2 Exclusão de uma política de controle de acesso

Cenário

Você pode excluir políticas de controle de acesso que você não precisa mais.

Pré-requisitos

Você criou uma política de controle de acesso.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Access Control**.

Passo 6 Exclua uma política de controlo de acesso utilizando um dos seguintes métodos:

- Na coluna **Operation** da política de controle de acesso que você deseja excluir, clique em **Delete**.
- Clique no nome da política de controle de acesso de destino e clique em **Delete** no canto superior direito da página de detalhes da política de controle de acesso exibida.

NOTA

- Se uma política de controle de acesso tiver sido vinculada a APIs, desvincule-a e exclua-a.
- Para excluir várias políticas de controle de acesso, selecione as políticas e clique em **Delete**. Você pode excluir um máximo de 1000 políticas de controle de acesso por vez.

Passo 7 Clique em **Yes**.

----Fim

12.3.5 Gerenciamento de ambiente

12.3.5.1 Criação de um ambiente e uma variável de ambiente

Cenário

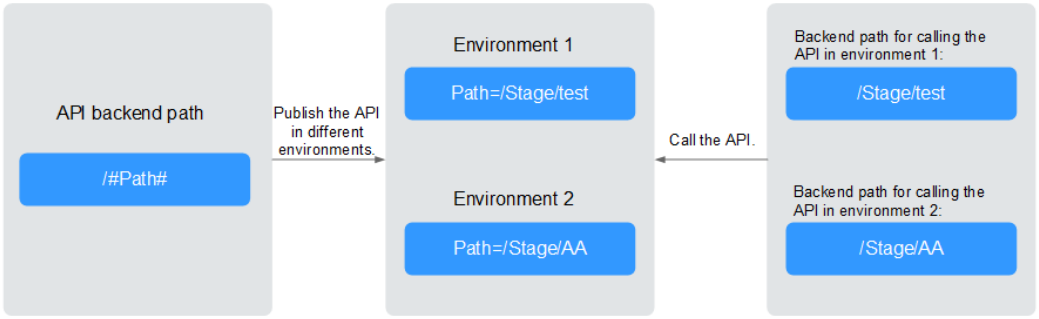
Uma API pode ser chamada em diferentes ambientes, como ambientes de produção, teste e desenvolvimento. RELEASE é o ambiente padrão fornecido pelo APIG. Você pode definir variáveis de ambiente para permitir que uma API seja chamada em ambientes diferentes.

As variáveis de ambiente são gerenciáveis e específicas para ambientes. Você pode criar variáveis em ambientes diferentes para chamar diferentes serviços de back-end usando a mesma API.

Para variáveis definidas durante a criação da API, você deve criar variáveis e valores correspondentes. Por exemplo, a variável **Path** é definida para uma API e duas variáveis com

o mesmo nome são criadas e atribuídas valores **/Stage/test** e **/Stage/AA** nos ambientes 1 e 2, respectivamente. Se a API for publicada e chamada no ambiente 1, o caminho **/Stage/test** será usado. Se a API for publicada e chamada no ambiente 2, o caminho **/Stage/AA** será usado.

Figura 12-28 Uso de variáveis de ambiente



NOTA

Você pode criar no máximo 50 variáveis para um grupo de API em cada ambiente.

Pré-requisitos

Você **criou um grupo de APIs**.

Criação de um ambiente

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Environments**.

Passo 6 Clique em **Create Environment** e defina os parâmetros listados em **Tabela 12-24**.

Figura 12-29 Criação de um ambiente

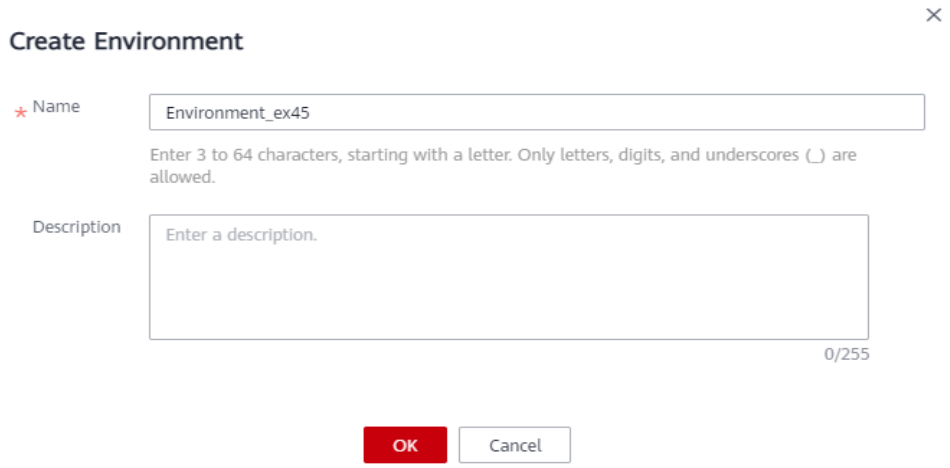


Tabela 12-24 Informações de ambiente

Parâmetro	Descrição
Name	Nome do ambiente.
Description	Descrição do ambiente.

Passo 7 Clique em **OK**.

Depois que o ambiente é criado, ele é exibido na lista de ambientes.

----Fim

Acessar um ambiente

Você pode chamar uma API no ambiente RELEASE usando uma API RESTful. Para acessar a API em outros ambientes, adicione o cabeçalho **X-Stage** à solicitação para especificar um nome de ambiente. Por exemplo, adicione **X-Stage:DEVELOP** ao cabeçalho da solicitação para acessar uma API no ambiente **DEVELOP**.

NOTA

O APIG não suporta depuração de API usando variáveis de ambiente.

Criação de uma variável de ambiente

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.

- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **API Groups**.

Passo 6 Crie uma variável. Você pode usar um dos seguintes métodos:

- Clique no nome do grupo de API de destino e clique na guia **Variables** na página de detalhes do grupo de API exibida.
- Na coluna **Operation** do grupo de APIs de destino, escolha **More** > **Manage Variable**.

Passo 7 Selecione um ambiente na lista suspensa **Environment** e clique em **Create Variable**.

Passo 8 Defina os parâmetros listados em **Tabela 12-25**.

Figura 12-30 Criação de uma variável de ambiente

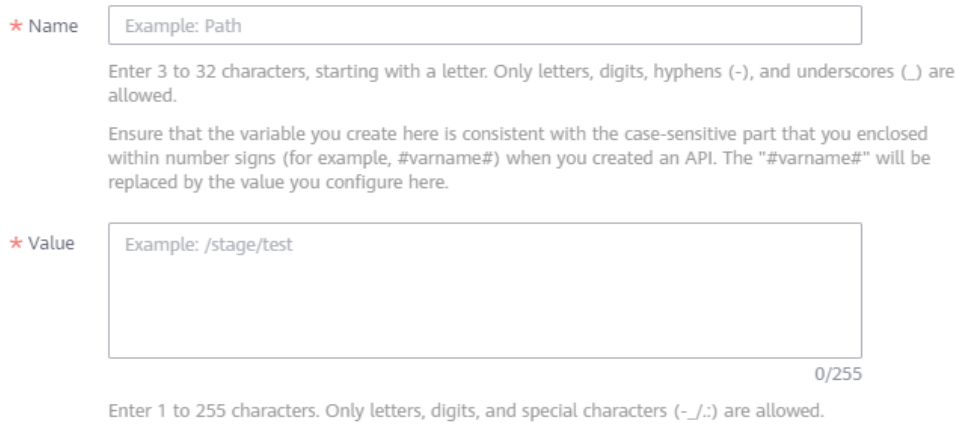


Tabela 12-25 Parâmetros para criar uma variável de ambiente

Parâmetro	Descrição
Name	Nome da variável que você deseja criar. Verifique se o nome é igual ao nome da variável definida para a API.
Value	O caminho a ser usado no ambiente selecionado.

Passo 9 Clique em **OK**.

NOTA

Se uma variável não for necessária, clique em **Delete** na linha que contém a variável para excluí-la.

Os nomes e valores das variáveis de ambiente serão exibidos em texto sem formatação nas solicitações da API. Não inclua informações confidenciais nos nomes e valores das variáveis.

----Fim

Operações de acompanhamento

Depois de criar um ambiente e uma variável, **publique APIs** no ambiente para que possam ser chamadas pelos chamadores da API.

Criação de um ambiente e variável de ambiente chamando uma API

Você também pode criar um ambiente e uma variável de ambiente chamando uma API fornecida pelo APIG. Para detalhes, consulte as seguintes referências:

Criação de um ambiente

Criação de uma variável de ambiente

Perguntas frequentes sobre variáveis de ambiente

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

12.3.5.2 Exclusão de um ambiente

Cenário

Você pode excluir ambientes que você não precisa mais.

Pré-requisitos

Você criou um ambiente.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Environments**.

Passo 6 Na coluna **Operation** do ambiente que deseja excluir, clique em **Delete**.

NOTA

Você pode excluir um ambiente somente se nenhuma API tiver sido publicada no ambiente.

Passo 7 Clique em **Yes**.

----Fim

Exclusão de um ambiente chamando uma API

Você também pode excluir um ambiente chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de um ambiente**.

12.3.6 Gerenciamento de chaves de assinatura

12.3.6.1 Criação e uso de uma chave de assinatura

Cenário

As chaves de assinatura são usadas pelos serviços de back-end para verificar a identidade do APIG.

Uma chave de assinatura consiste em uma chave e um segredo e pode ser usada somente depois de vinculada a uma API. Quando uma API vinculada a uma chave de assinatura é chamada, o APIG adiciona detalhes de assinatura à solicitação da API. O serviço de back-end da API assina a solicitação da mesma maneira e verifica a identidade da APIG verificando se a assinatura é consistente com a do cabeçalho de **Authorization** enviado pelo APIG.

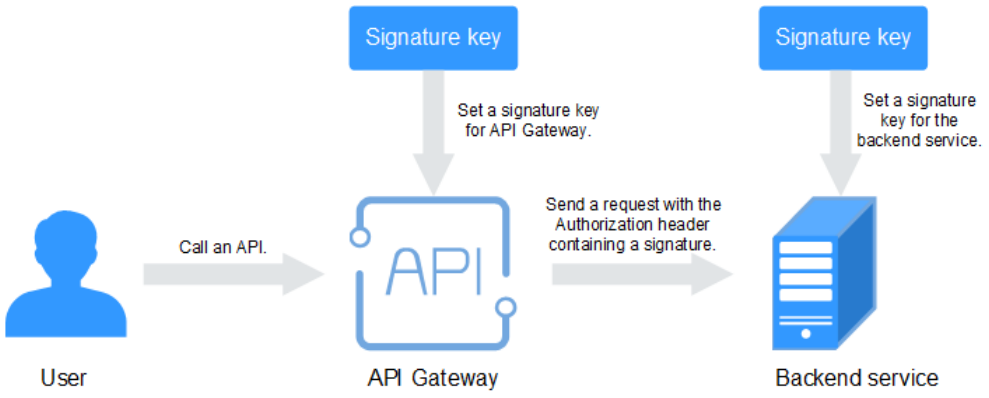
NOTA

Cada API só pode ser vinculada a uma chave de assinatura em um determinado ambiente, mas cada chave de assinatura pode ser vinculada a várias APIs.

Procedimento

1. Crie uma chave de assinatura no console do APIG.
2. Vincule a chave de assinatura a uma API.
3. APIG envia solicitações assinadas contendo uma assinatura no cabeçalho **Authorization** para o serviço de back-end. O serviço de back-end pode usar diferentes linguagens de programação (como Java, Go, Python, JavaScript, C#, PHP, C++, C e Android) para assinar cada solicitação e verificar se as duas assinaturas são consistentes.

Figura 12-31 Fluxo de processo de chave de assinatura



Criação de uma chave de assinatura

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Signature Keys**.

Passo 6 Clique em **Create Signature Key**.

Passo 7 Na caixa de diálogo **Create Signature Key**, defina os parâmetros listados em **Tabela 12-26**.

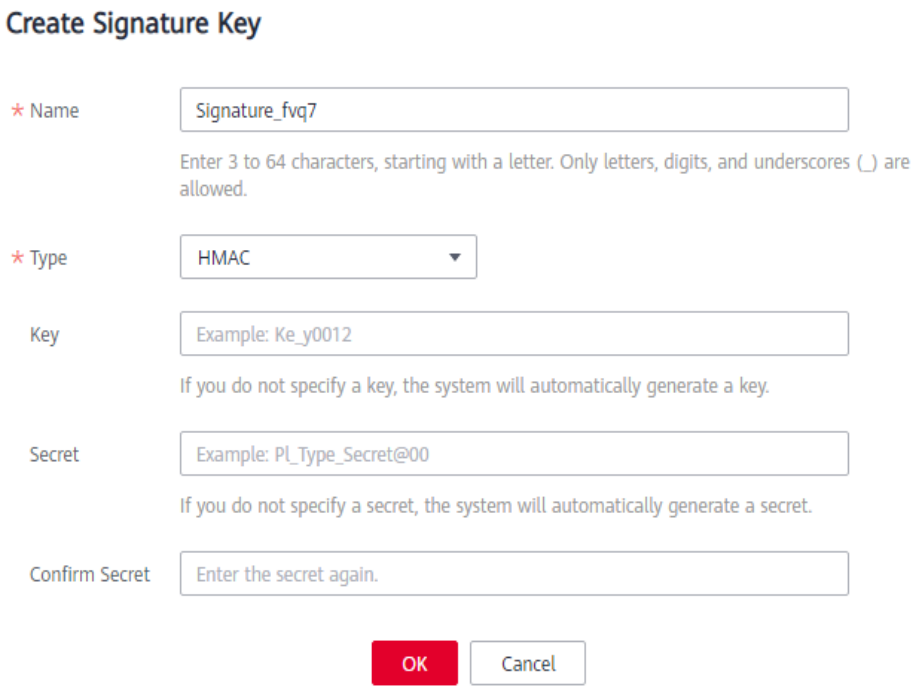


Tabela 12-26 Parâmetros para criar uma chave de assinatura

Parâmetro	Descrição
Name	Nome da chave de assinatura.
Type	Tipo da chave de assinatura. Selecione **HMAC** ou **Basic**. Este parâmetro está disponível apenas para gateways dedicados.
Key	Combinado com **Secret** para formar um par de chaves de assinatura. ● Se você definir **Type** como **HMAC**, insira a chave do par de chaves usado para autenticação de código de autenticação de mensagem baseado em hash (HMAC). ● Se você definir **Type** como **Basic**, digite o nome de usuário usado para autenticação básica.

Parâmetro	Descrição
Secret	Combinado com **Key** para formar um par de chaves de assinatura. ● Se você definir **Type** como **HMAC**, insira o segredo do par de chaves usado para autenticação HMAC. ● Se você definir **Type** como **Basic**, digite a senha usada para autenticação básica.
Confirm Secret	Digite o segredo novamente.

Passo 8 Clique em **OK**.

----Fim

Vinculação de uma chave de assinatura a uma API

Passo 1 No painel de navegação, escolha **API Publishing** > **Signature Keys**.

Passo 2 Vincule uma chave de assinatura a uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da chave de assinatura a ser vinculada a uma API, clique em **Bind to API**.
- Clique no nome da chave de assinatura de destino.

Passo 3 Clique em **Select API**.

Passo 4 Especifique um grupo de APIs, um ambiente e uma palavra-chave de nome de API para pesquisar a API desejada.

Passo 5 Selecione a API e clique em **OK**.

NOTA

Se uma chave de assinatura não for mais necessária para uma API, desvincule-a da API.

----Fim

Verificar o resultado da assinatura

Assine cada solicitação de back-end seguindo as instruções em **Algoritmo de assinatura** e verifique se a assinatura do back-end é consistente com a assinatura no cabeçalho **Authorization** da solicitação da API.

Criação de uma chave de assinatura chamando uma API

Você também pode criar uma chave de assinatura chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Criação de uma chave de assinatura**.

12.3.6.2 Exclusão de uma chave de assinatura

Cenário

Você pode excluir chaves de assinatura que você não precisa mais.

Pré-requisitos

Você criou uma chave de assinatura.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **Signature Keys**.

Passo 6 Exclua uma chave de assinatura. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da chave de assinatura que você deseja excluir, clique em **Delete**.
- Clique no nome da chave de assinatura de destino e clique em **Delete** no canto superior direito da página de detalhes da chave de assinatura exibida.

NOTA

Se a chave de assinatura tiver sido vinculada a qualquer API, desvincule-a e exclua-a.

Passo 7 Clique em **Yes**.

----Fim

Excluir uma chave de assinatura chamando uma API

Você também pode excluir uma chave de assinatura chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de uma chave de assinatura**.

12.3.7 Gerenciamento de canais da VPC

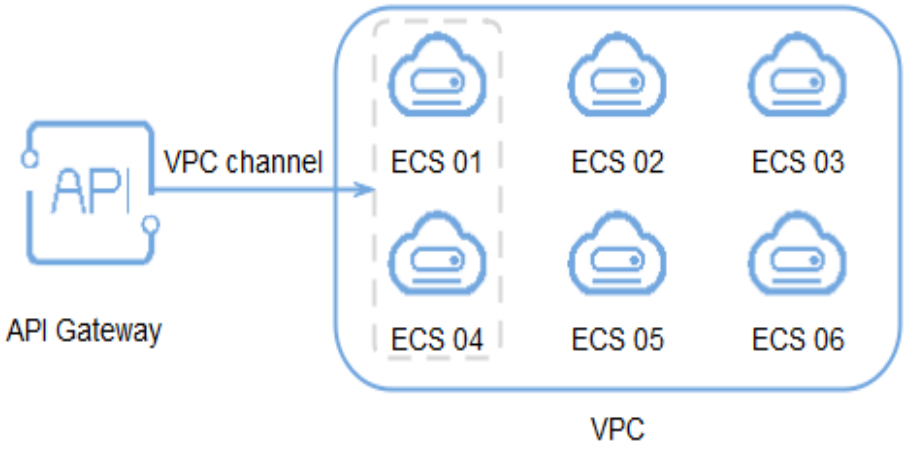
12.3.7.1 Criação de um canal da VPC

Cenário

Os canais da VPC permitem que os serviços implementados em VPCs sejam acessados por meio de suas sub-redes, reduzindo a latência e equilibrando as cargas de serviços de back-end.

Depois de criar um canal da VPC, você pode configurá-lo para uma API com um serviço de back-end HTTP/HTTPS. Por exemplo, seis ECSs foram implementados em um VPC e um canal da VPC foi criado para alcançar o ECS 01 e o ECS 04. O APIG pode acessar esses dois ECSs por meio do canal da VPC.

Figura 12-32 Acessar ECSs em um canal da VPC por meio de APIG



NOTA

Os gateways dedicados suportam balanceadores de carga de rede privada como canais da VPC, enquanto o gateway compartilhado não.

Pré-requisitos

- Você criou um servidor em nuvem.
- Você tem a permissão **VPC Administrator**.

Criação de um canal rápido

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **VPC Channels**.

Passo 6 Clique em **Create VPC Channel** e defina os parâmetros listados em **Tabela 12-27**.

Figura 12-33 Criação de um canal da VPC

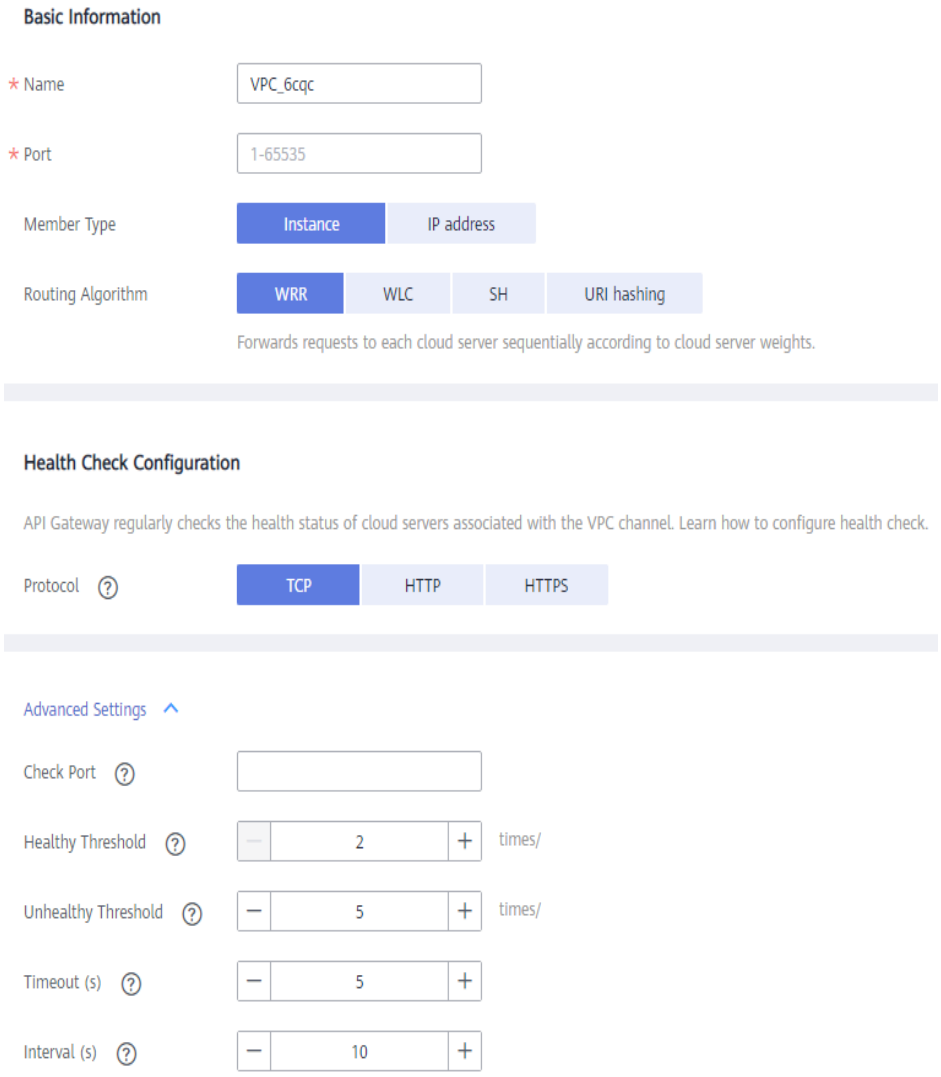


Tabela 12-27 Parâmetros para criar um canal da VPC

Parâmetro	Descrição
Name	Nome do canal da VPC.
Port	A porta do host do canal da VPC, ou seja, a porta do serviço de back-end. Faixa: 1 – 65535.
Member Type	Selecione um método que você deseja usar para especificar servidores para o canal da VPC. O tipo de membro é uma configuração única e não pode ser alterado após a criação do canal da VPC. ● **Instance**: selecione servidores de nuvem. ● **IP address**: especifique os endereços IP do servidor de nuvem. Este parâmetro só está disponível para gateways dedicados.

Parâmetro	Descrição
Routing Algorithm	O algoritmo a ser usado para encaminhar solicitações para os servidores em nuvem que você selecionar. Os seguintes algoritmos de roteamento estão disponíveis: ● **WRR**: round robin ponderado ● **WLC**: conexão mínima ponderada ● **SH**: hash de origem ● **URI hashing**
Protocol	O protocolo usado para executar verificações de integridade em servidores de nuvem associados ao canal da VPC. Opções: ● TCP ● HTTP ● HTTPS Valor padrão: **TCP**.
Path	O caminho de destino para verificações de integridade. Defina este parâmetro apenas quando o **Protocol** não estiver definido como **TCP**.
Check Port	A porta de destino para verificações de integridade. Por padrão, a porta do canal da VPC será usada.
Healthy Threshold	O número de verificações consecutivas bem-sucedidas necessárias para que um servidor de nuvem seja considerado saudável. Faixa: 2 – 10. Valor padrão: **2**.
Unhealthy Threshold	O número de verificações consecutivas com falhas necessárias para que um servidor de nuvem seja considerado não íntegro. Faixa: 2 – 10. Valor padrão: **5**.
Timeout (s)	O tempo limite usado para determinar se uma verificação de integridade falhou. Unidade: s. Faixa: 2 – 30. Valor padrão: **5**.
Interval (s)	O intervalo entre verificações consecutivas. Unidade: s. Faixa: 5 – 300. Valor padrão: **10**.
Response Codes	Os códigos HTTP usados para verificar uma resposta bem-sucedida de um destino. Defina este parâmetro apenas quando o **Protocol** não estiver definido como **TCP**.

Passo 7 Clique em **Next**.

Passo 8 Clique em **Select Cloud Server**.

Passo 9 Selecione os servidores de nuvem que você deseja adicionar e clique em **OK**.

NOTA

Para garantir uma verificação de integridade e disponibilidade de serviço bem-sucedida, configure os grupos de segurança dos servidores em nuvem para permitir o acesso de 100.125.0.0/16.

Passo 10 Clique em **Finish**.

----Fim

Criação de um canal da VPC chamando uma API

Você também pode criar um canal da VPC chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Criação de um canal da VPC**.

Operações de acompanhamento

Crie uma API para serviços de back-end implementados em uma VPC para balancear cargas.

12.3.7.2 Exclusão de um canal da VPC

Cenário

Você pode excluir os canais de VPC que não são mais necessários.

NOTA

Os canais de VPC que estão atualmente em uso por APIs publicadas não podem ser excluídos.

Pré-requisitos

Você criou um canal da VPC.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **VPC Channels**.

Passo 6 Exclua um canal da VPC. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** do canal da VPC que você deseja excluir, clique em **Delete**.
- Clique no nome do canal da VPC de destino e clique em **Delete** no canto superior direito da página de detalhes do canal da VPC exibida.

Passo 7 Clique em **Yes**.

----Fim

Excluir um canal de VPC chamando uma API

Você também pode excluir um canal da VPC chamando uma API fornecida pela APIG. Para obter detalhes, consulte **Exclusão de um canal da VPC**.

12.3.7.3 Edição de configurações de verificação de integridade

Cenário

Você pode modificar as configurações de verificação de integridade de um canal da VPC para atender aos requisitos de serviço.

Pré-requisitos

Você criou um canal da VPC.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **VPC Channels**.

Passo 6 Clique no nome do canal da VPC de destino.

Passo 7 Clique na guia **Health Check**.

Passo 8 Clique em **Edit Health Check**.

Passo 9 Na caixa de diálogo **Edit Health Check Configuration**, modifique os parâmetros listados em **Tabela 12-28**.

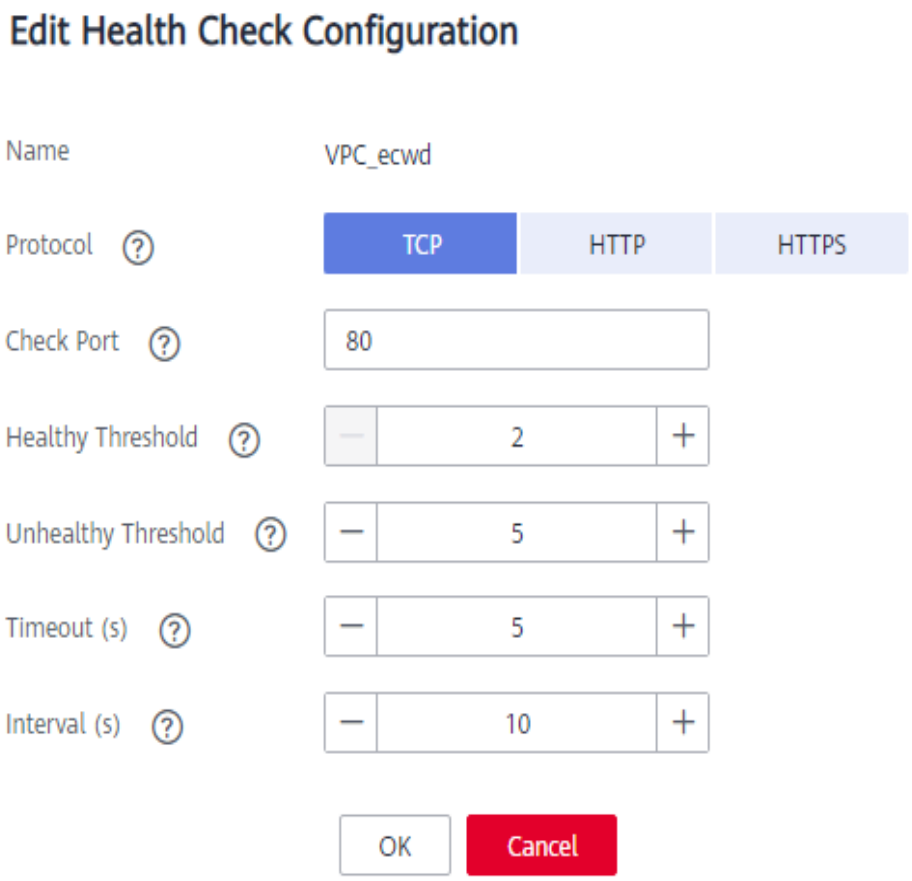


Tabela 12-28 Configurações de verificação de integridade

Parâmetro	Descrição
Protocol	O protocolo usado para executar verificações de integridade em servidores de nuvem associados ao canal da VPC. Opções: ● TCP ● HTTP ● HTTPS Valor padrão: **TCP**.
Path	O caminho de destino para verificações de integridade. Defina este parâmetro apenas quando o **Protocol** não estiver definido como **TCP**.
Check Port	A porta de destino para verificações de integridade. Por padrão, a porta do canal da VPC será usada.
Healthy Threshold	O número de verificações consecutivas bem-sucedidas necessárias para que um servidor de nuvem seja considerado saudável. Faixa: 2 – 10. Valor padrão: **2**.

Parâmetro	Descrição
Unhealthy Threshold	O número de verificações consecutivas com falhas necessárias para que um servidor de nuvem seja considerado não íntegro. Faixa: 2 – 10. Valor padrão: **5**.
Timeout (s)	O tempo limite usado para determinar se uma verificação de integridade falhou. Unidade: s. Faixa: 2 – 30. Valor padrão: **5**.
Interval (s)	O intervalo entre verificações consecutivas. Unidade: s. Faixa: 5 – 300. Valor padrão: **10**.
Response Codes	Os códigos HTTP usados para verificar uma resposta bem-sucedida de um destino. Defina este parâmetro apenas quando o **Protocol** não estiver definido como **TCP**.

Passo 10 Clique em **OK**.

----Fim

12.3.7.4 Edição de configurações de servidor em nuvem de um canal da VPC

Cenário

Você pode adicionar ou remover servidores em nuvem e editar pesos de servidores em nuvem para canais da VPC para atender aos requisitos de serviço.

Pré-requisitos

Você criou um canal da VPC.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **VPC Channels**.

Passo 6 Clique no nome do canal da VPC de destino.

Passo 7 Clique na guia **Cloud Servers**.

Passo 8 Adicione ou remova servidores em nuvem e edite pesos de servidores em nuvem.

- Adicionar servidores em nuvem
  a. Clique em **Select Cloud Server**.
  b. Selecione os servidores de nuvem que você deseja adicionar, defina os pesos do servidor de nuvem e clique em **OK**.

  NOTA

  Para garantir uma verificação de integridade bem-sucedida e a disponibilidade do serviço, configure os grupos de segurança dos servidores de nuvem de back-end para permitir o acesso a partir de 100.125.0.0/16.
- Remover servidores de nuvem
  a. Na coluna **Operation** dos servidores de nuvem que você deseja remover, clique em **Remove**.
  b. Clique em **Yes**.
- Editar o peso de um servidor de nuvem
  a. Na coluna **Weight** do servidor de nuvem de destino, clique em .
  b. Altere o peso e clique em .
- Editar os pesos de vários servidores em nuvem
  a. Selecione os servidores de nuvem a serem editados e clique em **Edit Weight**.
  b. Altere os pesos dos servidores de nuvem selecionados e clique em **OK**.

----Fim

Editar configurações de servidor de nuvem de um canal da VPC chamando uma API

Você também pode editar as configurações do servidor em nuvem de um canal da VPC chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Adição de instâncias de back-end (servidores de nuvem)**.

12.3.8 Autorizadores personalizados

12.3.8.1 Criação de um autorizador personalizado

Cenário

O APIG suporta autenticação personalizada de solicitações de front-end e back-end.

- Autenticação personalizada do front-end: se você já tiver um sistema de autenticação, poderá configurá-lo em uma função e criar um autorizador personalizado usando a função para autenticar solicitações de API.
- Autenticação personalizada de back-end: você pode criar um autorizador personalizado 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 APIG para se conectar ao sistema de autenticação de back-end.

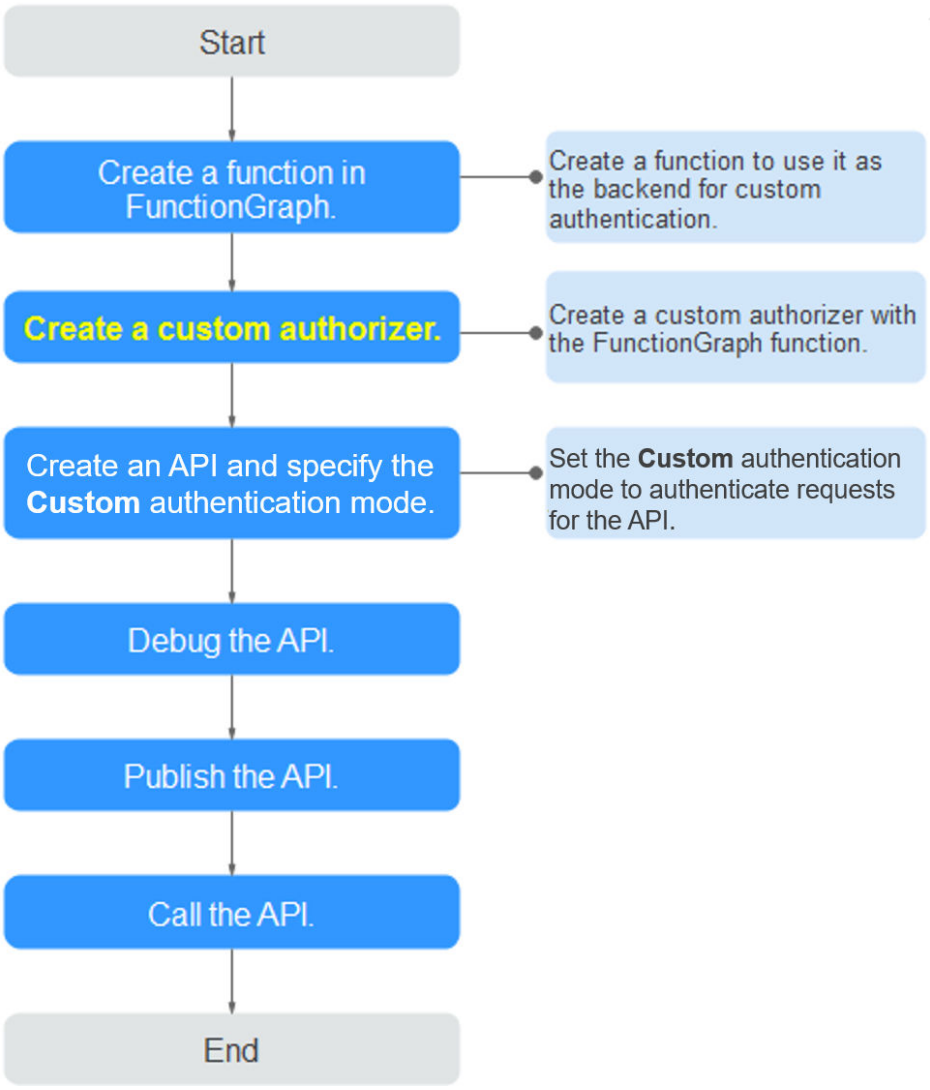
NOTA

A autenticação personalizada é implementada usando o FunctionGraph e não é suportada se o FunctionGraph não estiver disponível na região selecionada.

Para obter detalhes sobre a autenticação personalizada, consulte *Guia de desenvolvedor*.

A figura a seguir mostra o processo de chamada de APIs por meio de autenticação personalizada.

Figura 12-34 Chamar APIs por meio de autenticação personalizada



Pré-requisitos

- Você criou uma função no FunctionGraph.
- Você tem a permissão de **FunctionGraph Administrator**.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 Escolha **API Publishing** > **Custom Authorizers** e clique em **Create Custom Authorizer**.

Passo 6 Defina os parâmetros listados em **Tabela 12-29**.

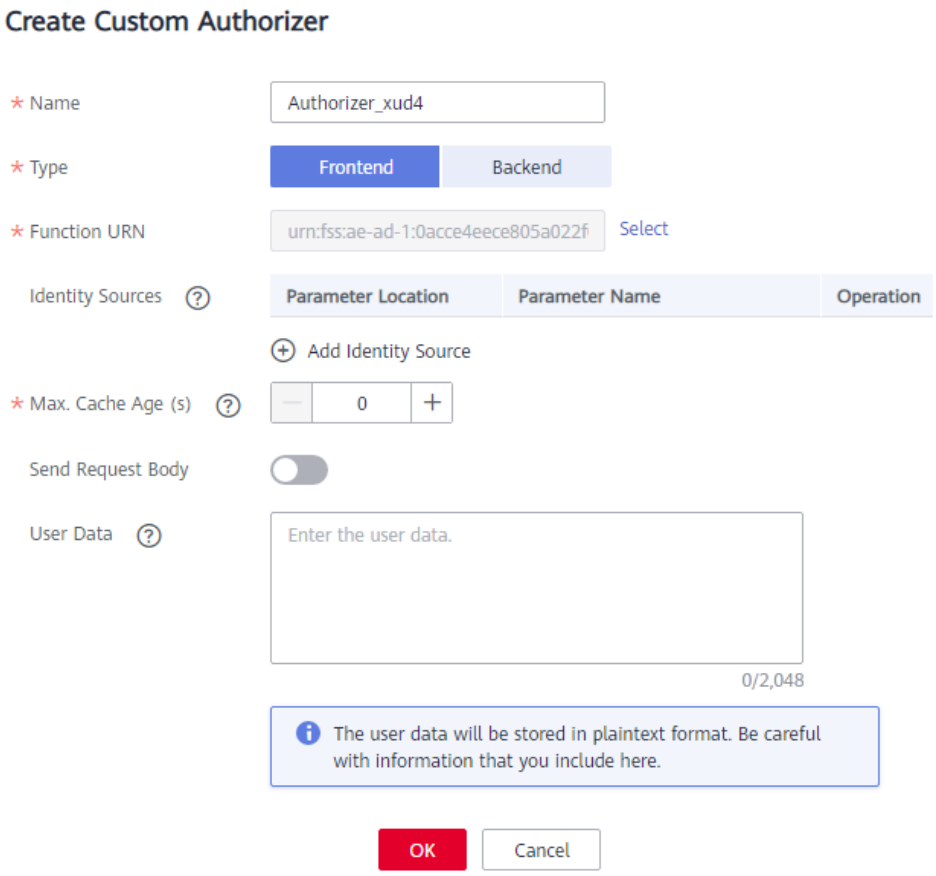


Tabela 12-29 Parâmetros para criar um autorizador personalizado

Parâmetro	Descrição
Name	Nome do autorizador.

Parâmetro	Descrição
Type	● **Front-end**: autentica o acesso às APIs. ● **Back-end**: autentica o acesso aos serviços de back-end.
Function URN	Selecione uma função do FunctionGraph.
Identity Sources	Parâmetros de solicitação para autenticação. Você pode adicionar cabeçalhos e consultar cadeias. Os nomes dos cabeçalhos não diferenciam maiúsculas de minúsculas. Esse parâmetro é obrigatório somente se você definir **Type** como **Frontend** e **Max. Cache Age (s)** é maior que **0**. Quando o cache é usado, esse parâmetro é usado como um critério de pesquisa para consultar resultados de autenticação.
Max. Cache Age (s)	O tempo para resultados de autenticação de cache. O valor **0** significa que os resultados da autenticação não serão armazenados em cache. O valor máximo é **3600**.
Send Request Body	Determine se o corpo de cada solicitação de API deve ser enviado para a função de autenticação. Se você habilitar essa opção, o corpo da solicitação será enviado para a função de autenticação da mesma maneira que os cabeçalhos e as cadeias de consulta. **NOTA** Esta opção está disponível apenas para gateways de API dedicados.
User Data	Parâmetros de solicitação personalizados a serem usados em conjunto com **Identity Sources** quando o APIG invoca uma função.

Passo 7 Clique em **OK**.

----Fim

12.3.8.2 Exclusão de um autorizador personalizado

Cenário

Você pode excluir os autorizadores personalizados que você não precisa mais.

NOTA

- A autenticação personalizada é implementada usando o FunctionGraph e não é suportada se o FunctionGraph não estiver disponível na região selecionada.
- Os autorizadores personalizados que foram configurados para APIs não podem ser excluídos.

Pré-requisitos

Você **criou um autorizador personalizado**.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 Escolha **API Publishing** > **Custom Authorizers** e clique em **Delete** na linha que contém o autorizador personalizado que você deseja excluir.

Passo 6 Clique em **Yes**.

----Fim

12.3.9 Plug-ins

12.3.9.1 Criação de um plug-in

O APIG fornece recursos de extensão flexíveis para APIs por meio de plug-ins.

Diretrizes para o uso de plug-ins

- Uma API pode ser vinculada a apenas um plug-in do mesmo tipo.
- Os plug-ins são independentes das APIs. Um plug-in entra em vigor para uma API somente depois que eles são vinculados um ao outro. Ao vincular um plug-in a uma API, você deve especificar um ambiente no qual a API foi publicada. O plug-in entra em vigor para a API apenas no ambiente especificado.
- Depois de ligar um plug-in a uma API, desvincular o plug-in da API ou atualizar o plug-in, não é necessário publicar a API novamente.
- Colocar uma API off-line não afeta os plug-ins vinculados a ela. Os plug-ins ainda estarão vinculados à API se a API for publicada novamente.
- Os plug-ins vinculados a APIs não podem ser excluídos.

Criação de um plug-in

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**. Em seguida, clique em **Access Console** no canto superior direito de um gateway dedicado.

Passo 5 No painel de navegação, escolha **API Publishing** > **Plug-ins**.

Passo 6 Clique em **Create Plug-in**.

Na caixa de diálogo **Create Plug-in**, configure as informações do plug-in.

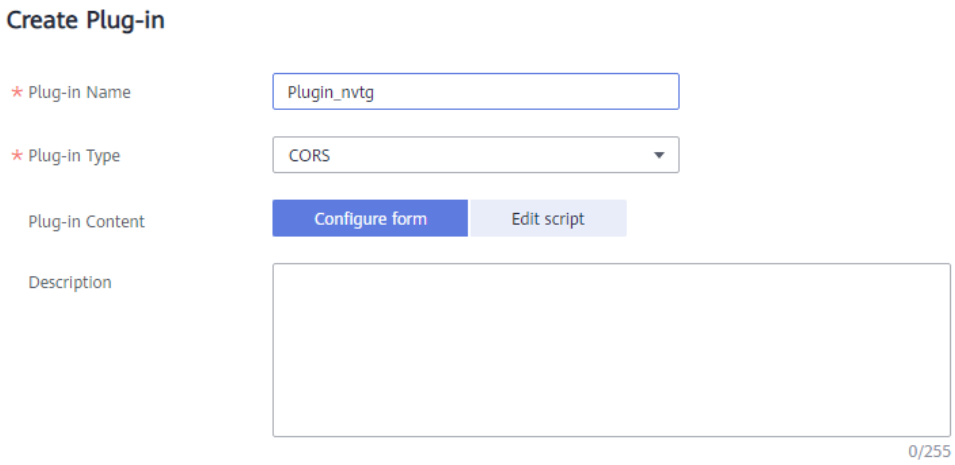


Tabela 12-30 Configuração do plug-in

Parâmetro	Descrição
Plug-in Name	Nome do plug-in que você deseja criar. Recomenda-se que você digite um nome com base em certas regras de nomenclatura para facilitar a identificação e a pesquisa.
Plug-in Type	Tipo do plug-in, que determina os recursos de extensão do plug-in. ● **CORS**: especifica cabeçalhos de solicitação de simulação e cabeçalhos de resposta e cria automaticamente APIs de solicitação de simulação para acesso à API de origem cruzada. ● **HTTP Response Headers**: permite personalizar cabeçalhos de resposta HTTP que serão exibidos em uma resposta da API. ● **Request throttling**: limita o número de vezes que uma API pode ser chamada dentro de um período de tempo específico. A limitação baseada em parâmetro, básica e excluída é suportada.
Plug-in Content	Conteúdo do plug-in, que pode ser configurado em um formulário ou usando um script. O conteúdo do plug-in varia dependendo do tipo de plug-in: ● **Plug-in CORS** ● **Plug-in de gerenciamento de cabeçalho de resposta HTTP** ● **Plug-in de limitação de solicitação**
Description	Descrição do plug-in.

Passo 7 Clique em **OK**.

Depois de criar o plug-in, **vincule-o à API** para a qual o plug-in entrará em vigor.

----Fim

Vinculação de um plug-in a uma API

Passo 1 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 2 Clique no nome da API de destino para acessar a página de detalhes da API.

Passo 3 Na página de guia **Plug-ins**, clique em **Bind**.

Passo 4 Na caixa de diálogo **Bind Plug-in**, selecione um ambiente e tipo de plug-in e selecione o plug-in a ser vinculado.

Passo 5 Clique em **OK**.

----Fim

12.3.9.2 Plug-in CORS

Por motivos de segurança, o navegador restringe solicitações entre domínios de serem iniciadas a partir de um script de página. Nesse caso, a página pode acessar apenas os recursos do domínio atual. O CORS permite que o navegador envie XMLHttpRequest para o servidor em um domínio diferente. Para obter mais informações, consulte **CORS**.

O plug-in CORS fornece os recursos de especificação de cabeçalhos de solicitação de simulação e cabeçalhos de resposta e criação automática de APIs de solicitação de simulação para acesso à API entre origens.

NOTA

Somente gateways dedicados criados a partir de 10 de fevereiro de 2021 oferecem suporte ao plug-in CORS. Para usar o plug-in CORS para gateways dedicados criados antes de 10 de fevereiro de 2021, entre em contato com o atendimento ao cliente.

Diretrizes de uso

- Você entendeu as **Diretrizes para o uso de plug-ins**.
- As APIs com o mesmo caminho de solicitação em um grupo de APIs só podem ser vinculadas ao mesmo plug-in CORS.
- Se você ativou o CORS para uma API e também vinculou o plug-in CORS à API, o plug-in CORS será usado.
- Não é possível vincular o plug-in CORS a APIs com o mesmo caminho de solicitação de outra API que use o método OPTIONS.
- Ao **vincular um plug-in a uma API**, certifique-se de que o método de solicitação da API esteja incluído em **allow_methods**.

Parâmetros de configuração

Tabela 12-31 Parâmetros de configuração

Parâmetro	Descrição
allowed origins	Cabeçalho de resposta **Access-Control-Allow-Origin**, que especifica uma única origem, que diz aos navegadores para permitir que essa origem acesse uma API; ou então — para solicitações sem credenciais — o curinga "*", para dizer aos navegadores para permitir que qualquer origem acesse a API. Separe vários URIs usando vírgulas.
allowed methods	Cabeçalho de resposta **Access-Control-Allow-Methods**, que especifica os métodos HTTP permitidos ao acessar a API. Separe vários métodos usando vírgulas.
allowed headers	Cabeçalho de resposta **Access-Control-Allow-Headers**, que especifica os cabeçalhos de solicitação que podem ser usados ao fazer uma XMLHttpRequest. Separe vários cabeçalhos usando vírgulas. Por padrão, os cabeçalhos de solicitação simples **Accept**, **Accept-Language**, **Content-Language** e **Content-Type** (somente se o valor for **application/x-www-form-urlencoded**, **multipart/form-data** ou **text/plain**) são transportados em solicitações. Você não precisa configurar esses cabeçalhos neste parâmetro.
exposed headers	Cabeçalho de resposta **Access-Control-Expose-Headers**, que especifica quais cabeçalhos de resposta podem ser contidos na resposta de XMLHttpRequest. Separe vários cabeçalhos usando vírgulas. Por padrão, os cabeçalhos básicos de resposta **Cache-Control**, **Content-Language**, **Content-Type**, **Expires**, **Last-Modified** e **Pragma** podem ser contidos na resposta. Você não precisa configurar esses cabeçalhos neste parâmetro.
maximum age	Cabeçalho de resposta **Access-Control-Max-Age**, que especifica por quantos segundos os resultados de uma solicitação de simulação podem ser armazenados em cache. Não serão enviadas mais solicitações de simulação dentro do período especificado.
allowed credentials	Cabeçalho de resposta **Access-Control-Allow-Credentials**, que especifica se solicitações XMLHttpRequest podem levar cookies.

Exemplo de script

```
{
  "allow_origin": "*",
  "allow_methods": "GET,POST,PUT",
  "allow_headers": "Content-Type,Accept,Accept-Ranges,Cache-Control",
  "expose_headers": "X-Request-Id,X-Apig-Latency",
```



```
  "max_age": 172800,
  "allow_credentials": true
}
```

12.3.9.3 Plug-in de gerenciamento de cabeçalho de resposta HTTP

Cabeçalhos de resposta HTTP são parte da resposta retornada pelo APIG para um cliente que chama uma API. Você pode personalizar cabeçalhos de resposta HTTP que estarão contidos em uma resposta da API.

NOTA

Somente gateways dedicados criados a partir de 1º de junho de 2021 são compatíveis com o plug-in de gerenciamento de cabeçalho de resposta HTTP. Para usar este plug-in para gateways dedicados criados antes de 1º de junho de 2021, entre em contato com o atendimento ao cliente.

Diretrizes de uso

Você não pode modificar os cabeçalhos de resposta, como **x-apig-*** e **x-request-id**, adicionados pelo APIG ou os cabeçalhos configurados para CORS.

Parâmetros de configuração

Tabela 12-32 Parâmetros de configuração

Parâmetro	Descrição
Name	Nome do cabeçalho da resposta, que não faz distinção entre maiúsculas e minúsculas e deve ser exclusivo em um plug-in. Você pode adicionar um máximo de 10 cabeçalhos de resposta.
Value	Valor do cabeçalho da resposta. Esse parâmetro não tem efeito e pode ser deixado em branco se você definir **Action** para **Delete**.

Parâmetro	Descrição
Action	Operação de cabeçalho de resposta. Você pode substituir, anexar, excluir, pular ou adicionar o cabeçalho especificado. **Override** ● O valor desse cabeçalho de resposta substituirá o do mesmo cabeçalho que existe em uma resposta de API. ● Se uma resposta da API contiver vários cabeçalhos com o mesmo nome que você definiu aqui, apenas o valor do cabeçalho especificado será retornado. ● Se uma resposta da API não contiver o cabeçalho especificado, o valor definido aqui será retornado. **Append** ● Se uma resposta da API contiver o cabeçalho especificado, o valor definido aqui será adicionado, seguindo o valor existente. Os dois valores serão separados por vírgulas (,). ● Se uma resposta da API contiver vários cabeçalhos com o mesmo nome que você definiu aqui, os valores desses cabeçalhos serão separados por vírgulas (,) e seguidos pelo valor do cabeçalho especificado. ● Se uma resposta da API não contiver o cabeçalho especificado, o valor definido aqui será retornado. **Delete** ● Se uma resposta da API contiver o cabeçalho especificado, o cabeçalho será excluído. ● Se uma resposta da API contiver vários cabeçalhos com o mesmo nome que você definiu aqui, todos esses cabeçalhos serão excluídos. **Skip** ● Se uma resposta da API contiver o cabeçalho especificado, o cabeçalho será ignorado. ● Se uma resposta da API contiver vários cabeçalhos com o mesmo nome que você definiu aqui, os valores de todos esses cabeçalhos serão retornados sem modificação. ● Se uma resposta da API não contiver o cabeçalho especificado, o valor definido aqui será retornado. **Add** O valor do cabeçalho especificado será retornado mesmo que o cabeçalho não exista em uma resposta da API.

Exemplo de script

```
{
    "response_headers": [
        {
            "name": "test",
            "value": "test",
            "action": "append"
```



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

12.3.9.4 Plug-in de limitação de solicitação

O plug-in de limitação de solicitação limita o número de vezes que uma API pode ser chamada em um período de tempo específico. Suporta estrangulamento baseado em parâmetros, básico e excluído.

NOTA

Somente os gateways dedicados criados em e após 4 de dezembro de 2021 suportam o plug-in de limitação de solicitação. Para usar este plug-in para gateways dedicados criados antes de 4 de dezembro de 2021, entre em contato com o atendimento ao cliente.

- Limitação básica

  Solicitações de limitação por API, usuário, aplicação ou endereço IP de origem. Essa função é equivalente a uma **política de limitação de solicitações**, mas é incompatível com ela.

- Limitação baseada em parâmetros

  Solicitações de limitação com base em cabeçalhos, parâmetros de caminho, métodos, cadeias de consulta ou variáveis do sistema.

- Limitação excluída

  Solicitações de limitação com base em aplicações ou locatários específicos.

Restrições

- Uma política de limitação de solicitação se torna inválida se um plug-in de limitação de solicitação estiver vinculado à mesma API da política.
- Você pode definir um máximo de 100 regras de parâmetro.
- O conteúdo do plug-in não pode exceder 65.535 caracteres.

Parâmetros de configuração

Tabela 12-33 Parâmetros de configuração

Parâmetro	Descrição
Policy Type	• API específica Monitore e controle as solicitações de uma única API. • Compartilhamento de API Monitore e controle o total de solicitações de todas as APIs vinculadas ao plug-in.

Parâmetro	Descrição
Period	Por quanto tempo você deseja limitar o número de solicitações de API. ● **Max. API Requests**: limite o número máximo de vezes que uma API pode ser chamada em um período de tempo específico. ● **Max. User Requests**: limite o número máximo de vezes que uma API pode ser chamada por um usuário em um período de tempo específico. ● **Max. App Requests**: limite o número máximo de vezes que uma API pode ser chamada por uma aplicação em um período de tempo específico. ● **Max. IP Address Requests**: limite o número máximo de vezes que uma API pode ser chamada por um endereço IP em um período de tempo específico.
Max. API Requests	O número máximo de vezes que cada API vinculada pode ser chamada dentro do período especificado. Este parâmetro deve ser utilizado em conjunto com o **Period**.
Max. User Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um usuário dentro do período especificado. Para APIs com autenticação do IAM, a limitação é baseada em um código de projeto; para APIs com autenticação de aplicação, a limitação é baseada em um código de conta. Para obter detalhes sobre IDs de conta e IDs de projeto, consulte a descrição sobre **Excluded Tenants** nesta tabela. ● O valor deste parâmetro não pode exceder o de **Máximo de solicitações de API**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**. ● Se houver muitos usuários na sua conta que acessam uma API, os limites de limitação de solicitações da API serão aplicados a todos esses usuários.
Max. App Requests	O número máximo de vezes que cada API vinculada pode ser chamada por uma aplicação dentro do período especificado. Esse limite se aplica apenas a APIs acessadas por meio de autenticação de aplicação. ● O valor deste parâmetro não pode exceder o de **Max. User Requests**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.

Parâmetro	Descrição
Max. IP Address Requests	O número máximo de vezes que cada API vinculada pode ser chamada por um endereço IP dentro do período especificado. ● O valor deste parâmetro não pode exceder o de **Máximo de solicitações de API**. ● Este parâmetro deve ser utilizado em conjunto com o **Period**.
Parameter-based Throttling	Habilitar ou desabilitar a limitação baseada em parâmetro. Depois que essa função é ativada, as solicitações de API são limitadas com base em parâmetros especificados.
Parameters	Definir parâmetros para regras de limitação. ● **Parameter Location**: a localização de um parâmetro a ser usado em uma regra. – **path**: URI de solicitação da API. Este parâmetro é configurado por padrão. – **method**: método de solicitação da API. Este parâmetro é configurado por padrão. – **Header**: o valor do primeiro cabeçalho HTTP com o nome do parâmetro que você definiu. – **Query**: o valor da primeira cadeia de consulta com o nome do parâmetro que você definiu. – **System**: um parâmetro do sistema. ● **Parameter Name**: o nome de um parâmetro que corresponde ao valor especificado em uma regra.

Parâmetro	Descrição
Rules	Defina regras de limitação. Uma regra consiste em condições, uma limitação de solicitações de API e um período. Para adicionar mais regras, clique em **Add Rule**. ● Condições Clique em  para definir expressões de condição. Para definir uma expressão, selecione um parâmetro e um operador e insira um valor. – =: igual a – **!=**: não igual a – **pattern**: expressão regular – **enum**: valores enumerados. Separe vários valores com vírgulas (,). ● Máx. solicitações de API O número máximo de vezes que uma API pode ser chamada em um período de tempo específico. ● Período Um período de tempo que será aplicado com o limite definido. Se não for especificado, o período definido na área **Police Details** será usado. Por exemplo, configure a limitação baseada em parâmetro da seguinte forma: adicione o parâmetro **Host** e especifique o local como **header**; adicione a condição **Host = www.abc.com**, e defina o limite de limitação como **10** e o período como 60s. Para APIs cujo parâmetro **Host** no cabeçalho da solicitação é igual a **www.abc.com**, elas não podem ser chamadas novamente uma vez chamadas 10 vezes em 60s.
Excluded Throttling	Ativar ou desativar a limitação excluída. Depois que essa função é habilitada, os limites para locatários e aplicações excluídos substituem o **Max. User Requests** e **Max. App Requests** na área **Basic Throttling**.
Excluded Tenants	**Tenant ID**: um ID de conta ou um ID de projeto. ● Especifique um ID de projeto para uma API com autenticação de aplicação. Para obter detalhes, consulte **Obtenção de um ID de projeto**. ● Especifique um ID de conta (não ID de usuário do IAM) para uma API com autenticação do IAM. Para obter detalhes, consulte **Obtenção de um nome de conta e um ID de conta**. **Threshold**: o número máximo de vezes que um locatário específico pode acessar uma API dentro do período especificado. O limite não pode exceder o valor de **Max. API Requests** na área **Basic Throttling**.

Parâmetro	Descrição
Excluded Apps	Selecione uma aplicação e especifique o número máximo de vezes que a aplicação pode acessar uma API dentro do período especificado. O limite não pode exceder o valor de **Max. API Requests** na área **Basic Throttling**.

Exemplo de script

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


12.3.9.5 Exclusão de um plug-in

Cenário

Você pode excluir plug-ins que você não precisa mais. Para excluir um plug-in vinculado a APIs, desvincule o plug-in das APIs e exclua-o.

Pré-requisitos

Você criou um plug-in.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**. Em seguida, clique em **Access Console** no canto superior direito de um gateway dedicado.

Passo 5 No painel de navegação, escolha **API Publishing** > **Plug-ins**.

Passo 6 Clique no nome do plug-in de destino para acessar a página de detalhes do plug-in.

- Se o plug-in não estiver vinculado a nenhuma API, clique em **Delete** no canto superior direito.
- Se o plug-in tiver sido vinculado a APIs, desvincule o plug-in das APIs na área **Bound APIs** e clique em **Delete** no canto superior direito.

Passo 7 Clique em **Yes**.

----Fim

12.3.10 Monitoramento

12.3.10.1 Métricas do APIG

Introdução

Esta seção descreve as métricas que o APIG reporta ao serviço Cloud Eye. Você pode visualizar métricas e alarmes usando o console do Cloud Eye.

Namespace

Gateway compartilhado: SYS.APIG

Gateway dedicado: SYS.APIC

Métricas

Tabela 12-34 Métricas de gateway compartilhadas

ID	Nome	Descrição	Intervalo de valores	Objeto monitorado	Intervalo de monitorização (minuto)
avg_latency	Latência média	Latência média da API.	≥ 0 Unidade: ms	API	1
input_throughput	Tráfego de entrada	Tráfego de entrada da API.	≥ 0 Unidade: byte, KB, MB ou GB	API	1
max_latency	Máxima latência	Máxima latência da API.	≥ 0 Unidade: ms	API	1
output_throughput	Tráfego de saída	Tráfego de saída da API.	≥ 0 Unidade: byte, KB, MB ou GB	API	1
req_count	Solicitações	Número de vezes que a API foi chamada.	≥ 0	API	1
req_count_2xx	Respostas 2xx	Número de vezes que a API retorna uma resposta 2xx.	≥ 0	API	1
req_count_4xx	Erros 4xx	Número de vezes que a API retorna um erro 4xx.	≥ 0	API	1
req_count_5xx	Erros 5xx	Número de vezes que a API retorna um erro 5xx.	≥ 0	API	1
req_count_error	Erros totais	Número total de erros retornados pela API.	≥ 0	API	1

Tabela 12-35 Métricas de gateway dedicadas

ID	Nome	Descrição	Intervalo de valores	Objeto monitorado	Período de monitoramento (minuto)
requests	Solicitações	Número de vezes que todas as APIs em um gateway dedicado foram chamadas.	≥0	Gateway dedicado	1
error_4xx	Erros 4xx	Número de vezes que todas as APIs no gateway dedicado retornam um erro 4xx.	≥0	Gateway dedicado	1
error_5xx	Erros 5xx	Número de vezes que todas as APIs no gateway dedicado retornam um erro 5xx.	≥0	Gateway dedicado	1
throttled_calls	Chamadas API limitadas	Número de vezes que todas as APIs no gateway dedicado foram limitadas.	≥0	Gateway dedicado	1
avg_latency	Latência média	Latência média de todas as APIs no gateway.	≥0 Unidade: ms	Gateway dedicado	1
max_latency	Máxima latência	Máxima latência de todas as APIs no gateway.	≥0 Unidade: ms	Gateway dedicado	1
req_count	Solicitações	Número de vezes que uma API foi chamada.	≥ 0	API	1
req_count_2xx	Respostas 2xx	Número de vezes que a API retorna uma resposta 2xx.	≥ 0	API	1
req_count_4xx	Erros 4xx	Número de vezes que a API retorna um erro 4xx.	≥ 0	API	1

ID	Nome	Descrição	Intervalo de valores	Objeto monitorado	Período de monitoramento (minuto)
req_count_5xx	Erros 5xx	Número de vezes que a API retorna um erro 5xx.	≥ 0	API	1
req_count_error	Erros totais	Número total de erros retornados pela API.	≥ 0	API	1
avg_latency	Latência média	Latência média da API.	≥ 0 Unidade: ms	API	1
max_latency	Máxima latência	Máxima latência da API.	≥ 0 Unidade: ms	API	1
input_throughput	Tráfego de entrada	Tráfego de entrada da API.	≥ 0 Unidade: byte, KB, MB ou GB	API	1
output_throughput	Tráfego de saída	Tráfego de saída da API.	≥ 0 Unidade: byte, KB, MB ou GB	API	1

Dimensão

Tabela 12-36 Dimensão de monitoramento de gateway compartilhado

Chave	Valor
api_id	API

Tabela 12-37 Dimensões dedicadas de monitoramento de gateway

Chave	Valor
instance_id	Gateway dedicado
api_id	API

12.3.10.2 Criação de regras de alarme

Cenário

Você pode criar regras de alarme para monitorar o status de suas APIs.

Uma regra de alarme consiste em um nome de regra, objetos monitorados, métricas, limites de alarme, intervalo de monitoramento e notificação.

Pré-requisitos

Uma API foi chamada.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Clique no nome da API de destino.

Passo 7 Na página de guia **Dashboard**, clique em **View Metric** para acessar o console do Cloud Eye. Em seguida, crie uma regra de alarme. Para detalhes, veja **Criação de uma regra de alarme**.

----Fim

12.3.10.3 Exibição de métricas

Cenário

O Cloud Eye monitora o status de suas APIs e permite que você visualize suas métricas.

Pré-requisitos

Você criou um grupo de API e uma API.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.

- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Publishing** > **APIs**.

Passo 6 Clique no nome da API de destino.

As métricas da API são exibidas na página de guia **Dashboard**.

Passo 7 Clique em **View Metric** para exibir mais métricas no console do Cloud Eye.

NOTA

Os dados de monitoramento são mantidos por dois dias. Para reter os dados por um período mais longo, salve-os em um intervalo do OBS.

----Fim

12.4 Chamada de API

12.4.1 Gerenciamento de aplicações

12.4.1.1 Criação de uma aplicação e obtenção de autorização

Cenário

Para uma API que usa autenticação de aplicação, crie uma aplicação e use o ID e o par de chaves (AppKey e AppSecret) para chamar a API. Você pode usar uma aplicação para chamar uma API somente depois de vincular a aplicação à API. Ao chamar a API, substitua o par de chaves no SDK por seu próprio par de chaves para que o APIG possa autenticar sua identidade. Para obter detalhes sobre a autenticação de aplicativos, consulte **Guia de desenvolvedor**.

NOTA

- Se o modo de autenticação da API de destino tiver sido definido como **None** ou **IAM**, não será necessário criar aplicações para chamar essa API.

Criação de uma aplicação

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em  no canto superior esquerdo e selecione uma região.

Passo 3 Clique em  no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Clique em **Create App** e configure as informações da aplicação.

Tabela 12-38 Informações da aplicação

Parâmetro	Descrição
Name	Nome de aplicação.
Description	Descrição da aplicação.

NOTA

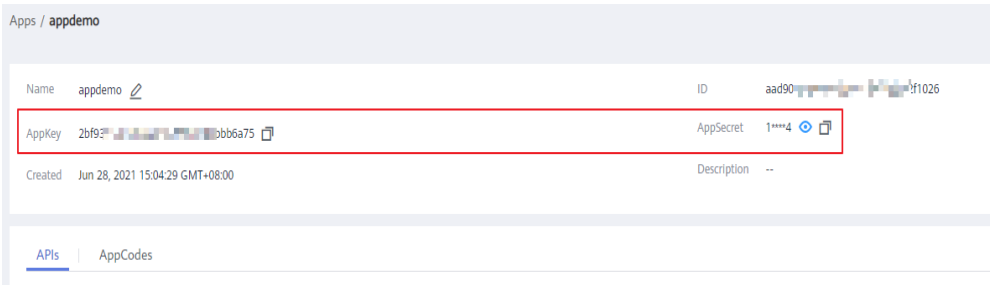
Você pode personalizar AppKeys e AppSecrets em gateways dedicados. Um AppKey é um identificador e deve ser globalmente exclusivo. Ele é gerado automaticamente. Não é aconselhável personalizar um, a menos que seja necessário.

Passo 7 Clique em **OK**.

Depois que a aplicação é criada, sua nome e ID são exibidos na lista de aplicações.

Passo 8 Clique no nome da aplicação e visualize o AppKey e o AppSecret na página de detalhes da aplicação.

Figura 12-35 Detalhes da aplicação



----Fim

Vinculação de uma aplicação a uma API

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Vincule uma aplicação a uma API. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da aplicação, clique em **Bind to API** e, em seguida, clique em **Select API**.
- Clique no nome da aplicação de destino e clique em **Select API**.

Passo 7 Selecione um ambiente, selecione uma API e clique em **OK**.

Depois que a vinculação for concluída, você poderá visualizar a API na página de detalhes da aplicação.

NOTA

- Somente APIs que usam autenticação de aplicações podem ser vinculadas a aplicações.
- Uma aplicação pode ser vinculada a várias APIs que usam autenticação de aplicação, e cada uma dessas API pode ser vinculada a várias aplicações.
- Para depurar uma API à qual a aplicação está vinculada, clique em **Debug** na linha que contém a API.

----Fim

Criação de uma aplicação chamando uma API

Você também pode criar uma aplicação chamando uma API fornecida pelo APIG. Para obter detalhes, consulte a seguinte referência:

Criação de uma aplicação

Operações de acompanhamento

Você pode chamar APIs usando métodos de autenticação diferentes. Para mais detalhes, consulte **Chamada das APIs**.

12.4.1.2 Exclusão de uma aplicação

Cenário

Você pode excluir aplicações que não precisam mais.

Pré-requisitos

Você criou uma aplicação.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Exclua uma aplicação. Você pode usar um dos seguintes métodos:

- Na coluna **Operation** da aplicação que você deseja excluir, clique em **Delete**.
- Clique no nome da aplicação de destino e clique em **Delete App** no canto superior direito da página de detalhes da aplicação exibida.

NOTA

Se a aplicação tiver sido vinculada a qualquer API, você deverá desvinculá-la e excluí-la.

Passo 7 Clique em **Yes**.

----Fim

Excluir uma aplicação chamando uma API

Você também pode excluir uma aplicação chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Exclusão de uma aplicação**.

12.4.1.3 Redefinição do AppSecret de uma aplicação

Cenário

Você pode redefinir o AppSecret de uma aplicação. A AppKey é única e não pode ser redefinida. Quando você redefine o AppSecret, ele se torna inválido e as APIs vinculadas à aplicação não podem ser chamadas. Para ativar as chamadas de API para essa aplicação novamente, você precisará atualizar o AppSecret da aplicação usada.

Pré-requisitos

Você criou uma aplicação.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Clique no nome da aplicação de destino.

Passo 7 No canto superior direito da página de detalhes da aplicação exibida, clique em **Reset AppSecret**.

Passo 8 Clique em **Yes**.

----Fim

Redefinição do AppSecret chamando uma API

Você também pode redefinir o AppSecret de uma aplicação chamando uma API fornecida pelo APIG. Para obter detalhes, consulte **Redefinição de um AppSecret**.

12.4.1.4 Adição de um AppCode para autenticação simples

Cenário

AppCodes são credenciais de identidade de uma aplicação usada para chamar APIs no modo de autenticação simples. Nesse modo, o parâmetro **X-Apig-AppCode** (cujo valor é um AppCode na página de detalhes do aplicação) é adicionado ao cabeçalho da solicitação HTTP para resposta rápida. O APIG verifica apenas o AppCode e o conteúdo da solicitação não precisa ser assinado.

Quando uma API é chamada usando a autenticação de aplicação e a autenticação simples está habilitada para a API, AppKey e AppSecret podem ser usados para assinar e verificar a solicitação de API. AppCode também pode ser usado para autenticação simples.

NOTA

- Por motivos de segurança, a autenticação simples suporta apenas chamadas de API por HTTPS.
- Você pode criar no máximo cinco AppCodes para cada aplicação.

Pré-requisitos

Você criou uma aplicação.

Gerenciamento de um AppCode

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

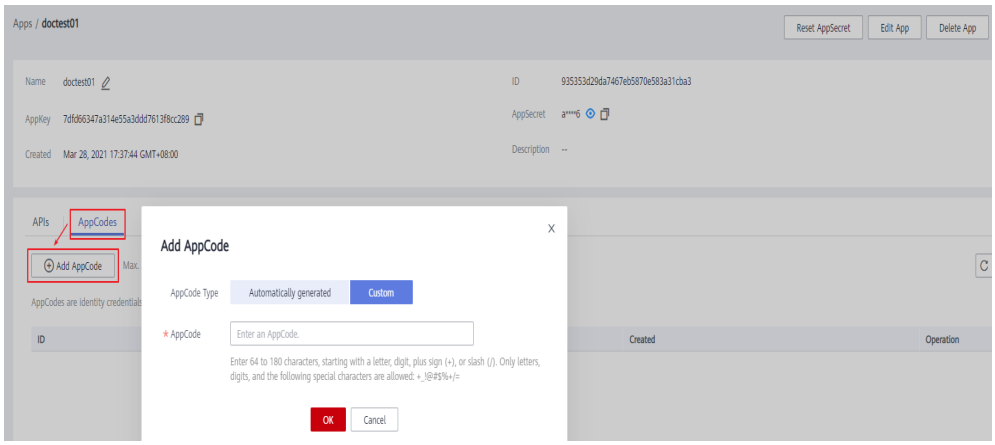
- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Clique no nome da aplicação de destino.

Passo 7 Clique na guia **AppCodes**.

Passo 8 Clique em **Add AppCode** para gerar um arquivo. Ele pode ser gerado automaticamente ou personalizado.



----Fim

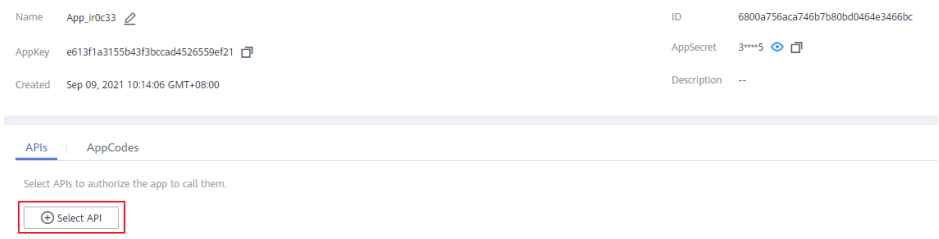
Usar o AppCode para autenticação simples de solicitações de API

Passo 1 Ao criar uma API, defina **Security Authentication** como **App** e ative **Simple Authentication**.

NOTA

Depois de habilitar a autenticação simples para uma API existente, você precisa publicar a API novamente para que a configuração entre em vigor.

Passo 2 Vincule uma aplicação à API.



Passo 3 Ao enviar uma solicitação, adicione o parâmetro **X-Apig-AppCode** ao cabeçalho da solicitação e omita a assinatura da solicitação.

Por exemplo, ao usar curl, adicione o parâmetro **X-Apig-AppCode** ao cabeçalho da solicitação e defina o valor do parâmetro como **AppCode gerado**.

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

----Fim

12.4.1.5 Visualização de detalhes da API

Cenário

Você pode ver os detalhes de uma API à qual uma aplicação foi vinculada.

Pré-requisitos

- Você criou uma aplicação.
- A aplicação foi vinculada a uma API.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha um tipo de gateway no painel de navegação.

- **Shared Gateway**: você pode criar e gerenciar APIs imediatamente. Você será cobrado com base no número de chamadas de API.
- **Dedicated Gateways**: você pode criar e gerenciar APIs depois de comprar um gateway. Você será cobrado com base na duração de uso do gateway.

Passo 5 No painel de navegação, escolha **API Calling** > **Apps**.

Passo 6 Clique no nome da aplicação de destino.

Passo 7 Clique no nome da API de destino para visualizar seus detalhes.

----Fim

12.4.2 Análise de logs

Cenário

Esta seção descreve como obter e analisar os logs de chamadas da API de gateways dedicados.

Pré-requisitos

APIs foram chamadas.

Procedimento

Passo 1 Acesse o console de gerenciamento.

Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Dedicated Gateways**. Em seguida, clique em **Access Console** no canto superior direito de um gateway dedicado.

Passo 5 Escolha **API Calling > Access Logs** e clique em **Configure Log Collection**.

Passo 6 Habilite a coleta de logs ( ).

Passo 7 Especifique um grupo de logs e um fluxo de logs e clique em **OK**. Para obter detalhes sobre grupos de logs e fluxos de logs, consulte **Gerenciamento de log**.

Passo 8 Clique em **Log Fields** para exibir a descrição de cada campo de log. Em seguida, visualize e analise os logs consultando as descrições dos campos de log.

Passo 9 Para exportar logs, consulte **Transferência de log**.

Os campos nos logs de acesso são separados usando espaços. A tabela a seguir descreve cada campo de log.

Tabela 12-39 Descrição do campo de log

Nº	Campo	Descrição
1	remote_addr	Endereço IP do cliente
2	request_id	ID da solicitação
3	api_id	ID da API
4	user_id	ID do projeto fornecido por um solicitante para autenticação do IAM
5	app_id	ID da aplicação fornecido por um solicitante para autenticação baseada em aplicação
6	time_local	Hora em que uma solicitação é recebida
7	request_time	Latência de solicitação.
8	request_method	Método de solicitação HTTP
9	host	Nome de domínio
10	router_uri	URI de solicitação
11	server_protocol	Protocolo de solicitação
12	status	Código do status da resposta
13	bytes_sent	Tamanho da resposta em bytes, incluindo a linha de status, cabeçalho e corpo.
14	request_length	O comprimento da solicitação em bytes, incluindo a linha inicial, o cabeçalho e o corpo.
15	http_user_agent	ID do agente do usuário
16	http_x_forwarded_for	Campo de cabeçalho X-Forwarded-For

Nº	Campo	Descrição
17	upstream_addr	Endereço de back-end
18	upstream_uri	URI de back-end
19	upstream_status	Código de resposta do back-end
20	upstream_connect_time	Tempo necessário para estabelecer uma conexão com o back-end
21	upstream_header_time	Duração desde o início do estabelecimento de uma conexão até o recebimento do primeiro byte do back-end
22	upstream_response_time	Duração desde o início do estabelecimento de uma conexão até o recebimento do último byte do back-end
23	region_id	ID da região

----Fim

12.4.3 SDKs

O APIG é compatível com autenticação de API baseada em IAM, aplicações e autorizadores personalizados. Você também pode optar por não autenticar solicitações de API. Para obter detalhes sobre as diferenças entre os modos de autenticação, consulte **Como escolher um modo de autenticação**.

Esta seção descreve como fazer download de SDKs e visualizar instruções relacionadas.

Para obter detalhes sobre a autenticação do IAM, consulte **Chamada de APIs por meio da autenticação do IAM**.

Cenário

Os SDKs são usados quando você chama APIs por meio da autenticação da aplicação. Faça o download dos SDKs e da documentação relacionada e, em seguida, chame as APIs seguindo as instruções da documentação.

Procedimento

Passo 1 Acesse o console de gerenciamento.

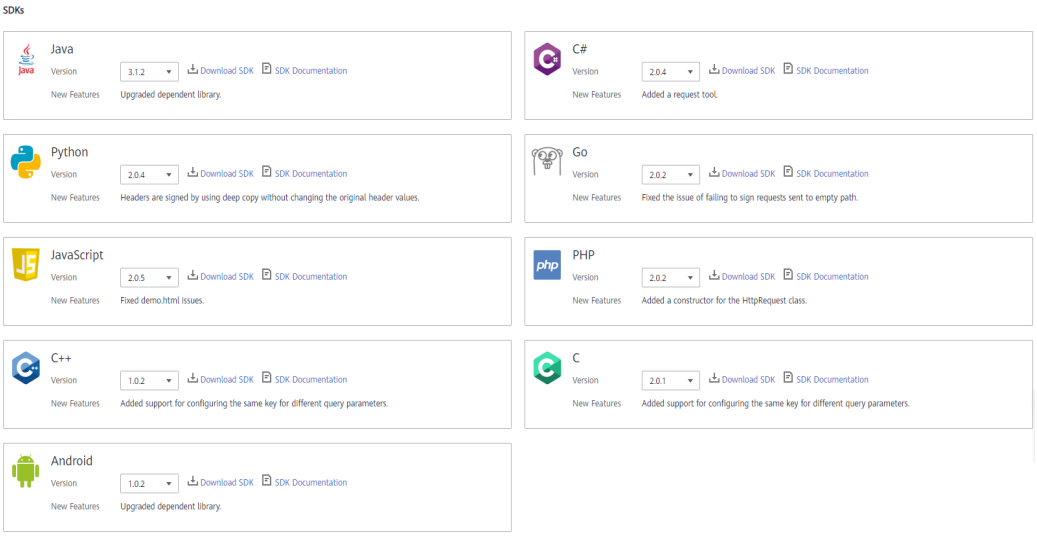
Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 Escolha **Help Center** > **SDK Process Flow**.

Passo 5 Clique em **Download SDK** da linguagem desejada.

Para ver o guia de suporte, clique em **SDK Documentation**.



----Fim

12.4.4 APIs compradas

Cenário

No gateway compartilhado, você pode visualizar as APIs compradas e depurar as APIs para verificar se elas estão sendo executadas corretamente.

As APIs compradas devem ser chamadas usando a autenticação da aplicação.

Pré-requisitos

Você comprou APIs por meio do KooGallery.

Procedimento

Passo 1 Acesse o console de gerenciamento.

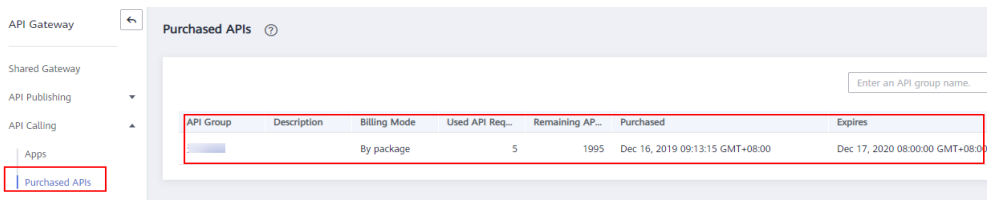
Passo 2 Clique em no canto superior esquerdo e selecione uma região.

Passo 3 Clique em no canto superior esquerdo e escolha **API Gateway**.

Passo 4 No painel de navegação, escolha **Shared Gateway**.

Passo 5 No painel de navegação, escolha **API Calling** > **Purchased APIs**.

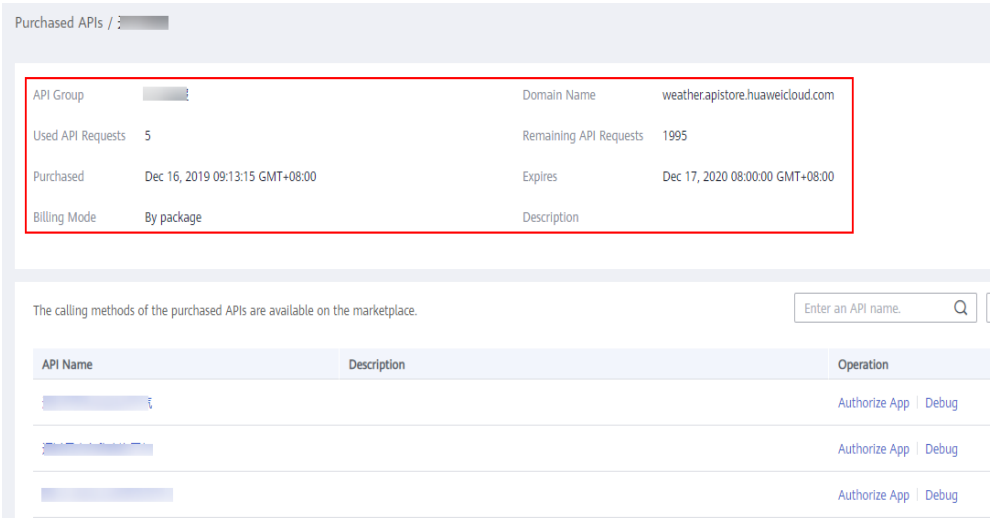
Figura 12-36 Grupo de API comprado



Passo 6 Clique no nome do grupo de API de destino.

Os detalhes do grupo de API e das APIs compradas sob o grupo são exibidos.

Figura 12-37 Detalhes do grupo de API



Passo 7 Na coluna **Operation** da API desejada, clique em **Debug**.

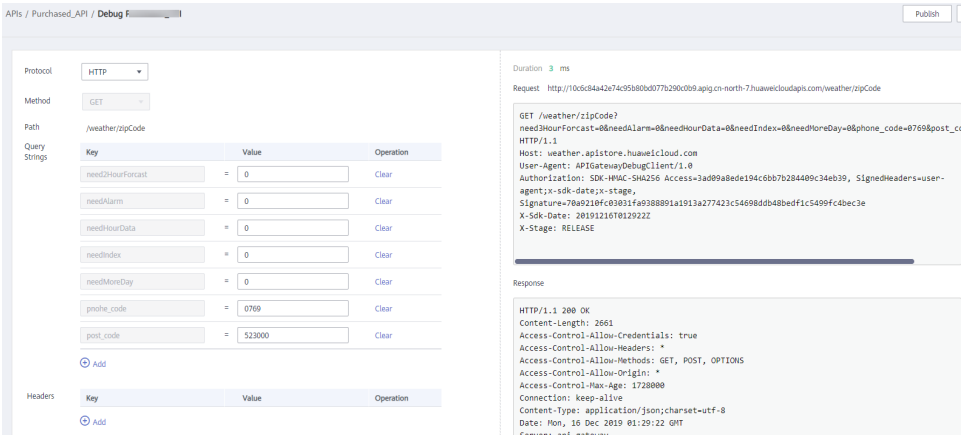
Passo 8 No lado esquerdo, defina os parâmetros de solicitação da API listados em **Tabela 12-40**. No lado direito, veja as informações de solicitação e resposta da API depois de clicar em **Send Request**.

Tabela 12-40 Parâmetros para depurar uma API

Parâmetro	Descrição
Protocol	Você pode modificar este parâmetro somente se tiver definido **Protocol** para **HTTP&HTTPS** para a API.
Method	Você pode modificar esse parâmetro somente se tiver definido **Method** como **ANY** para a API.
Suffix	Você pode modificar esse parâmetro somente se tiver definido **Matching** ao **Prefix match** para a API.
Path Parameters	Você pode modificar esse parâmetro somente se o valor de **Path** contiver aparelhos ortodônticos ({}).
Headers	Cabeçalhos e valores HTTP.
Query Strings	Consultar parâmetros e valores de cadeia.
Body	Você só pode modificar esse parâmetro se tiver definido **Method** como **PATCH**, **POST** ou **PUT** para a API.

Passo 9 Depois de definir os parâmetros da solicitação, clique em **Send Request**.

A seção **Response** exibe a resposta da solicitação da API.



Passo 10 Você pode enviar mais solicitações com diferentes parâmetros e valores para verificar a API.

----Fim

12.4.5 Chamada de APIs publicadas

12.4.5.1 Chamada das APIs

Obtenção de APIs e documentação

Antes de chamar as APIs, obtenha as informações de solicitação do provedor da API, incluindo os parâmetros de nome de domínio de acesso, protocolo, método, caminho e solicitação.

Obtenha APIs: da sua empresa ou de um parceiro

Obtenha a documentação relacionada

- Para APIs obtidas da Huawei Cloud, obtenha documentação na **Central de ajuda**.

As informações de autenticação a serem obtidas variam com o modo de autenticação da API.

- Autenticação de aplicação:
  - Autenticação de assinatura: obtenha a chave e o segredo (ou AppKey e AppSecret do cliente) da aplicação autorizada para a API do provedor de API, bem como o SDK para chamar a API.
  - Autenticação simples: obtenha o AppCode da aplicação autorizada para a API do provedor de API.
  - Outros modos de autenticação: obtenha a chave e o segredo (ou AppKey e AppSecret do cliente) da aplicação autorizada para a API do provedor de API.
- Autenticação do IAM: a credencial da conta (token ou AK/SK obtido com a conta e a senha) obtida na plataforma de serviço em nuvem é usada para autenticação. Se o AK/SK for usado para autenticação, você também precisará obter o SDK do provedor da API para chamar a API.
- Autenticação personalizada: obtenha as informações de autenticação personalizadas a serem transportadas nos parâmetros de solicitação do provedor de API.
- Nenhum: nenhuma informação de autenticação é necessária.

Chamar uma API

NOTA

Esta seção descreve somente a configuração do caminho da solicitação e dos parâmetros de autenticação. Para outros parâmetros, como tempo limite e SSL, configure-os conforme necessário. Para evitar perdas de serviço devido a parâmetros incorretos, configure-os consultando os padrões da indústria.

Passo 1 Defina o caminho da solicitação.

Cenário	Configuração de parâmetros de solicitação
Chamar uma API com um nome de domínio	Chame a API usando **o nome de subdomínio alocado para o grupo de API ou um nome de domínio associado ao grupo**. Não é necessária configuração adicional.
Chamar uma API no grupo DEFAULT com um endereço IP	No gateway compartilhado, chame uma API no grupo DEFAULT com um endereço IP. Não é necessária configuração adicional.
Chamar uma API em um grupo não DEFAULT com um endereço IP	● Para chamar APIs usando um endereço IP, certifique-se de que o parâmetro **app_route** tenha sido definido como **on** na página da guia **Parâmetros de configuração** do gateway dedicado. ● Para usar um endereço IP para chamar uma API que usa autenticação de aplicação em um grupo não-DEFAULT, adicione os parâmetros de cabeçalho **X-HW-ID** e **X-HW-APPKEY** e defina os valores de parâmetro para a chave e o segredo de uma aplicação autorizada para a API ou um AppKey e AppSecret do cliente. ● Para usar um endereço IP para chamar uma API que não usa autenticação de aplicação em um grupo que não é DEFAULT, adicione o parâmetro de cabeçalho **host**.

Passo 2 Defina os parâmetros de autenticação.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação de aplicação (com uma assinatura)	Use o SDK para assinar solicitações de API. Para obter detalhes, consulte **Chamar APIs por meio de autenticação de aplicação**.
Autenticação de aplicação (através de autenticação simples)	Adicione o parâmetro de cabeçalho **X-Apig-AppCode** e defina o valor do parâmetro para o AppCode obtido em **Obtenção de APIs e documentação**. Para obter detalhes, consulte **Primeiros passos**.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação de aplicação (com app_api_key)	● Para habilitar a autenticação app_api_key, certifique-se de que o parâmetro **app_api_key** tenha sido definido como **on** na página da guia **Parâmetros de configuração** do gateway dedicado. ● Adicione o parâmetro **apikey** do cabeçalho ou da cadeia de consulta e defina o valor do parâmetro para a chave ou AppKey obtida em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_secret)	● Na página da guia **Parâmetros de configuração** de um gateway dedicado, o parâmetro **app_secret** foi definido como **on** para ativar a autenticação app_secret e **app_api_key** foi definido como **off** para desativar a autenticação app_api_key. ● Adicione o parâmetro **X-HW-ID** do cabeçalho e defina o valor do parâmetro como a chave da aplicação autorizada para a API ou o AppKey do cliente. ● Adicione o parâmetro de cabeçalho **X-HW-AppKey** e defina o valor do parâmetro para o secret ou AppSecret obtido em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_basic)	● Para habilitar a autenticação app_basic, assegure-se de que o parâmetro **app_basic** tenha sido definido como **on** na página da guia **Parâmetros de configuração** do gateway dedicado. ● Adicione o parâmetro de cabeçalho **Authorization** e defina o valor do parâmetro como "Basic + base64 (*appkey* + : + *appsecret*)", em que *appkey* e *appsecret* são a chave e o segredo (ou AppKey e AppSecret) obtidos em **Obtenção de APIs e documentação**.
Autenticação de aplicação (com app_jwt)	● Para habilitar a autenticação app_jwt, verifique se o parâmetro **app_jwt** foi definido como **on** na página de guia **Parâmetros de configuração** do gateway dedicado. ● Adicione o parâmetro de cabeçalho **Timestamp** e defina o valor do parâmetro para o carimbo de data/hora Unix da hora atual. ● Adicione o parâmetro de cabeçalho **Authorization** e defina o valor do parâmetro como "sha256 (*appkey* + *appsecret* + *timestamp*)", no qual *appkey* e *appsecret* são a chave e segredo (ou AppKey e AppSecret) obtidos em **Obtenção de APIs e documentação** e *carimbo de data/hora* é o carimbo de data/hora Unix da hora atual.

Modo de autenticação	Configuração de parâmetros de solicitação
Autenticação do IAM (com um token)	Obtenha um token da plataforma de nuvem e transporte o token em solicitações de API para autenticação. Para obter detalhes, consulte **Autenticação de token**.
Autenticação do IAM (com AK/SK)	Use um SDK para assinar solicitações de API. Para obter detalhes, consulte **Autenticação de AK/SK**.
Autenticação personalizada	Carregue informações de autenticação em parâmetros de solicitação de API para autenticação.
Nenhum	Chamar APIs sem autenticação.

----Fim

12.4.5.2 Cabeçalhos de resposta

A tabela a seguir descreve os cabeçalhos de resposta que o APIG adiciona à resposta retornada quando uma API é chamada.

X-Apig-Mode: debug indica informações de depuração da API.

Cabeçalho de resposta	Descrição	Observações
X-Request-Id	ID de solicitação.	Retornado para todos as solicitações válidas.
X-Apig-Latency	Duração desde o momento em que o APIG recebe uma solicitação até o momento em que o back-end retorna um cabeçalho da mensagem.	Retornado somente quando o cabeçalho da requisição contém **X-Apig-Mode: debug**.
X-Apig-Upstream-Latency	Duração desde o momento em que o APIG envia uma solicitação para o back-end até o momento em que o back-end retorna um cabeçalho de mensagem.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e o tipo de back-end não é Mock.
X-Apig-RateLimit-api	Informações de limite de solicitação de API. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada.

Cabeçalho de resposta	Descrição	Observações
X-Apig-RateLimit-user	Informações de limite de solicitação do usuário. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por um usuário.
X-Apig-RateLimit-app	Informações de limite de solicitação de aplicação. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por uma aplicação.
X-Apig-RateLimit-ip	Informações de limite de solicitação de endereço IP. Exemplo: **remain:9,limit:10,time:10 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug** e um limite foi configurado para o número de vezes que a API pode ser chamada por um endereço IP.
X-Apig-RateLimit-api-allenv	Informações de limite de solicitação de API padrão. Exemplo: **remain:199,limit:200,time:1 second**.	Retornado somente quando o cabeçalho da solicitação contém **X-Apig-Mode: debug**.

12.4.5.3 Códigos de erro

A **Tabela 12-41** lista os códigos de erro que você pode encontrar ao chamar APIs. Se um código de erro começando com **APIGW** for retornado após chamar uma API, corrija a falha consultando as instruções fornecidas em **Códigos de erro**.

NOTA

- Para obter detalhes sobre os códigos de erro que podem ocorrer ao gerenciar APIs, consulte **Códigos de erro**.
- Se ocorrer um erro ao usar APIG, localize a mensagem de erro e a descrição na tabela a seguir de acordo com o código de erro, por exemplo, APIG.0101. As mensagens de erro estão sujeitas a alterações sem aviso prévio.

Tabela 12-41 Códigos de erro

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0101	The API does not exist or has not been published in the environment.	404	A API não existe ou não foi publicada no ambiente.	Verifique se o nome de domínio, o método e o caminho são consistentes com os da API registrada. Verifique se a API foi publicada. Se tiver sido publicado em um ambiente que não seja de produção, verifique se o cabeçalho X-Stage na solicitação é o nome do ambiente. Verifique se o nome de domínio usado para chamar a API foi vinculado ao grupo ao qual a API pertence.
APIG.0101	The API does not exist.	404	O método de solicitação da API não existe.	Verifique se o método de solicitação da API é o mesmo que o método definido pela API.
APIG.0103	The backend does not exist.	500	O serviço de back-end não foi encontrado.	Entre em contato com o suporte técnico.
APIG.0104	The plug-ins do not exist.	500	Nenhuma configuração de plug-in foi encontrada.	Entre em contato com o suporte técnico.
APIG.0105	The backend configurations do not exist.	500	Nenhuma configuração de back-end foi encontrada.	Entre em contato com o suporte técnico.
APIG.0106	Orchestration error.	400	Ocorreu um erro de orquestração.	Verifique se os parâmetros front-end e back-end da API estão corretos.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0201	API request error.	400	Parâmetros de solicitação inválidos.	Defina parâmetros de solicitação válidos.
APIG.0201	Request entity too large.	413	O corpo da solicitação excede 12 MB.	Reduza o tamanho do corpo da solicitação.
APIG.0201	Request URI too large.	414	O URI da solicitação excede 32 KB.	Reduza o tamanho do URI da solicitação.
APIG.0201	Request headers too large.	494	Os cabeçalhos de solicitação são muito grandes porque um deles excede 32 KB ou o comprimento total excede 128 KB.	Reduza o tamanho dos cabeçalhos da solicitação.
APIG.0201	Backend unavailable.	502	O serviço de back-end não está disponível.	Verifique se o endereço de back-end configurado para a API está acessível.
APIG.0201	Backend timeout.	504	O serviço de back-end expirou o tempo limite.	Aumente a duração do tempo limite do serviço de back-end ou reduza o tempo de processamento.
APIG.0201	An unexpected error occurred	500	Ocorreu um erro interno.	Entre em contato com o suporte técnico.
APIG.0202	Backend unavailable	502	O back-end não está disponível.	Verifique se o protocolo de solicitação de back-end configurado para a API é o mesmo que o protocolo de solicitação usado pelo serviço de back-end.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0203	Backend timeout.	504	O serviço de back-end expirou o tempo limite.	Aumente o tempo limite do serviço de back-end ou diminua seu tempo de processamento.
APIG.0204	SSL protocol is not supported: TLSv1.1	400	A versão do protocolo SSL não é suportada.	Use uma versão suportada do protocolo SSL.
APIG.0301	Incorrect IAM authentication information.	401	Os detalhes de autenticação do IAM estão incorretos.	Verifique se o token está correto.
APIG.0302	The IAM user is not authorized to access the API.	403	O usuário do IAM não tem permissão para acessar a API.	Verifique se o usuário é controlado por uma lista negra ou lista branca.
APIG.0303	Incorrect app authentication information.	401	Os detalhes de autenticação da aplicação estão incorretos.	Verifique se o método de solicitação, o caminho, as cadeias de consulta e o corpo da solicitação são consistentes com aqueles usados para assinatura; verificar se a data e hora do cliente estão corretas; e verifique se o código de assinatura está correto consultando **Chamada de APIs por meio de autenticação de aplicação**.
APIG.0304	The app is not authorized to access the API.	403	A aplicação não tem permissão para acessar a API.	Verifique se a aplicação foi autorizada a acessar a API.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0305	Incorrect authentication information.	401	As informações de autenticação estão incorretas.	Verifique se as informações de autenticação estão corretas.
APIG.0306	API access denied.	403	O acesso à API não é permitido.	Verifique se você foi autorizado a acessar a API.
APIG.0307	The token must be updated.	401	O token precisa ser atualizado.	Obtenha um novo token do IAM.
APIG.0308	The throttling threshold has been reached.	429	O limite de limitação foi atingido.	Tente novamente depois que a limitação for retomada. Se o número de solicitações de subdomínio por dia for atingido, vincule um nome de domínio independente à API.
APIG.0310	The project is unavailable.	403	O projeto está indisponível no momento.	Selecione outro projeto e tente novamente.
APIG.0311	Incorrect debugging authentication information.	401	Os detalhes de autenticação de depuração estão incorretos.	Entre em contato com o suporte técnico.
APIG.0401	Unknown client IP address.	403	O endereço IP do cliente não pode ser identificado.	Entre em contato com o suporte técnico.
APIG.0402	The IP address is not authorized to access the API.	403	O endereço IP não tem permissão para acessar a API.	Verifique se o endereço IP é controlado por uma lista negra ou lista branca.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0404	Access to the backend IP address has been denied.	403	O endereço IP do back-end não pode ser acessado.	Verifique se o endereço IP do back-end ou o endereço IP correspondente ao nome de domínio do back-end está acessível.
APIG.0501	The app quota has been used up.	405	A cota da aplicação foi atingida.	Aumente a cota da aplicação.
APIG.0502	The app has been frozen.	405	A aplicação foi congelada.	Verifique se o saldo da sua conta é suficiente.
APIG.0601	Internal server error.	500	Ocorreu um erro interno.	Entre em contato com o suporte técnico.
APIG.0602	Bad request.	400	Pedido inválido.	Verifique se a solicitação é válida.
APIG.0605	Domain name resolution failed.	500	Falha na resolução do nome de domínio.	Verifique se o nome de domínio está correto e foi vinculado a um endereço de back-end correto.
APIG.0606	Failed to load the API configurations.	500	As configurações da API não puderam ser carregadas.	Entre em contato com o suporte técnico.
APIG.0607	The following protocol is supported: {xxx}	400	O protocolo não é suportado. Somente *xxx* é suportado. *xxx* está sujeito ao valor real na resposta.	Use HTTP ou HTTPS para acessar a API.
APIG.0608	Failed to obtain the admin token.	500	Os detalhes do locatário não podem ser obtidos.	Entre em contato com o suporte técnico.

Código de erro	Mensagem de erro	Código de status HTTP	Descrição	Solução
APIG.0609	The VPC backend does not exist.	500	O serviço de back-end da VPC não pode ser encontrado.	Entre em contato com o suporte técnico.
APIG.0610	No backend available.	502	Não há serviços de back-end disponíveis.	Verifique se todos os serviços de back-end estão disponíveis. Por exemplo, verifique se as informações de chamada da API são consistentes com a configuração real.
APIG.0611	The backend port does not exist.	500	A porta de back-end não foi encontrada.	Entre em contato com o suporte técnico.
APIG.0612	An API cannot call itself.	500	Uma API não pode chamar a si mesma.	Modifique as configurações de back-end e garanta que o número de camadas que a API é chamada recursivamente não exceda 10.
APIG.0613	The IAM service is currently unavailable.	503	O IAM não está disponível no momento.	Entre em contato com o suporte técnico.
APIG.0705	Backend signature calculation failed.	500	Falha no cálculo da assinatura de back-end.	Entre em contato com o suporte técnico.
APIG.0802	The IAM user is forbidden in the currently selected region	403	O usuário do IAM está desativado na região atual.	Entre em contato com o suporte técnico.
APIG.1009	AppKey or AppSecret is invalid	400	O AppKey e o AppSecret são inválidos.	Verifique se o AppKey e o AppSecret da solicitação estão corretos.

12.5 Gerenciamento de permissões

12.5.1 Criação de um usuário e concessão de permissões do APIG

Este tópico descreve como usar o **Identity and Access Management** (IAM) para implementar o controle de permissões para seus recursos do APIG. Com o IAM, você pode:

- Criar usuários do IAM para funcionários com base na estrutura organizacional da sua empresa. Cada usuário do IAM terá suas próprias credenciais de segurança para acessar os recursos do APIG.
- Conceder somente as permissões necessárias para que os usuários executem uma tarefa específica.
- Confie uma conta da Huawei Cloud ou um serviço de nuvem para realizar O&M em seus recursos do APIG.

Se sua conta da Huawei Cloud não requer usuários individuais do IAM, pule este capítulo.

Esta seção descreve o procedimento para conceder permissões (consulte **Figura 12-38**).

Pré-requisitos

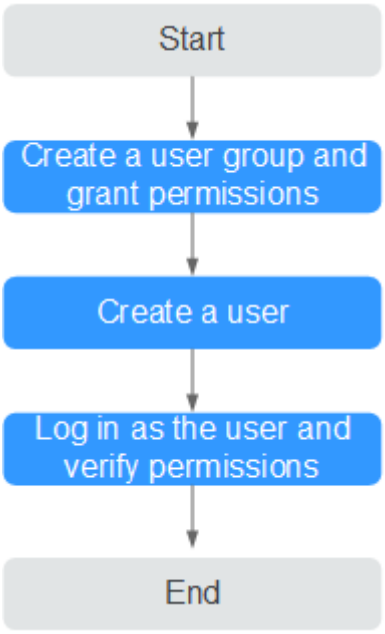
Saiba mais sobre as permissões (consulte **Tabela 12-42**) suportadas pelo APIG e escolha políticas ou funções de acordo com seus requisitos. Para obter as permissões de outros serviços, consulte **Others** > **System Permissions** na lista de serviços.

Tabela 12-42 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

Fluxo do processo

Figura 12-38 Processo para conceder permissões do APIG



1. **Criar um grupo de usuários e atribua permissões**.

   Crie um grupo de usuários no console do IAM e anexe o papel de **APIG Administrator** ou a política de **APIG FullAccess** ao grupo.

2. **Criar um usuário IAM**.

   Crie um usuário no console do IAM e adicione o usuário ao grupo criado em **1**.

3. **Faça logon** e verifique as permissões.

   Faça logon no console do APIG como o usuário criado e verifique se o usuário tem permissões de administrador para o APIG.

12.5.2 Políticas personalizadas do APIG

As políticas personalizadas podem ser criadas para complementar as políticas definidas pelo sistema do APIG. Para as ações que podem ser adicionadas às políticas personalizadas, consulte **Políticas de permissões e ações suportadas**.

Você pode criar políticas personalizadas usando um dos seguintes métodos:

- Editor visual: selecione serviços em nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe de política.
- JSON: edite políticas de JSON do rascunho ou com base em uma política existente.

Para obter detalhes, consulte **Criação de uma política personalizada**. A seção a seguir contém exemplos de políticas customizadas do APIG comuns.

NOTA

Apenas gateways de API dedicados suportam políticas definidas pelo sistema e políticas personalizadas.

Exemplo de políticas personalizadas

- Exemplo 1: permitir que os usuários criem e depurem APIs

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    apig:apis:create
                    apig:apis:debug
                 "
            ]
        }
    ]
}
```

- Exemplo 2: negar criação de grupo de API

  Uma política com apenas permissões "Deny" deve ser usada em conjunto com outras políticas para entrar em vigor. Se as permissões atribuídas a um usuário contiverem "Allow" e "Deny", as permissões "Deny" terão precedência sobre as permissões "Allow".

  O método a seguir pode ser usado se você precisar atribuir permissões da política **APIG FullAccess** a um usuário, mas quiser impedir que o usuário crie grupos de API. Crie uma política personalizada para negar a criação de grupo de API e anexe ambas as políticas ao grupo ao qual o usuário pertence. Em seguida, o usuário pode executar todas as operações em gateways de API, exceto a criação de grupos de API. O seguinte é um exemplo de uma política de negação:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Deny",
                        "Action": [
                                "apig:groups:create"
                        ]
                }
        ]
}
```

12.6 Principais operações gravadas pelo CTS

12.6.1 Operações do APIG que podem ser gravadas pelo CTS

Ativação de CTS

Se você quiser coletar, registrar ou consultar logs de operação para APIG em cenários comuns, como análise de segurança, auditoria e localização de problemas, **habilite o Cloud Trace Service (CTS)**.

O CTS fornece as seguintes funções:

- Gravação de logs de auditoria
- Consulta de logs de auditoria
- Despejo de logs de auditoria

- Criptografia de arquivos de rastreamento
- Ativação de notificações de operações-chave

Exibição de operações principais

Com o CTS, você pode registrar operações associadas ao APIG para consultas futuras, auditorias e rastreamento inverso.

Tabela 12-43 Operações do APIG que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Criação de um grupo de API	ApiGroup	createApiGroup
Exclusão de um grupo de API	ApiGroup	deleteApiGroup
Atualização de um grupo de API	ApiGroup	updateApiGroup
Vinculação de um nome de domínio	ApiGroup	createDomainBinding
Alteração da versão mínima do TLS	ApiGroup	modifySecureTransmission
Desvinculação de um nome de domínio	ApiGroup	relieveDomainBinding
Adição de um certificado de domínio	ApiGroup	addDomainCertificate
Exclusão de um certificado de domínio	ApiGroup	deleteDomainCertificate
Criação de uma API	Api	createApi
Exclusão de uma API	Api	deleteApi
Exclusão de várias APIs	Api	batchDeleteApi
Atualização de uma API	Api	updateApi
Publicação de uma API	Api	publishApi
Deixar uma API off-line	Api	offlineApi
Publicar várias APIs ou deixar APIs off-line	Api	batchPublishOrOfflineApi
Alternação de versões da API	Api	switchApiVersion
Deixar uma versão da API off-line	Api	offlineApiByVersion
Depuração de uma API	Api	debugApi

Operação	Tipo de recurso	Nome do rastreamento
Criação de um ambiente	Environment	createEnvironment
Exclusão de um ambiente	Environment	deleteEnvironment
Atualização de um ambiente	Environment	updateEnvironment
Criação de uma variável de ambiente	EnvVariable	createEnvVariable
Atualização de uma variável de ambiente	EnvVariable	updateEnvVariable
Exclusão de uma variável de ambiente	EnvVariable	deleteEnvVariable
Criação de uma aplicação	App	createApp
Exclusão de uma aplicação	App	deleteApp
Atualização de uma aplicação	App	updateApp
Redefinição do AppSecret	App	resetAppSecret
Vinculação de um cliente a uma API	AppAuth	grantAuth
Desvinculação de um cliente de uma API	AppAuth	relieveAuth
Criação de uma chave de assinatura	Signature	createSignature
Exclusão de uma chave de assinatura	Signature	deleteSignature
Atualização de uma chave de assinatura	Signature	updateSignature
Vinculação de uma chave de assinatura	SignatureBinding	createSignatureBinding
Desvinculação de uma chave de assinatura	SignatureBinding	relieveSignatureBinding
Criação de uma política de controle de acesso	Acl	createAcl
Exclusão de uma política de controle de acesso	Acl	deleteAcl
Exclusão de políticas de controle de acesso	Acl	batchDeleteAcl
Atualização de uma política de controle de acesso	Acl	updateAcl

Operação	Tipo de recurso	Nome do rastreamento
Criação de uma lista negra de controle de acesso	Acl	addAclValue
Exclusão de uma lista negra de controle de acesso	Acl	deleteAclValue
Vinculação de uma política de controle de acesso a uma API	AclBinding	createAclBinding
Desvinculação de uma política de controle de acesso de uma API	AclBinding	relieveAclBinding
Desvinculação de várias políticas de controle de acesso de APIs	AclBinding	batchRelieveAclBinding
Criação de uma política de limitação de solicitações	Throttle	createThrottle
Exclusão de uma política de limitação de solicitações	Throttle	deleteThrottle
Exclusão de várias políticas de limitação de solicitações	Throttle	batchDeleteThrottle
Atualização de uma política de limitação de solicitações	Throttle	updateThrottle
Vinculação de uma política de limitação de solicitações	ThrottleBinding	createThrottleBinding
Desvinculação de uma política de limitação de solicitações	ThrottleBinding	relieveThrottleBinding
Desvinculação de várias políticas de limitação de solicitações	ThrottleBinding	batchRelieveThrottleBinding
Criação de uma configuração de limitação de solicitação excluída	ThrottleSpecial	createSpecialThrottle
Exclusão de uma configuração de limitação de solicitação excluída	ThrottleSpecial	deleteSpecialThrottle
Atualização de uma configuração de limitação de solicitação excluída	ThrottleSpecial	updateSpecialThrottle
Criação de um canal de balanceamento de carga	Vpc	createVpc

Operação	Tipo de recurso	Nome do rastreamento
Exclusão de um canal de balanceamento de carga	Vpc	deleteVpc
Atualização de um canal de balanceamento de carga	Vpc	updateVpc
Adição de membros a um canal de balanceamento de carga	Vpc	addVpcMember
Exclusão de membros de um canal de balanceamento de carga	Vpc	deleteVpcMember
Exportação de uma API	Swagger	swaggerExportApi
Exportação de várias APIs	Swagger	swaggerExportApiList
Exportação de todas as APIs em um grupo	Swagger	swaggerExportApiByGroup
Importação de APIs para um novo grupo	Swagger	swaggerImportApiTo-NewGroup
Importação de APIs para um grupo existente	Swagger	swaggerImportApiToEx-istGroup
Exportação de todos os back-ends personalizados	Swagger	SwaggerExportLdApi
Importação de back-ends personalizados	Swagger	SwaggerImportLdApi
Criação de um autorizador personalizado	Authorizer	createAuthorizer
Exclusão de um autorizador personalizado	Authorizer	deleteAuthorizer
Atualização de um autorizador personalizado	Authorizer	updateAuthorizer
Criação de um plug-in	Plugin	createPlugin
Atualização de um plug-in	Plugin	updatePlugin
Exclusão de um plug-in	Plugin	deletePlugin
Vinculação de um plug-in a uma API	Plugin	pluginAttachApi
Desvinculação de uma API de um plug-in	Plugin	pluginDetachApi
Vinculação de um plug-in a uma API	Plugin	apiAttachPlugin

Operação	Tipo de recurso	Nome do rastreamento
Desvinculação de um plug-in de uma API	Plugin	apiDetachPlugin

Desativação de CTS

Desabilite o CTS seguindo o procedimento em **Exclusão de um rastreador**.

12.6.2 Consulta de logs de auditoria

Consulte logs de auditoria seguindo o procedimento em **Consulta de rastreamentos em tempo real**.

Figura 12-39 Visualização de logs