API Gateway

Melhores práticas

Edição	01
Data	2025-02-27

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 Exposição seletiva de cargas de trabalho do CCE com um gateway dedicado

1.1 Introdução

Cenário

Você pode usar o APIG para expor seletivamente suas cargas de trabalho e microsserviços no Cloud Container Engine (CCE).

Exponha as cargas de trabalho do CCE usando um dos métodos a seguir. O **método 1** é recomendado.

- Método 1

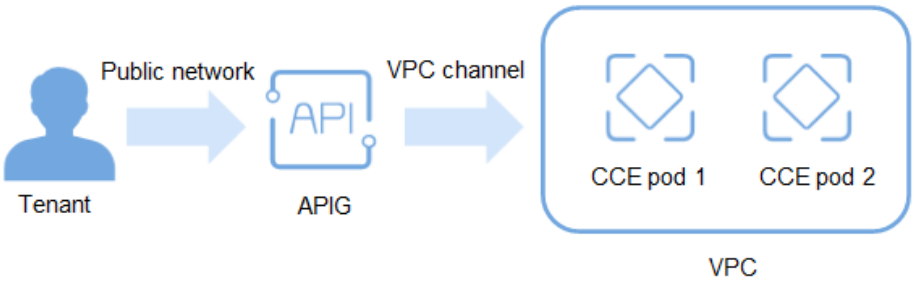
  Crie um canal de balanceamento de carga no APIG para acessar endereços IP de pod em cargas de trabalho do CCE, monitorando dinamicamente as alterações desses endereços. Ao abrir as APIs de uma aplicação em container, especifique um canal de balanceamento de carga para acessar o serviço de back-end.

- Método 2

  Importe uma carga de trabalho do CCE para o APIG. As APIs e um canal de balanceamento de carga são gerados e vinculados entre si para monitorar dinamicamente as alterações de endereço IP do pod. Exponha cargas de trabalho e microsserviços no CCE usando essas APIs.

Arquitetura da solução

Figura 1-1 Acesso a cargas de trabalho do CCE (compostas por pods) por meio do APIG



Vantagens

- Você não precisa definir endereços IP elásticos, reduzindo os custos de largura de banda da rede.

  Os endereços de carga de trabalho no CCE podem ser acessados por meio de um canal de balanceamento de carga que é criado ou gerado manualmente pela importação de uma carga de trabalho.
- Os endereços de pod de carga de trabalho no CCE podem ser monitorados dinamicamente e atualizados automaticamente por um canal de balanceamento de carga que é criado manualmente ou gerado pela importação de uma carga de trabalho.
- As cargas de trabalho do CCE podem ser liberadas por tag para teste e comutação de versão.
- Múltiplos modos de autenticação mantêm o acesso seguro.
- As políticas de limitação de solicitações garantem acesso seguro ao seu serviço de back-end.

  Em vez de acesso direto a aplicações em containers, o APIG fornece limitação de solicitações para garantir que seu serviço de back-end seja executado de forma estável.
- O balanceamento de carga do pod melhora a utilização de recursos e a confiabilidade do sistema.

Restrições

- Somente os clusters do CCE Turbo e os clusters do CCE que usam o modelo de rede da VPC são suportados.
- O cluster do CCE e o gateway devem estar na mesma VPC ou conectados.
- Se você selecionar um cluster do CCE que usa o modelo de rede da VPC, adicione o bloco CIDR do container do cluster na área **Routes** da página de detalhes do gateway.

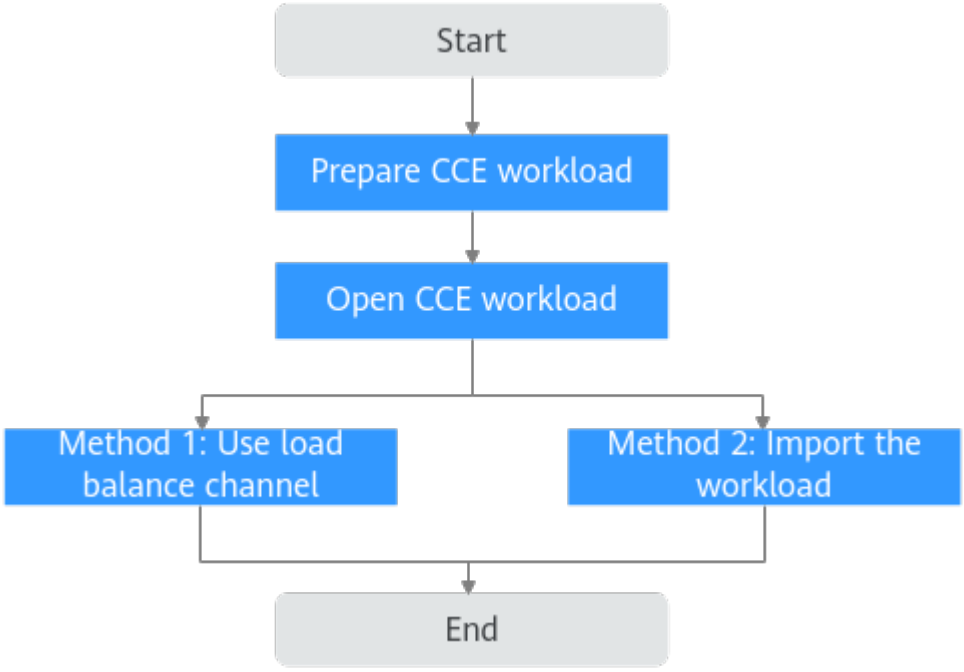
1.2 Planejamento de recursos

Tabela 1-1 Planejamento de recursos e custos

Recurso	Quantidade
CCE	1

Recurso	Quantidade
Gateway dedicado	1

1.3 Procedimento geral



1. **Prepare a carga de trabalho do CCE**

   Antes de abrir uma carga de trabalho de container com APIG, compre um cluster do CCE que use o modelo de rede de VPC ou um cluster Turbo no console do CCE.

2. Abra a carga de trabalho do CCE

   Método 1: crie um canal de balanceamento de carga no APIG para acessar endereços de pod na carga de trabalho do CCE.

   Método 2: importe uma carga de trabalho do CCE para o APIG. APIs e um canal de balanceamento de carga são gerados e vinculados entre si para acessar endereços IP do pod na carga de trabalho.

3. **(Opcional) Configure rótulo da carga de trabalho para lançamento em escala de cinza**

   O lançamento em escala de cinza é uma política de lançamento de serviço que muda gradualmente o tráfego de uma versão anterior para uma versão posterior, especificando o peso da distribuição do tráfego.

1.4 Procedimento de implementação

Preparação de uma carga de trabalho do CCE

Passo 1 Compre um cluster.

1. Faça logon no console do CCE e compre um cluster do CCE (modelo de rede da VPC) ou um cluster Turbo na página **Clusters**. Selecione **CCE Cluster** e defina **Network Model** como **VPC network**. Para obter detalhes, consulte **Compra de um cluster do CCE**.
2. Depois que o cluster é criado, registre o bloco CIDR do container.
3. Adicione este bloco CIDR na área **Routes** de um gateway dedicado.
   a. Faça logon no console do APIG e escolha **Gateways** no painel de navegação.
   b. Clique no nome do gateway para acessar a página de detalhes.
   c. Adicione o bloco CIDR do container na área **Routes**.

Passo 2 Crie uma carga de trabalho.

1. Na página **Clusters** do console do CCE, clique no nome do cluster para acessar a página de detalhes.
2. No painel de navegação, escolha **Workloads**.
3. Clique em **Create Workload**. Defina **Workload Type** como **Deployment**. Para obter detalhes, consulte o **Guia de usuário do CCE**.

   Na área **Advanced Settings** > **Labels and Annotations**, defina rótulos de pod para alternar a carga de trabalho e a versão de serviço. Neste exemplo, defina **app=deployment-demo** e **version=v1**. Se você criar uma carga de trabalho importando um arquivo YAML, adicione rótulos de pod nesse arquivo. Para obter detalhes sobre os rótulos do pod, consulte **Rótulos e anotações de pods**

   Adicione rótulos de pod em um arquivo YAML:

```
spec:
  replicas: 2
  selector:
    matchLabels:
      app: deployment-demo
      version: v1
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: deployment-demo
        version: v1
```

----Fim

Método 1: abrir uma carga de trabalho do CCE criando um canal de balanceamento de carga

Passo 1 Crie um canal de balanceamento de carga.

1. Vá para o console do APIG e escolha **Gateways** no painel de navegação.
2. Escolha **API Management** > **API Policies**.
3. Na guia **Load Balance Channels**, clique em **Create Load Balance Channel**.
   a. Defina as informações básicas.

Tabela 1-2 Parâmetros de informações básicas

Parâmetro	Descrição
Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa. Neste exemplo, insira **VPC_demo**.
Port	Porta de container de uma carga de trabalho para serviços de abertura. Defina esse parâmetro como **80**, que é a porta HTTP padrão.
Routing Algorithm	Selecione **WRR**. Esse algoritmo será usado para encaminhar solicitações para cada um dos servidores de nuvem que você selecionar na ordem de peso do servidor.
Type	Selecione **Microservice**.

b. Configure informações de microsserviços.

Tabela 1-3 Configuração de microsserviços

Parâmetro	Descrição
Microservice Type	O **Cloud Container Engine (CCE)** é sempre selecionado.
Cluster	Selecione o **cluster comprado**.
Namespace	Selecione um namespace no cluster. Neste exemplo, selecione **default**.
Workload Type	Selecione **Deployment**. Este parâmetro deve ser o mesmo que o tipo da carga de trabalho criada.
Service Label Key	Selecione o rótulo do pod **app** e seu valor **deployment-demo** da **carga de trabalho criada**.
Service Label Value	

c. Configure um grupo de servidores.

Tabela 1-4 Configuração do grupo de servidores

Parâmetro	Descrição
Server Group Name	Digite **server_group_v1**.
Weight	Digite **1**.
Backend Service Port	Digite **80**. Isso deve ser o mesmo que a porta do container na carga de trabalho.
Description	Digite "Server group with version v1".

Parâmetro	Descrição
Tag	Selecione o rótulo do pod **version=v1** da **carga de trabalho criada**.

d. Configure verificação de integridade.

Tabela 1-5 Configuração de verificação de integridade

Parâmetro	Descrição
Protocol	Padrão: **TCP**.
Check Port	Porta do servidor back-end no canal.
Healthy threshold	Padrão: **2**. Este é o número de verificações consecutivas bem-sucedidas necessárias para que um servidor em nuvem seja considerado íntegro.
Unhealthy Threshold	Padrão: **5**. Esse é o número de verificações consecutivas com falha necessárias para que um servidor em nuvem seja considerado não íntegro.
Timeout (s)	Padrão: **5**. Este é o tempo limite usado para determinar se uma verificação de integridade falhou.
Interval (s)	Padrão: **10**. Este é o intervalo entre verificações consecutivas.

e. Clique em **Finish**.

Na lista de canais de balanceamento de carga, clique em um nome de canal para exibir os detalhes.

Passo 2 Abra uma API.

1. Crie um grupo de APIs.
   a. Escolha **API Management** > **API Groups**.
   b. Clique em **Create API Group** e escolha **Create Directly**.
   c. Configure as informações do grupo e clique em **OK**.
2. Crie uma API e vincule o canal de balanceamento de carga anterior a ela.
   a. Clique no nome do grupo para acessar a página de detalhes. Na guia **APIs**, clique em **Create**.
   b. Configure as informações de front-end e clique em **Next**.

Tabela 1-6 Configuração de front-end

Parâmetro	Descrição
API Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.

Parâmetro	Descrição
Group	Selecione o **grupo de APIs anterior**.
URL	**Method**: método de solicitação da API. Defina este parâmetro como **ANY**. **Protocol**: protocolo de solicitação da API. Defina este parâmetro como **HTTPS**. **Subdomain Name**: o sistema aloca automaticamente um nome de subdomínio para cada grupo de APIs para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia. **Path**: caminho para solicitar a API.
Gateway Response	Selecione uma resposta a ser exibida se o gateway falhar ao processar uma solicitação de API. Padrão: **default**.
Matching	Selecione **Prefix match**.
Authentication Mode	Modo de autenticação da API. Selecione **None**. (**None**: não recomendado para serviços reais. Todos os usuários terão acesso à API.)

c. Configure as informações de back-end e clique em **Next**.

Tabela 1-7 Parâmetros para definir um serviço de back-end HTTP/HTTPS

Parâmetro	Descrição
Load Balance Channel	Determine se o serviço de back-end será acessado usando um canal de balanceamento de carga. Para este exemplo, selecione **Configure**.
URL	**Method**: método de solicitação da API. Defina este parâmetro como **ANY**. **Protocol**: defina este parâmetro como **HTTP**. **Load Balance Channel**: selecione o **canal criado**. **Path**: caminho do serviço de back-end.

d. Defina a resposta e clique em **Finish**.

3. Depure a API.

   Na guia **APIs**, clique em **Debug**. Clique no botão **Debug** no fundo vermelho. Se o código de status **200** for retornado no resultado da resposta, a depuração será bem-sucedida. Em seguida, vá para a próxima etapa. Caso contrário, corrija o erro indicado na mensagem de erro.

4. Publique a API.

   Na guia **APIs**, clique em **Publish**, mantenha a opção padrão **RELEASE** e clique em **OK**. Quando o ponto de exclamação no canto superior esquerdo do botão **Publish**

desaparecer, a publicação foi bem-sucedida. Em seguida, vá para a próxima etapa. Caso contrário, corrija o erro indicado na mensagem de erro.

Passo 3 Chame a API.

1. Vincule nomes de domínio independentes ao grupo desta API.

   Na página de detalhes do grupo, clique na guia **Group Information**. O nome de domínio de depuração é usado apenas para desenvolvimento e teste e pode ser acessado 1000 vezes por dia. Vincule nomes de domínio independentes para expor APIs no grupo.

   Clique em **Bind Independent Domain Name** para vincular nomes de domínio públicos registrados. Para obter detalhes, consulte **Vinculação de um nome de domínio**.

2. Copie o URL da API.

   Na guia **APIs**, copie o URL da API. Abra um navegador e insira o URL. Quando a resposta de sucesso definida é exibida, a invocação é bem-sucedida.

   Figura 1-2 Cópia do URL

   Agora, a carga de trabalho do CCE é aberta criando um canal de balanceamento de carga.

----Fim

Método 2: abrir uma carga de trabalho do CCE importando-a

Passo 1 Importe uma carga de trabalho do CCE.

1. Vá para o console do APIG e escolha **Gateways** no painel de navegação.
2. Escolha **API Management** > **API Groups**.
3. Escolha **Create API Group** > **Import CCE Workload**.
   a. Especifique informações sobre a carga de trabalho do CCE a ser importada.

   Tabela 1-8 Informações sobre a carga de trabalho

Parâmetro	Descrição
Group	Padrão: **New group**.
Cluster	Selecione o **cluster comprado**.
Namespace	Selecione um namespace no cluster. Neste exemplo, selecione **default**.
Workload Type	Selecione **Deployment**. Este parâmetro deve ser o mesmo que o tipo da carga de trabalho criada.

Parâmetro	Descrição
Service Label Key	Selecione o rótulo do pod **app** e seu valor **deployment-demo** da **carga de trabalho criada**.
Service Label Value	
Tag	Outro rótulo de pod **version=v1** da carga de trabalho é selecionado automaticamente.

b. Configure informações da API.

Tabela 1-9 Informações da API

Parâmetro	Descrição
Protocol	Protocolo de solicitação da API. **HTTPS** é selecionado por padrão.
Request Path	Caminho de solicitação da API para correspondência de prefixo. Padrão: /. Neste exemplo, retenha o valor padrão.
Port	Digite **80**. Isso deve ser o mesmo que a porta do container na carga de trabalho.
Authentication Mode	Padrão: **None**.
CORS	Desativado por padrão.
Timeout (ms)	Tempo limite de back-end. Padrão: **5000**.

4. Clique em **OK**. A carga de trabalho do CCE é importada, com um grupo de APIs, uma API e um canal de balanceamento de carga gerados.

Passo 2 Veja a API gerada e o canal de balanceamento de carga.

1. Veja a API gerada.
   a. Clique no **nome do grupo de APIs** e, em seguida, veja o nome da API, o método de solicitação e o status de publicação na guia **APIs**.
   b. Clique na guia **Backend Configuration** e veja o canal de balanceamento de carga vinculado.
2. Veja o canal de balanceamento de carga gerado.
   a. Escolha **API Management** > **API Policies**.
   b. Na guia **Load Balance Channels**, clique no nome do canal para exibir os detalhes.
3. Verifique se esse canal de balanceamento de carga é o vinculado à API e, em seguida, vá para a próxima etapa. Se não estiver, repita **Passo 1**.

Passo 3 Abra a API.

Como a importação de uma carga de trabalho do CCE já cria um grupo de APIs e uma API, você só precisa publicar a API em um ambiente.

1. Depure a API.

Na guia **APIs**, clique em **Debug**. Clique no botão **Debug** no fundo vermelho. Se o código de status **200** for retornado no resultado da resposta, a depuração será bem-sucedida. Em seguida, vá para a próxima etapa.

2. Publique a API.

   Na guia **APIs**, clique em **Publish**, mantenha a opção padrão **RELEASE** e clique em **OK**. Quando o ponto de exclamação no canto superior esquerdo do botão **Publish** desaparecer, a publicação foi bem-sucedida. Em seguida, vá para a próxima etapa.

Passo 4 Chame a API.

1. Vincule nomes de domínio independentes ao grupo desta API.

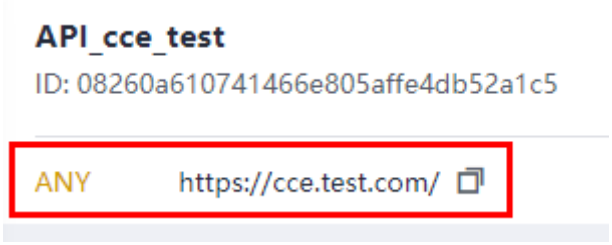
   Na página de detalhes do grupo, clique na guia **Group Information**. O nome de domínio de depuração é usado apenas para desenvolvimento e teste e pode ser acessado 1000 vezes por dia. Vincule nomes de domínio independentes para expor APIs no grupo.

   Clique em **Bind Independent Domain Name** para vincular nomes de domínio públicos registrados. Para obter detalhes, consulte **Vinculação de um nome de domínio**.

2. Copie o URL da API.

   Na guia **APIs**, copie o URL da API. Abra um navegador e insira o URL. Quando a resposta de sucesso definida é exibida, a invocação é bem-sucedida.

   Figura 1-3 Cópia do URL

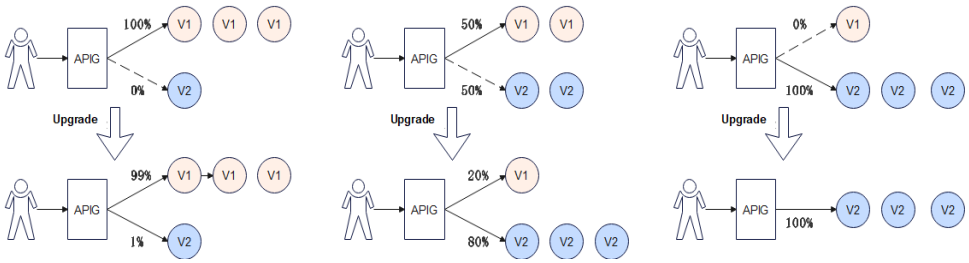
   Agora, a carga de trabalho do CCE foi aberta importando-a.

----Fim

(Opcional) Configuração de rótulos de carga de trabalho para lançamento em escala de cinza

O lançamento em escala de cinza é uma política de lançamento de serviço que muda gradualmente o tráfego de uma versão anterior para uma versão posterior, especificando o peso da distribuição do tráfego. Os serviços são verificados durante o lançamento e a atualização. Se uma versão posterior atender à expectativa, você poderá aumentar a porcentagem de tráfego dessa versão e diminuir a da versão anterior. Repita esse processo até que uma versão posterior represente 100% e uma versão anterior seja reduzida a 0. Em seguida, o tráfego é alternado com sucesso para a versão posterior.

Figura 1-4 Princípio de lançamento em escala de cinza



As cargas de trabalho do CCE são configuradas usando o seletor de rótulo do pod para o lançamento em escala de cinza. Você pode implementar e verificar rapidamente novos recursos e alternar servidores para processamento de tráfego. Para obter detalhes, consulte **Uso de serviços para implementar o lançamento simples em escala de cinza e a implementação azul-verde**.

O seguinte descreve como alternar suavemente o tráfego de V1 para V2 por meio do lançamento em escala de cinza.

Passo 1 Crie uma carga de trabalho, defina um rótulo de pod com o mesmo valor que o rótulo **app** da carga de trabalho anterior. Para obter detalhes, consulte a **carga de trabalho anterior**.

Na página de criação da carga de trabalho, vá para a área **Advanced Settings** > **Labels and Annotations** e defina **app=deployment-demo** e **version=v2**. Se você criar uma carga de trabalho importando um arquivo YAML, adicione rótulos de pod nesse arquivo.

Passo 2 Para o grupo de servidores com rótulo de pod **version=v1**, ajuste o peso do tráfego.

1. No console do APIG, escolha **Gateways** no painel de navegação.
2. Escolha **API Management** > **API Policies**.
3. Na guia **Load Balance Channels**, clique no nome do **canal criado**.
4. Na área **Backend Server Address**, clique em **Modify**.
5. Altere o peso para **100** e clique em **OK**.

   Peso é a porcentagem de tráfego a ser encaminhado. Todo o tráfego será encaminhado para os endereços IP do pod no grupo de servidores **server_group_v1**.

Passo 3 Crie um grupo de servidores com o rótulo do pod **version=v2** e, em seguida, defina o peso do tráfego.

1. Na área **Backend Server Address**, clique em **Create Server Group**.

   Tabela 1-10 Configuração do grupo de servidores

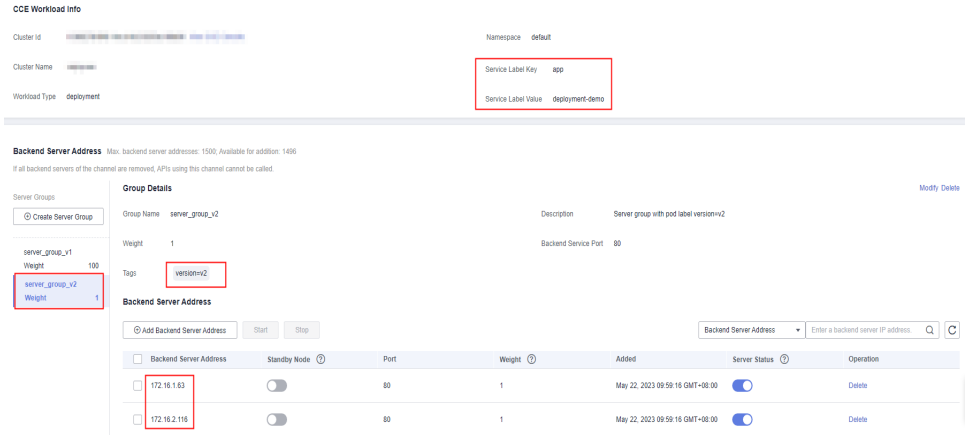
Parâmetro	Descrição
Server Group Name	Digite **server_group_v2**.
Weight	Digite **1**.
Backend Service Port	Digite **80**.
Tag	Selecione o rótulo do pod **version=v2**.

2. Clique em **OK**.

Passo 4 Atualize os endereços do servidor back-end.

Atualize a página para os endereços de servidor back-end. O canal de balanceamento de carga monitora automaticamente os endereços IP do pod da carga de trabalho e adiciona dinamicamente os endereços como endereços de servidor back-end. Conforme mostrado na figura a seguir, as tags **app=deployment-demo** e **version=v2** correspondem automaticamente aos endereços IP do pod (endereços de servidor back-end) da **carga de trabalho**.

Figura 1-5 Endereços IP do pod correspondidos automaticamente



100 de 101 (peso do grupo de servidores do peso total) tráfego é distribuído para **server_group_v1** e o restante para a versão posterior de **server_group_v2**.

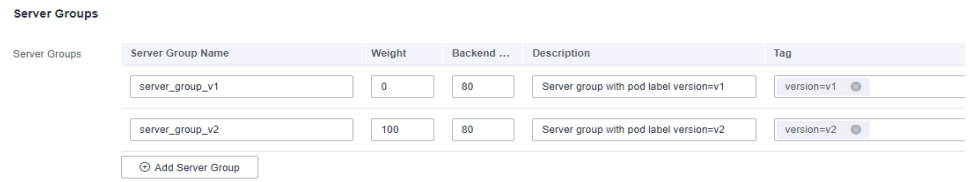
Figura 1-6 Clique em **Modify** no canto superior direito da página.

Passo 5 Verifique se os novos recursos lançados em V2 por meio da versão em escala de cinza estão funcionando de forma estável.

Se a nova versão atender à expectativa, vá para **Passo 6**. Caso contrário, o lançamento do novo recurso falhará.

Passo 6 Ajuste os pesos dos grupos de servidores para diferentes versões.

Diminua gradualmente o peso do **server_group_v1** e aumente o do **server_group_v2**. Repita de **Passo 5** a **Passo 6** até que o peso do **server_group_v1** seja **0** e o do **server_group_v2** chegue a **100**.



Como mostrado na figura anterior, todas as solicitações são encaminhadas para **server_group_v2**. Novos recursos são alterados de **deployment-demo** da carga de trabalho

de **version=v1** para **deployment-demo2** de **version=v2** por meio do lançamento em escala de cinza. (Você pode ajustar o peso do tráfego para atender aos requisitos de serviço.)

Passo 7 Exclua o grupo de servidores back-end **server_group_v1** de **version=v1**.

Agora todo o tráfego foi alterado para o grupo de servidores back-end de **version=v2**. Você pode excluir o grupo de servidores de **version=v1**.

1. Vá para a página de detalhes do canal de balanceamento de carga no console do APIG, exclua todos os endereços IP do grupo de servidores de **version=v1** na área **Backend Server Address**.
2. Clique em **Delete** à direita desta área para excluir o grupo de servidores de **version=v1**.

   O grupo de servidores back-end **server_group_v2** de **version=v2** é mantido.

----Fim

2 Exposição seletiva dos recursos de serviço de um data center usando um gateway dedicado

Os serviços de back-end do APIG podem ser implementados nos seguintes modos:

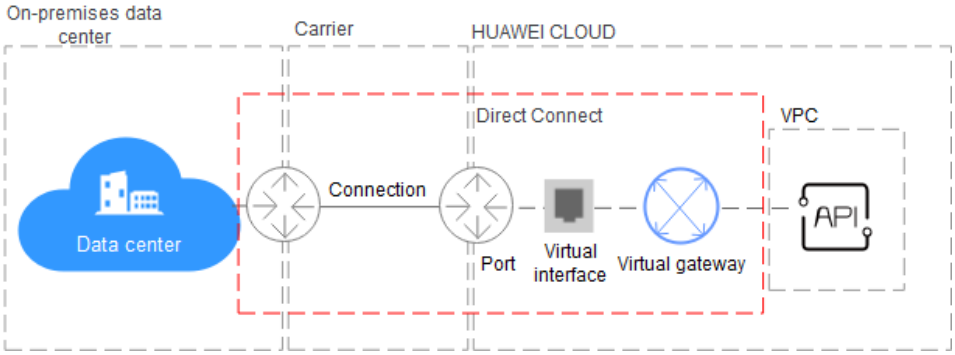
- Implementados em uma VPC e acessíveis somente por meio de endereços IP privados.

  Você pode criar um canal da VPC no APIG para ativar o roteamento de rede entre o APIG e a VPC.
- Implementados na rede pública e acessíveis usando um endereço IP público.
- Implementados em um data center local e não acessíveis usando um endereço IP público.

  Se você usa um gateway de API dedicado, pode configurar uma conexão entre o seu data center local e o gateway (ou a VPC vinculada ao gateway).

Esta seção descreve as precauções para usar APIG para expor seletivamente APIs de serviços de back-end implementados em um data center local.

Figura 2-1 Conexão de um data center a um gateway de API dedicado com Direct Connect



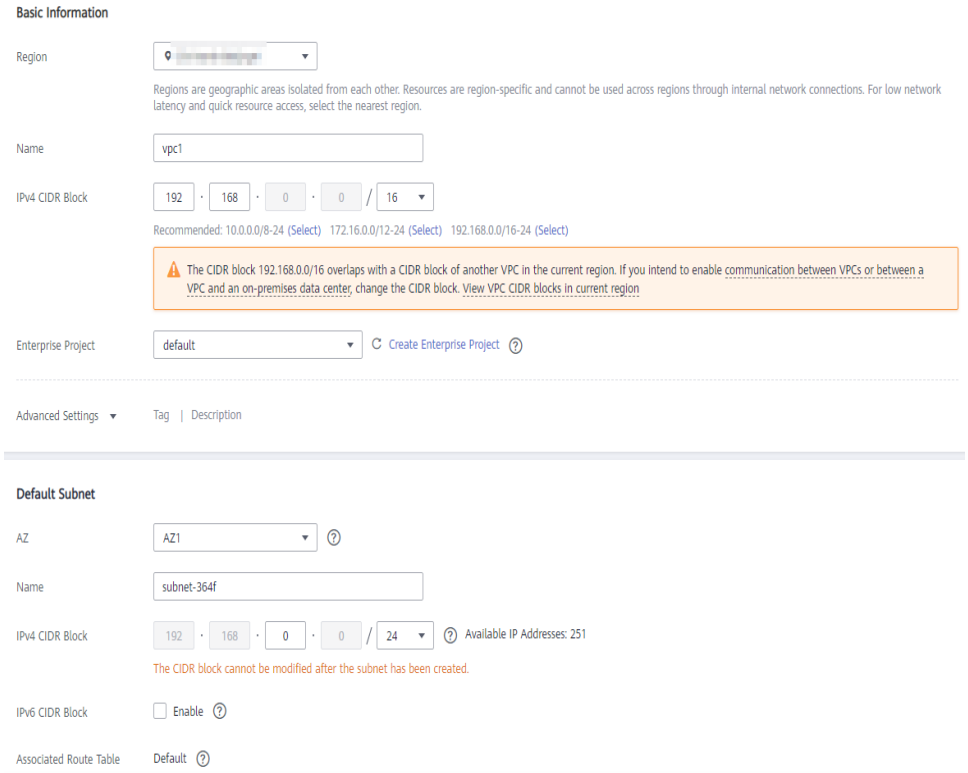
Conexão de um data center ao APIG

Passo 1 Crie uma VPC.

Para obter detalhes, consulte o **Guia de usuário da Virtual Private Cloud**.

Para permitir que o APIG acesse serviços no seu data center local, vincule uma VPC ao seu gateway dedicado e estabeleça uma conexão entre o data center e a VPC.

Figura 2-2 Criação de uma VPC



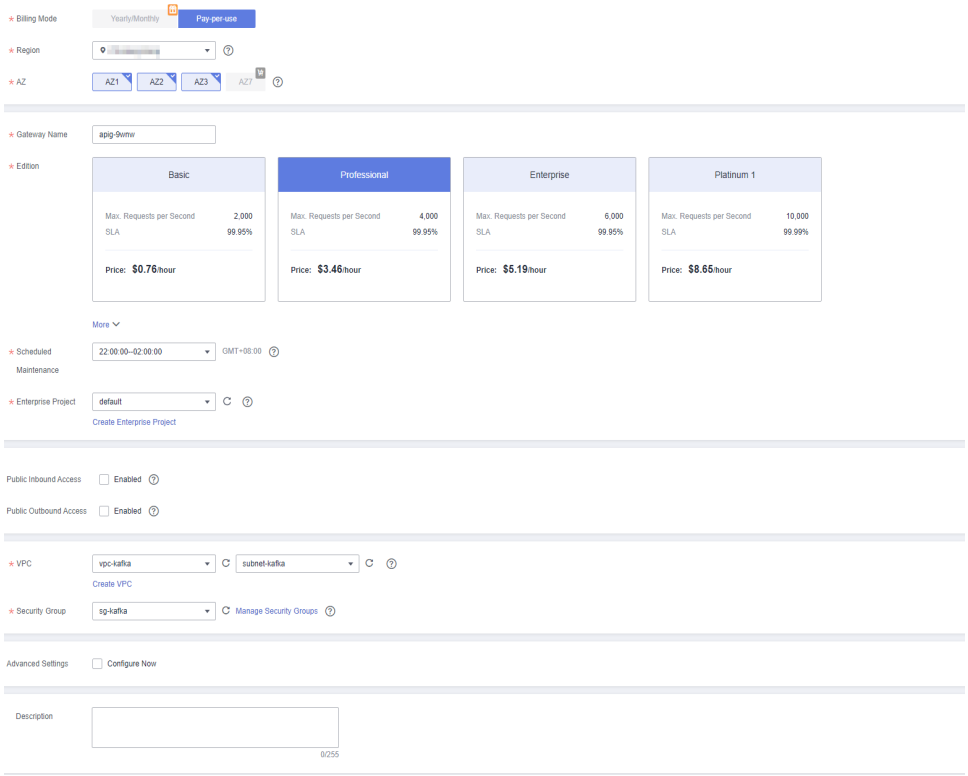
NOTA

- Especifique uma sub-rede para o seu gateway dedicado.
- Uma conexão pode ser usada para conectar um data center local a apenas uma VPC. É recomendável vincular a mesma VPC a todos os seus recursos de nuvem para reduzir os custos.
- Se uma VPC já existir, não será necessário criar uma nova.

Passo 2 Compre um gateway de API dedicado.

Para obter detalhes, consulte **Compra de um gateway dedicado**.

Figura 2-3 Compra de um gateway dedicado



Passo 3 Compre uma conexão.

Para comprar uma conexão para conectar o data center ao APIG (VPC vinculada), faça o seguinte:

1. **Crie uma conexão**

   Compre uma conexão para estabelecer conectividade entre seu data center local e a Huawei Cloud. Você é aconselhado a escolher **Full Service Installation**, o que significa que a Huawei Cloud concluirá a construção.

   Se você já tiver uma conexão entre seu data center e a Huawei Cloud, use a conexão em vez disso.

2. **Crie um gateway virtual**

   O gateway virtual é um gateway lógico para acessar a VPC vinculada ao gateway dedicado.

   > NOTA
   >
   > Selecione a sub-rede que o gateway dedicado usa para se conectar à VPC. Para obter detalhes sobre a sub-rede, vá para a página de detalhes do gateway.

3. **Crie uma interface virtual**

   A interface virtual vincula a conexão com o gateway virtual, permitindo a conectividade entre a conexão e a VPC do gateway dedicado.

   Configure o gateway remoto e a sub-rede remota como gateway e sub-rede para acessar a API aberta do seu data center local. Por exemplo, se o endereço de chamada da API do seu data center for **http://192.168.0.25:80/***{URI}*, configure o gateway remoto e a sub-rede remota como **192.168.0.25**.

4. **Configure rotas**

Configure rotas em suas instalações se a sub-rede do seu 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.

Passo 4 Verifique a conectividade de rede.

Crie outro ECS de pagamento por uso e selecione a mesma VPC, sub-rede e grupo de segurança que o gateway dedicado. Se o data center puder se conectar ao ECS, o data center também poderá se conectar ao gateway dedicado.

----Fim

Exposição de APIs com o gateway dedicado

Depois de conectar o data center ao gateway dedicado, você pode expor APIs usando o gateway. Para obter detalhes, consulte **Primeiros passos** in the *API Gateway User Guide*.

Ao criar uma API, especifique o endereço de back-end como o endereço de chamada da API do seu data center.

3 Desenvolvimento de um autorizador personalizado com FunctionGraph

Visão geral

As melhores práticas para o APIG da Huawei Cloud orientam você pelo desenvolvimento de autorizadores personalizados.

Além do IAM e da autenticação de aplicações, o APIG também suporta autenticação personalizada com seu próprio sistema de autenticação, que pode se adaptar melhor aos recursos de sua empresa.

A autenticação personalizada é implementada usando o serviço FunctionGraph. Você pode criar uma função de FunctionGraph para que o APIG possa invocá-la para autenticar solicitações para sua API. Esta seção usa a autenticação básica como um exemplo para descrever como implementar a autenticação personalizada com o FunctionGraph.

Desenvolvimento de uma função de autenticação personalizada

Crie uma função no console do FunctionGraph consultando **Criação de uma função para autenticação personalizada de front-end**.

Especifique o tempo de execução como Python 3.6.

Tabela 3-1 Configuração da função

Parâmetro	Descrição
Function Type	Padrão: **Event Function**
Region	Selecione a mesma região que a do APIG.
Function Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Agency	Uma agência que delega FunctionGraph para acessar outros serviços em nuvem. Para este exemplo, selecione **Use no agency**.
Enterprise Project	A opção padrão é **default**.

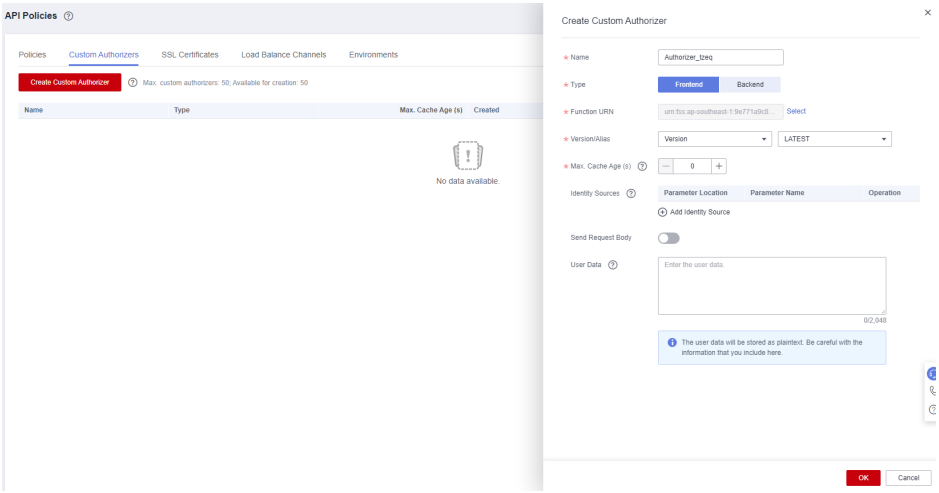
Parâmetro	Descrição
Runtime	Selecione **Python 3.6**.

Na página de guia **Code**, copie o seguinte código para **index.py** (se você estiver usando um gateway dedicado, para o qual o parâmetro **authorizer_context_support_num_bool** foi ativado, o tipo de **value** no **context** pode ser boolean ou number).

```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
# If the authentication information is correct, the username is returned.
    if event["headers"]["authorization"]=='Basic dXN****cmQ=':
        return {
            'statusCode': 200,
            'body': json.dumps({
                "status":"allow",
                "context":{
                    "user_name":"user1"
                }
            })
        }
    else:
        return {
            'statusCode': 200,
            'body': json.dumps({
                "status":"deny",
                "context":{
                    "code": "1001",
                    "message":"incorrect username or password",
                    "authorizer_success": "false"
                }
            })
        }
```

Criação de um autorizador personalizado

No console do APIG, acesse a página **Create Custom Authorizer**, defina **Type** como **Frontend**, selecione a função criada na seção anterior e clique em **OK**.



Criação de uma API de autenticação personalizada

Crie uma API consultando **Criação de uma API**. Defina o modo de autenticação como **Custom** e selecione o autorizador personalizado criado na seção anterior. Depois de modificar a API, publique-a.

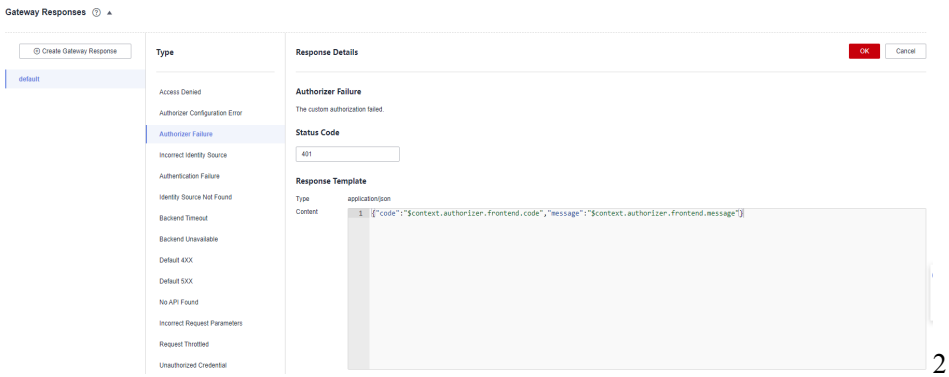
Configuração da resposta a erros

Se informações de autenticação incorretas forem transportadas em uma solicitação para a API, a resposta será exibida da seguinte forma:

```
{"error_msg":"Incorrect authentication information: frontend
authorizer","error_code":"APIG.0305","request_id":"36e42b3019077c2b720b6fc847733ce
9"}
```

Para retornar o campo no **context** da função como a resposta da API (se você estiver usando um gateway dedicado, para o qual o parâmetro **authorizer_context_support_num_bool** foi ativado, o tipo de **value** em **context** pode ser boolean ou number), modifique o modelo de resposta do gateway. Na página de detalhes do grupo ao qual a API pertence, navegue até a área **Gateway Responses** na guia **Gateway Information** e clique em **Edit**. Altere o código de status para **401**, modifique o modelo de resposta com o seguinte código e clique em **OK** (não é necessário adicionar aspas duplas para variáveis do tipo boolean ou number):

```
{"code":"$context.authorizer.frontend.code","message":"$context.authorizer.fronten
d.message", "authorizer_success":
"$context.authorizer.frontend.authorizer_success"}
```



2

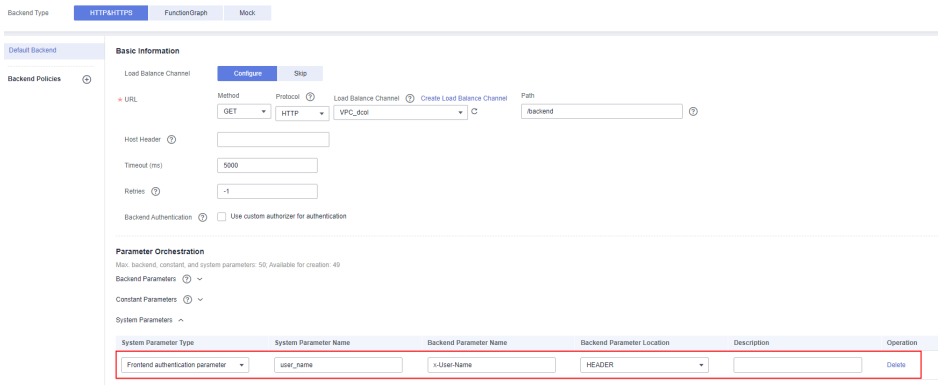
Após a modificação, se a autenticação incorreta for transferida ao chamar a API, o código de status **401** será retornado e o resultado da resposta será o seguinte:

```
 {"code":"1001","message":"incorrect username or password","authorizer_success":
"false"}
```

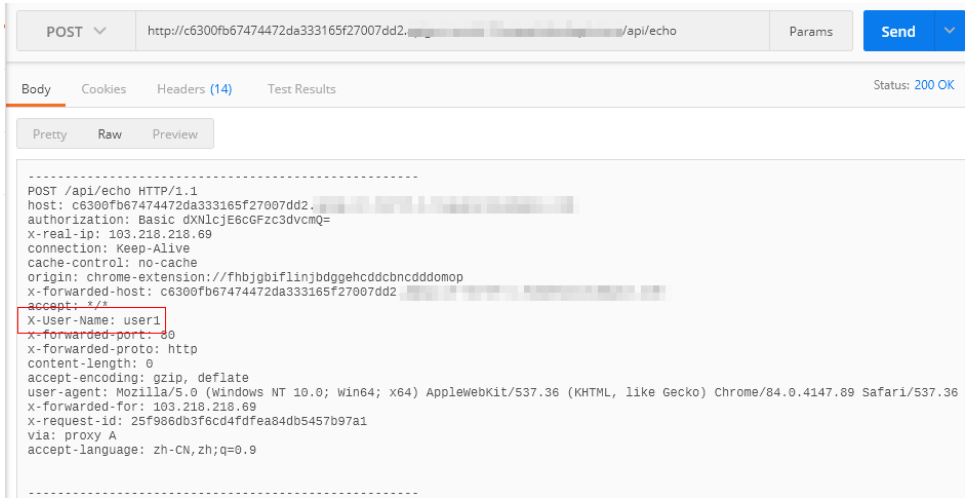
Mapeamento de parâmetros de autenticação de front-end para parâmetros de back-end

Se a autenticação for bem-sucedida, as informações de contexto retornadas pela função podem ser transferidas para o back-end da API. Para fazer isso, execute as seguintes configurações:

Na página **APIs**, escolha **More** > **Edit** na linha que contém a API e vá para a página **Define Backend Request**. Adicione um parâmetro do sistema, especifique o tipo de parâmetro como **Frontend authentication parameter**, defina o nome do parâmetro para o conteúdo do campo **context** na resposta da função e defina o nome e a localização do parâmetro de back-end para o qual você deseja mapear o parâmetro de autenticação do front-end.



Depois de modificar a API, publique-a novamente. Se as informações de autenticação transportadas em uma solicitação para a API estiverem corretas, o resultado da resposta conterá o campo de cabeçalho **X-User-Name** cujo valor é o mesmo do **user_name** no campo **context** da função de autenticação.



4 Exposição de serviços de back-end entre VPCs usando um gateway dedicado

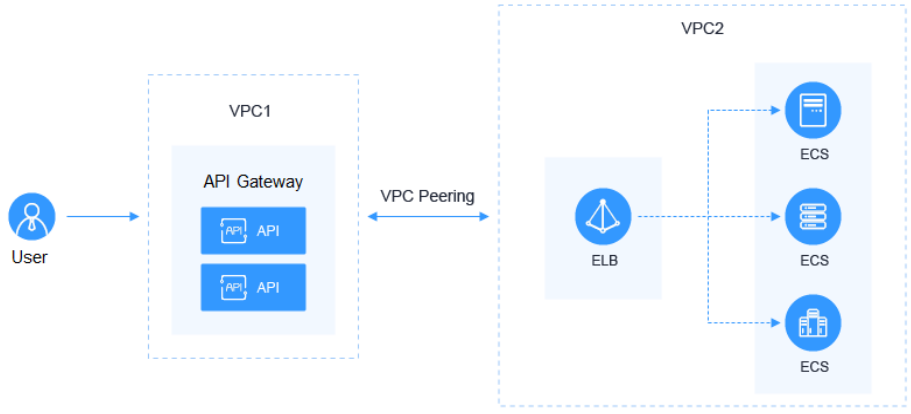
4.1 Introdução

Cenário

Se a VPC do seu servidor back-end for diferente da do seu gateway, como você configura a interconexão entre VPCs? Esta seção usa o Elastic Load Balance (ELB) como um exemplo para descrever como expor serviços em um balanceador de carga de rede privada usando o APIG.

Arquitetura da solução

Figura 4-1 Exposição de serviços de back-end em VPCs



Vantagens

Sem modificar a arquitetura de rede existente, você pode ter todas as solicitações diretamente encaminhadas para o servidor back-end por meio de uma configuração flexível.

Restrições

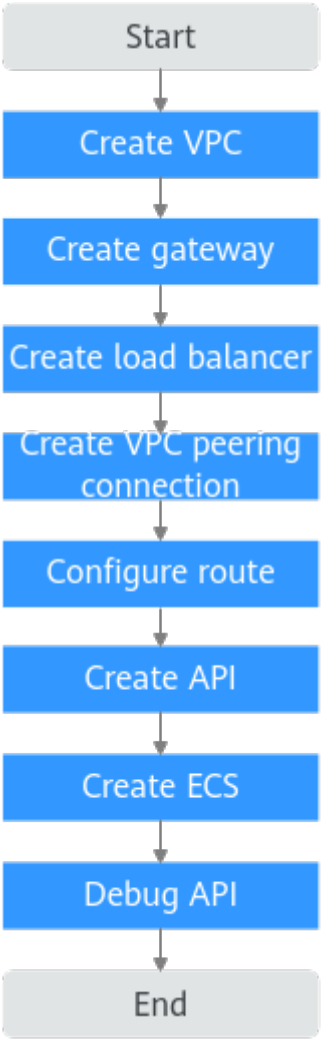
A VPC 1, a VPC 2 e o bloco CIDR da VPC do gateway não podem se sobrepor. Para obter detalhes sobre o planejamento de blocos CIDR da VPC do gateway, consulte **Tabela 4-3**.

4.2 Planejamento de recursos

Tabela 4-1 Planejamento de recursos

Recurso	Quantidade
VPC	2
Gateway dedicado	1
Balanceador de carga	1
ECS	1

4.3 Procedimento geral



1. **Crie uma VPC.**

   Crie duas VPCs, uma para seu gateway e outra para seu serviço de back-end.
2. **Crie um gateway.**

   Crie um gateway dedicado na VPC 1.
3. **Crie um balanceador de carga.**

   Crie um balanceador de carga na VPC 2.
4. **Crie uma conexão de emparelhamento de VPC.**

   Crie uma conexão de emparelhamento de VPC para conectar a VPC 1 e a VPC 2.
5. **Configure uma rota.**

   Configure uma rota para o gateway dedicado definindo o endereço IP como o bloco CIDR IPv4 da VPC 2 em que o balanceador de carga comprado está localizado.
6. **Crie uma API**.

   Crie uma API e defina o endereço de serviço de back-end como o endereço IP do balanceador de carga.

7. **Crie um ECS**.

   Crie um ECS na VPC 2 e implemente o serviço de back-end no ECS.

8. **Depure a API.**

   Verifique se a conexão com o balanceador de carga de rede privada foi bem-sucedida.

4.4 Procedimento de implementação

Criação de uma VPC

Passo 1 Faça logon no console da rede.

Passo 2 No painel de navegação, escolha **Virtual Private Cloud** > **My VPCs**.

Passo 3 Na página **Virtual Private Cloud**, clique em **Create VPC** e configure os parâmetros consultando **Tabela 4-2** e **Tabela 4-3**. Para obter detalhes, consulte as seções "Criação de uma VPC" e "Criação de uma sub-rede para a VPC" no *Guia de usuário do Virtual Private Cloud*.

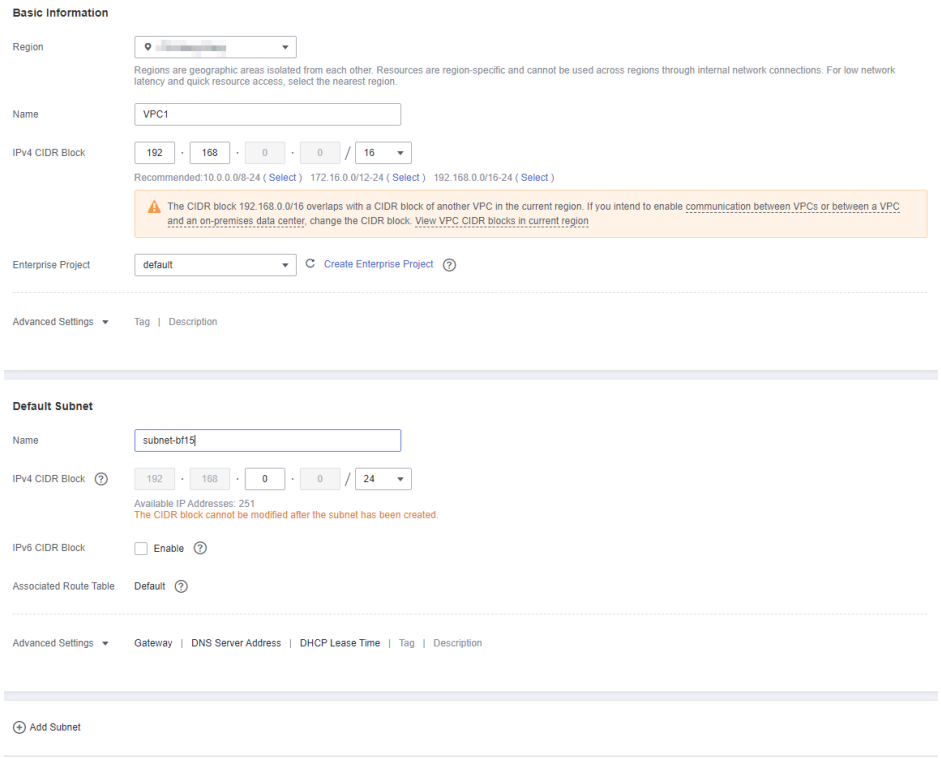


Tabela 4-2 Informações de configuração

Parâmetro	Descrição
Region	Selecione uma região.
Name	Insira **VPC1**. Essa VPC será usada para executar um gateway.
Enterprise Project	Selecione **default**.

Parâmetro	Descrição
Name	Uma sub-rede é criada automaticamente quando você cria uma VPC.

Tabela 4-3 Planejamento de bloco CIDR da VPC

VPC 1	VPC do APIG	VPC 2
10.X	172.31.0.0/16	Deve ser diferente da VPC 1 e da VPC do gateway.
172.X	192.168.0.0/16	
192.X	172.31.0.0/16	

Passo 4 Clique em **Create Now**.

Passo 5 Repita **Passo 3** a **Passo 4** para criar **VPC2** para executar seu serviço de back-end.

----Fim

Criação de um gateway

Passo 1 Vá para o console do APIG.

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

Passo 3 Clique em **Buy Gateway**.

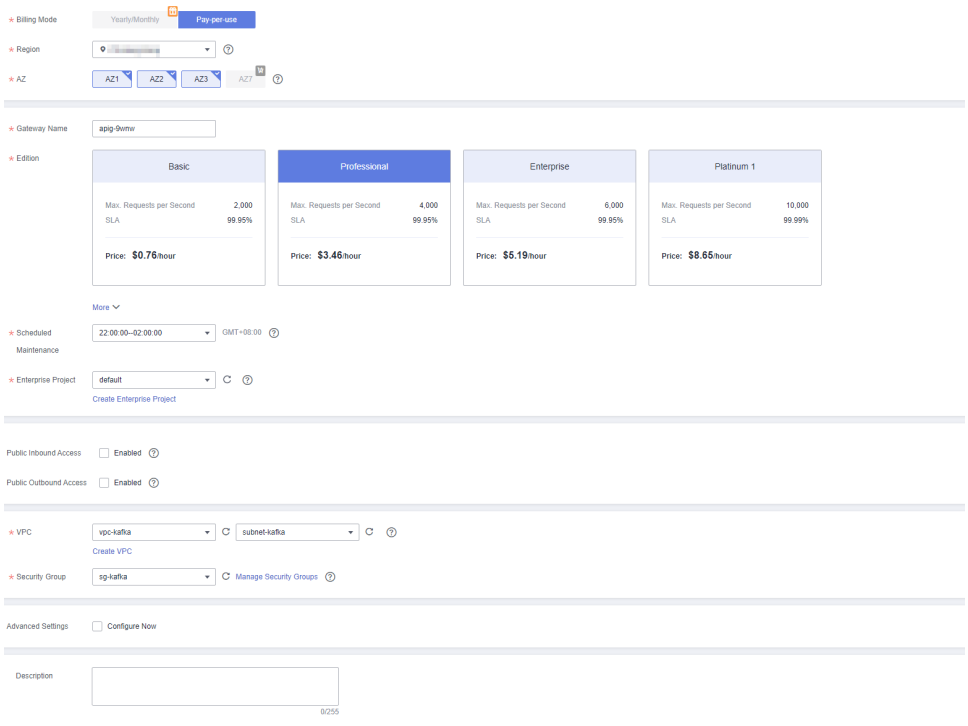


Tabela 4-4 Informações do gateway

Parâmetro	Descrição
Billing Mode	Modo de cobrança do gateway. Selecione **Pay-per-use**.
Region	Selecione a região onde o gateway está localizado. Deve ser a mesma que a região da VPC 1.
AZ	A AZ onde o gateway está localizado. Selecione **AZ1**.
Gateway Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Edition	Selecione **Professional**. A edição não pode ser alterada após a criação do gateway.
Scheduled Maintenance	Selecione um período de tempo em que o gateway pode ser mantido por engenheiros de suporte técnico. Recomenda-se um período com baixo tráfego de serviços. Neste exemplo, mantenha o valor padrão **22:00:00---02:00:00**.
Enterprise Project	Selecione o projeto empresarial ao qual o gateway pertence. Para este exemplo, mantenha o valor padrão **default**.
Network	Selecione **VPC 1** e uma sub-rede.
Security Group	Clique em **Manage Security Groups** e crie um grupo de segurança. Certifique-se de que você selecionou **default** para **Enterprise Project**.
Description	Descrição do gateway.

Passo 4 Clique em **Next**.

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

----Fim

Compra de um balanceador de carga

Passo 1 Retorne ao console da rede.

Passo 2 No painel de navegação, escolha **Elastic Load Balance** > **Load Balancers**.

Passo 3 Clique em **Buy Elastic Load Balancer**.

Passo 4 Configure as informações do balanceador de carga. Para obter detalhes, consulte a seção **Load Balancer** no *Guia de usuário do Elastic Load Balance*.

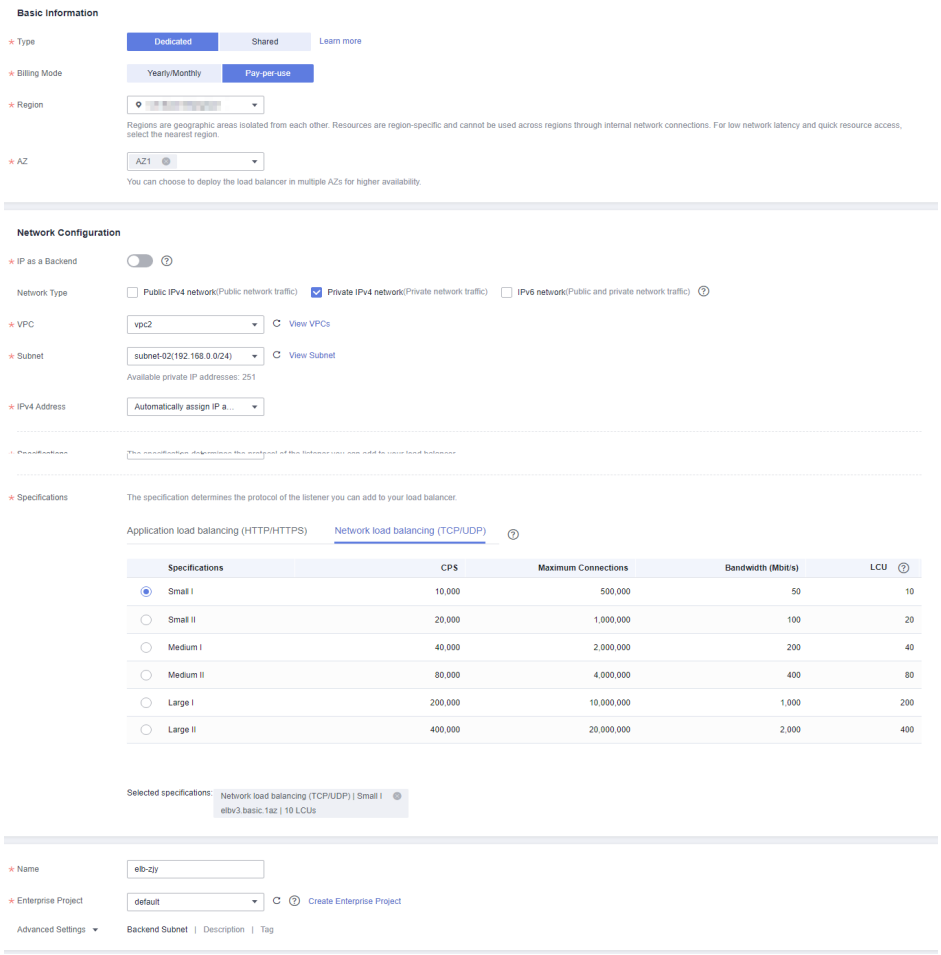


Tabela 4-5 Parâmetros do balanceador de carga

Parâmetro	Descrição
Type	Tipo do balanceador de carga.
Billing Mode	Por padrão, **Pay-per-use** é selecionado.
Region	Selecione a região onde o balanceador de carga está localizado. Deve ser a mesma que a região da VPC 2.
AZ	A AZ onde o balanceador de carga está localizado. Selecione **AZ1**.
Network Type	Selecione **Private Network**.
VPC	Selecione **VPC 2**.
Subnet	Selecione uma sub-rede.
Specification	Selecione **Network load balancing**.
Name	Insira um nome de balanceador de carga que esteja em conformidade com regras específicas para facilitar a pesquisa.
Enterprise Project	Selecione **default**.

Passo 5 Clique em **Next**.

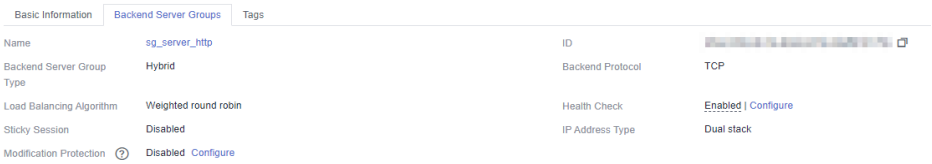
Passo 6 Confirme a configuração e clique em **Submit**.

Passo 7 Adicione um ouvinte.

1. Clique no nome do balanceador de carga. Na página de guia **Listeners**, clique em **Add Listener**.
2. Configure o nome do ouvinte, o protocolo de front-end e a porta e clique em **Next**.
3. Configure o nome do grupo de servidores back-end, o protocolo de back-end e o algoritmo de balanceamento de carga. Em seguida, clique em **Next**.
4. Adicione servidores back-end e clique em **Next**.
5. Clique em **Submit**. A figura a seguir mostra a configuração.

Figura 4-2 Informações do ouvinte

Figura 4-3 Informações do grupo do servidor back-end



----Fim

Criação de uma conexão de emparelhamento de VPC

Passo 1 No painel de navegação, escolha **Virtual Private Cloud** > **VPC Peering Connections**.

Passo 2 Clique em **Create VPC Peering Connection** e configure os parâmetros.

Tabela 4-6 Configuração de uma conexão de emparelhamento de VPC

Parâmetro	Descrição
Name	Insira um nome de conexão de emparelhamento de VPC que esteja em conformidade com regras específicas para facilitar a pesquisa.
Local VPC	Selecione **VPC 1**.
Account	Por padrão, **My account** está selecionada.
Peer Project	Selecione um projeto

Parâmetro	Descrição
Peer VPC	Selecione **VPC 2**.

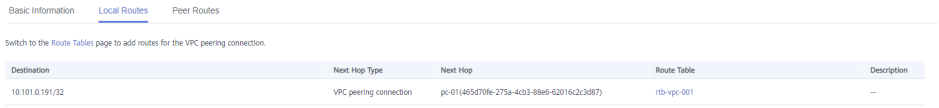
Passo 3 Clique em **OK**.

Passo 4 Na caixa de diálogo exibida, clique em **Add Route** para acessar a página de detalhes da conexão de emparelhamento da VPC.

Passo 5 Na página de guia **Local Routes**, clique em **Route Tables**.

1. Em **Routes**, clique em **Add Route**.
2. Na caixa de diálogo exibida, insira as informações da rota.
   - **Destination**: insira o endereço de serviço exibido na página de detalhes do **balanceador de carga**.
   - **Next Hop Type**: selecione **VPC peering connection**.
3. Clique em **OK**.

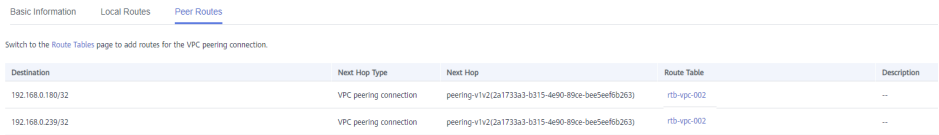
Figura 4-4 Rotas locais



Passo 6 Vá para a página de guia **Peer Routes** e clique em **Route Tables**.

1. Em **Routes**, clique em **Add Route**.
2. Na caixa de diálogo exibida, insira as informações da rota.
   - **Destination**: insira o endereço de saída privado exibido na página de detalhes do **gateway dedicado**.
   - **Next Hop Type**: selecione **VPC peering connection**.
3. Clique em **OK**.

Figura 4-5 Rotas de pares



----Fim

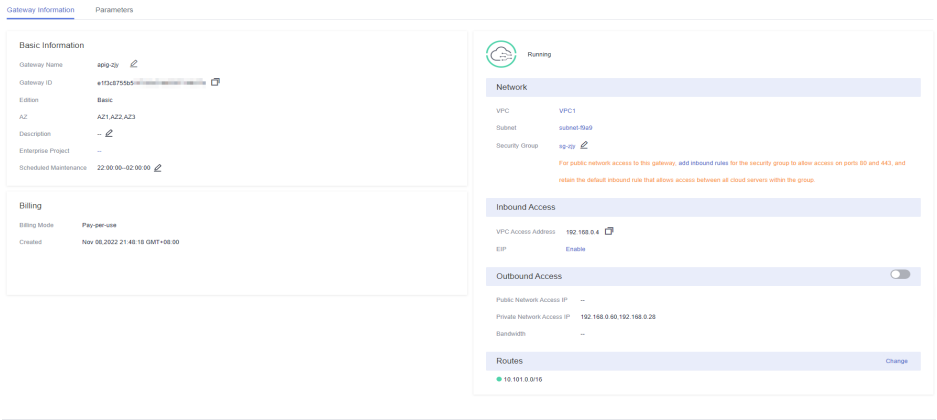
Configuração de uma rota

Passo 1 Retorne ao console do APIG.

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

Passo 3 Clique no nome do **gateway dedicado** criado ou clique em **Access Console**.

Passo 4 Clique em **Change** na área **Routes**, insira o bloco CIDR IPv4 da VPC 2 onde está localizado o balanceador de carga que você comprou.



Passo 5 Clique em **Save**.

----Fim

Criação de uma API

Passo 1 No console do APIG, escolha **API Management** > **APIs** e clique em **Create API**.

Passo 2 Configure as informações de front-end e clique em **Next**.

Tabela 4-7 Configuração de front-end

Parâmetro	Descrição
API Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Group	A opção padrão é **DEFAULT**.
URL	**Method**: método de solicitação da API. Defina este parâmetro como **GET**. **Protocol**: protocolo de solicitação da API. Defina este parâmetro como **HTTPS**. **Subdomain Name**: o sistema aloca automaticamente um nome de subdomínio para cada grupo de APIs para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia. **Path**: caminho para solicitar a API.
Gateway Response	Selecione uma resposta a ser exibida se o gateway falhar ao processar uma solicitação de API. A resposta de gateway padrão é **default**.
Authentication Mode	Modo de autenticação da API. Selecione **None**.

Passo 3 Configure as informações de back-end e clique em **Next**.

Tabela 4-8 Parâmetros para definir um serviço de back-end HTTP/HTTPS

Parâmetro	Descrição
Load Balance Channel	Determine se o serviço de back-end será acessado usando um canal de balanceamento de carga. Para este exemplo, selecione **Skip**.
URL	**Method**: método de solicitação da API. Defina este parâmetro como **GET**. **Protocol**: defina este parâmetro como **HTTP**. **Backend Address**: insira o endereço de serviço do balanceador de carga que você comprou. **Path**: caminho do serviço de back-end.

Passo 4 Defina a resposta e clique em **Finish**.

----Fim

Compra de um ECS

Passo 1 Faça logon no console do servidor de nuvem.

Passo 2 Clique em **Buy ECS**.

Passo 3 Configure as configurações básicas e clique em **Next: Configure Network**.

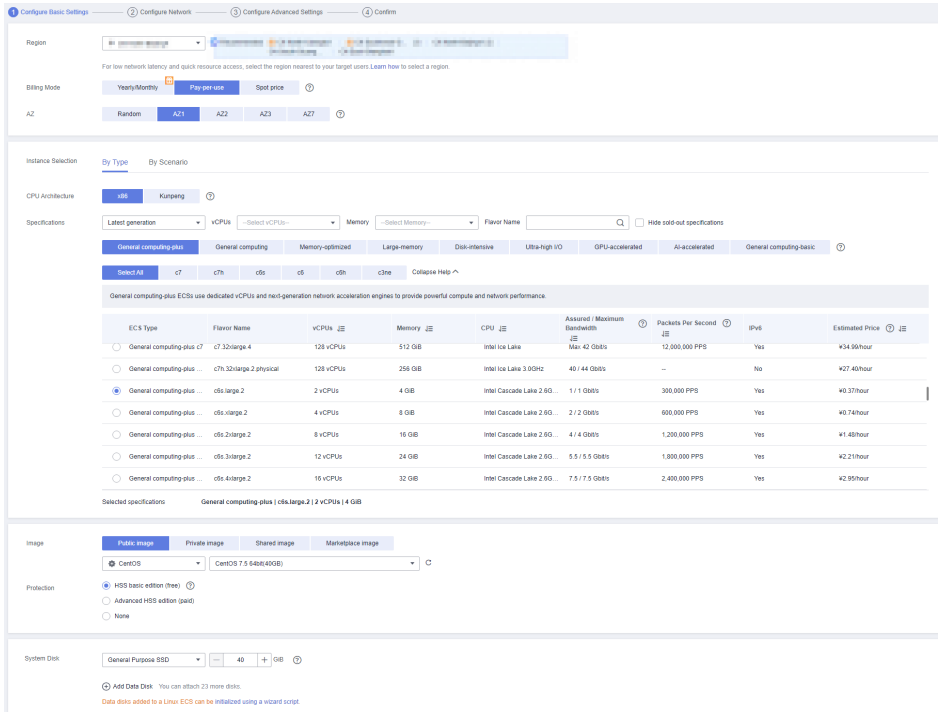


Tabela 4-9 Configurações básicas

Parâmetro	Descrição
Region	Selecione a região onde o ECS está localizado. Deve ser a mesma que a região da VPC 2.
Billing Mode	Selecione **Pay-per-use**.
AZ	Selecione a AZ onde o ECS está localizado.
CPU Architecture	A opção padrão é **x86**.
Specifications	Selecione as especificações que correspondem ao seu planejamento de serviço.
Image	Selecione uma imagem que corresponda ao seu planejamento de serviço.

Passo 4 Defina as configurações de rede e clique em **Next: Configure Advanced Settings**.

Tabela 4-10 Configurações da rede

Parâmetro	Descrição
Network	Selecione **VPC 2** e uma sub-rede.
Security Group	Selecione o grupo de segurança criado para o **gateway dedicado**.
EIP	Selecione **Not required**.

Passo 5 Configure as configurações avançadas e clique em **Next: Confirm**.

Tabela 4-11 Configurações avançadas

Parâmetro	Descrição
ECS Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Login Mode	Credencial para efetuar logon no ECS. A opção padrão é **Password**.
Username	O usuário padrão é **root**.
Password	Defina uma senha para efetuar logon no ECS.
Confirm Password	Insira a senha novamente.

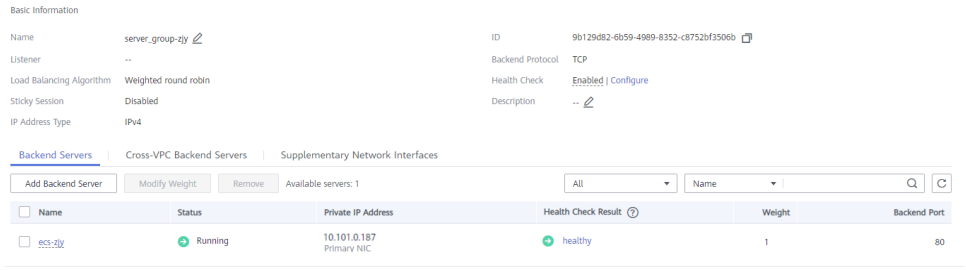
Passo 6 Confirme a configuração e selecione o projeto empresarial **default**.

Passo 7 Leia e confirme a sua aceitação do acordo. Em seguida, clique em **Submit**.

----Fim

Depuração da API

Passo 1 Na página de guia **Backend Server Groups** do **balanceador de carga**, adicione **o ECS**.



Passo 2 Vá para a página **API Management** > **APIs** do **gateway dedicado** e escolha **More** > **Debug** na linha que contém **a API que você criou**.

Passo 3 Insira os parâmetros da solicitação e clique em **Debug**.

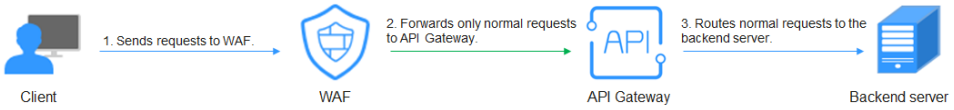
Se o código de status for **200**, a depuração será bem-sucedida.

----Fim

5 Interconexão de um gateway dedicado com o WAF

Para proteger o API Gateway e seus servidores back-end contra ataques maliciosos, implemente o Web Application Firewall (WAF) entre o API Gateway e a rede externa.

Figura 5-1 Acesso a um servidor back-end



NOTA

As instruções a seguir são baseadas no novo console. Se você estiver usando o console anterior, consulte o **Guia de usuário do API Gateway**.

(Recomendado) Solução 1: registrar o nome de domínio de depuração de grupo de APIs no WAF e usar o nome de domínio para acessar o serviço de back-end

Os grupos de APIs fornecem serviços usando nomes de domínio para alta escalabilidade.

Passo 1 Crie um grupo de APIs em um gateway, registre o nome de domínio e crie uma API no grupo.

Figura 5-2 Criação de um grupo de APIs e registro do nome de domínio de depuração

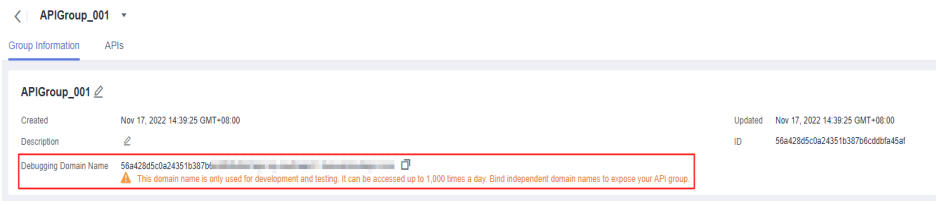
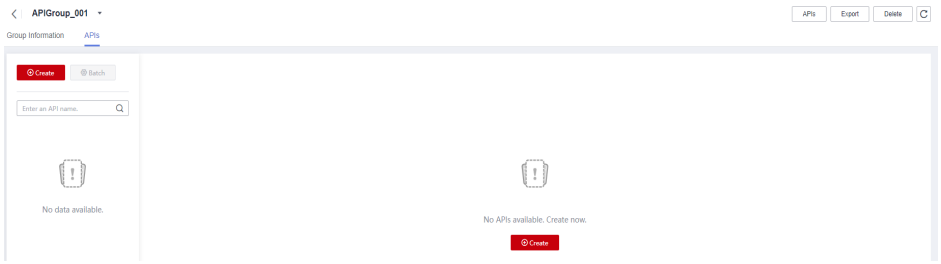


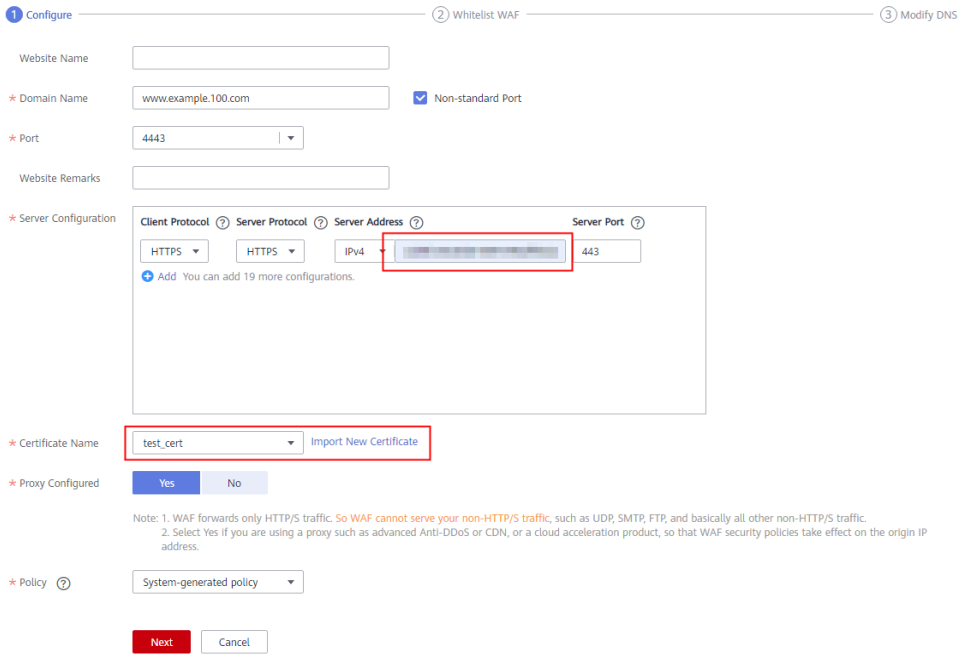
Figura 5-3 Criação de uma API



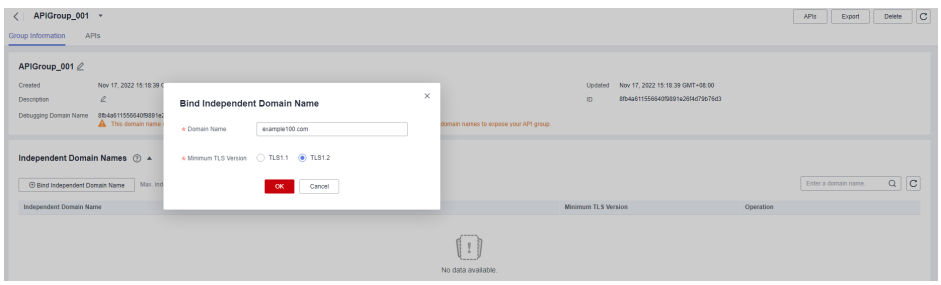
Passo 2 Vá para o console do WAF e adicione um nome de domínio configurando **Server Address** como o nome de domínio do grupo de APIs e adicionando um certificado. Para obter detalhes, consulte **Processo de conexão (modo de nuvem)**.

NOTA

Você pode usar um cliente de rede pública para acessar o WAF com seu nome de domínio. Em seguida, o WAF usa o mesmo nome de domínio para encaminhar suas solicitações para o API Gateway. Não há limite para o número de solicitações que o API Gateway pode receber para o nome de domínio.



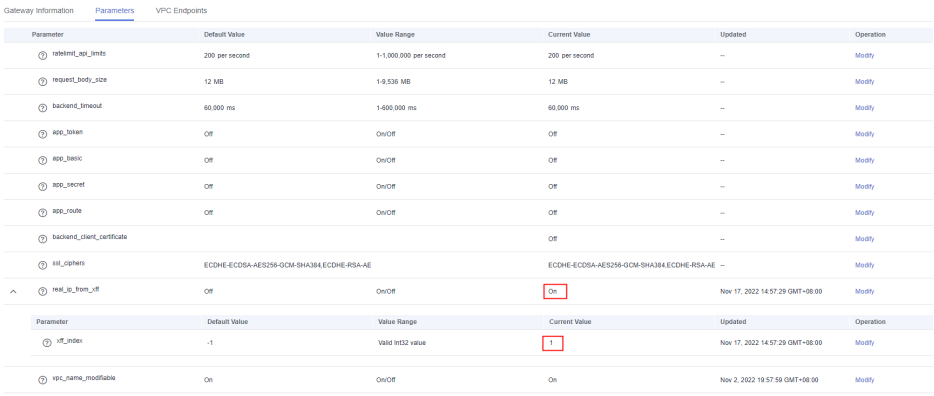
Passo 3 Na página de detalhes do gateway, vincule o nome de domínio ao grupo de APIs.



Passo 4 Ative **real_ip_from_xff** e defina o valor do parâmetro como **1**.

NOTA

Quando um usuário acessa o WAF usando um cliente de rede pública, o WAF registra o endereço IP real do usuário no cabeçalho HTTP **X-Forwarded-For**. O API Gateway resolve o endereço IP real do usuário com base no cabeçalho.

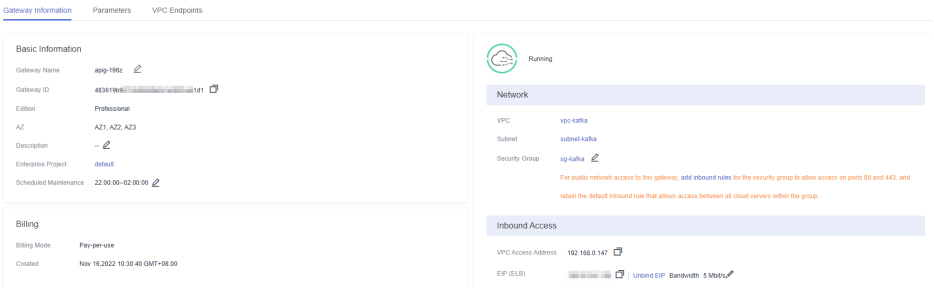


----Fim

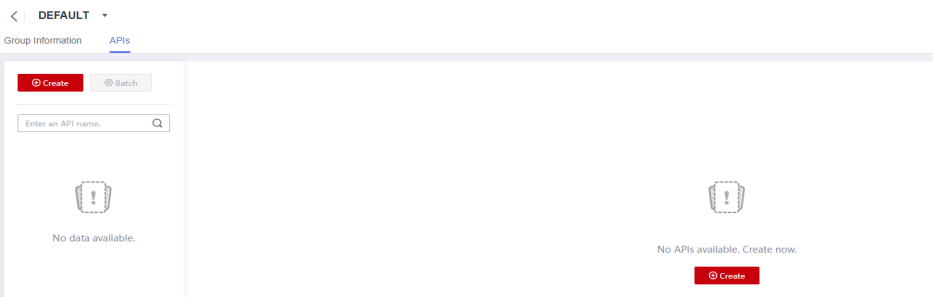
Solução 2: encaminhar solicitações pelo grupo DEFAULT e usar o endereço de acesso de entrada do gateway para acessar o serviço de back-end do WAF

Passo 1 Visualize os endereços de acesso de entrada do seu gateway. Não há limite para o número de vezes que o gateway da API pode ser acessado usando um endereço IP.

- **VPC Ingress Address**: endereço de acesso da VPC
- **EIP**: endereço de acesso à rede pública



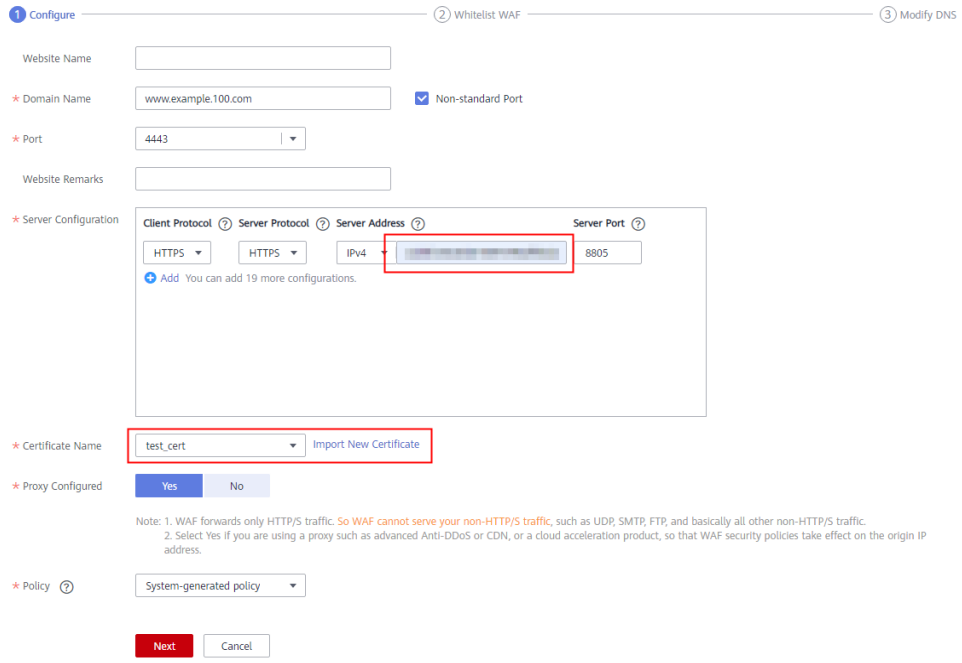
Passo 2 Crie uma API no grupo **DEFAULT**.



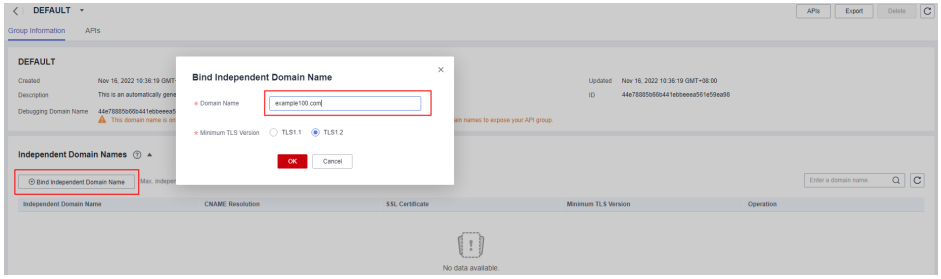
Passo 3 Vá para o console do WAF, adicione um nome de domínio configurando **Server Address** como um **endereço de acesso de entrada** do seu gateway da API e adicionando um certificado e, em seguida, copie os endereços IP de volta à origem do WAF. Para obter detalhes, consulte **Processo de conexão (modo de nuvem)**.

NOTA

- Se o WAF e o seu gateway estiverem na mesma VPC, defina **Server Address** como o endereço de acesso da VPC.
- Se o seu gateway estiver vinculado a um EIP, defina **Server Address** como o EIP.



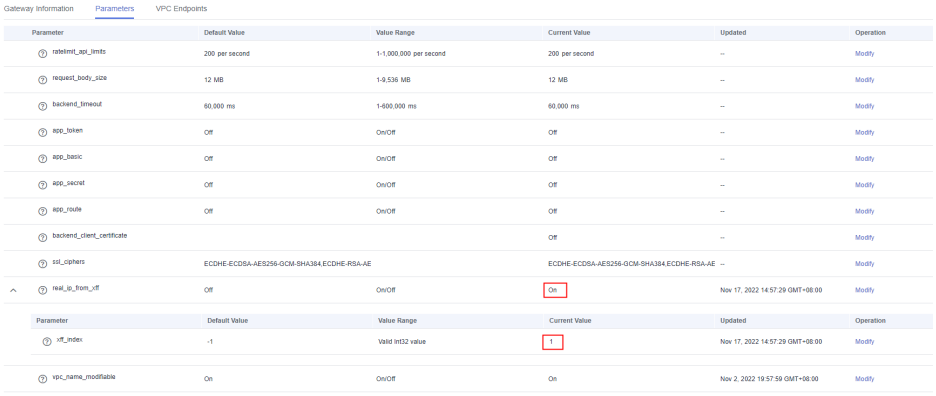
Passo 4 Na página de detalhes do gateway, vincule o nome de domínio ao grupo **DEFAULT**.



Passo 5 Ative **real_ip_from_xff** e defina o valor do parâmetro como **1**.

NOTA

Quando um usuário acessa o WAF usando um cliente de rede pública, o WAF registra o endereço IP real do usuário no cabeçalho HTTP **X-Forwarded-For**. O API Gateway resolve o endereço IP real do usuário com base no cabeçalho.



----Fim

6 Limitação de solicitações 2.0 com um gateway dedicado

6.1 Introdução

Cenário

Se o número de solicitações iniciadas de redes públicas para APIs abertas no APIG não for limitado, o aumento contínuo de usuários deteriorará o desempenho do back-end. E o que é pior, o site ou programa vai quebrar devido a um grande número de solicitações enviadas por usuários maliciosos. As políticas tradicionais de limitação de solicitações do APIG limitam as solicitações por API, usuário, credencial e endereço IP de origem.

No entanto, à medida que os usuários e suas demandas se tornam mais diversificados, essas políticas tradicionais não conseguem atender aos requisitos de limitação de taxa mais refinada. Para resolver esse problema, o APIG lançou a limitação de solicitação 2.0, que é um tipo de política de plug-in. As políticas 2.0 permitem que você configure uma limitação mais refinada, por exemplo, para limitar solicitações com base em um determinado parâmetro de solicitação ou locatário.

Esta seção descreve como criar uma política de limitação de solicitação 2.0 para limitação de taxa em diferentes cenários.

Vantagens

- 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. Há suporte para limitação básica, baseada em parâmetros e excluída.
  - Limitação básica: limitar as solicitações por API, usuário, credencial ou endereço IP de origem. Essa função é semelhante a uma política tradicional de limitação de solicitações, mas é incompatível com ela.
  - Limitação baseada em parâmetros: limitar as solicitações com base em cabeçalhos, parâmetro de caminho, método, cadeias de consulta ou parâmetros do sistema.
  - Limitação excluída: limitar as solicitações de credenciais ou locatários específicos.
- As solicitações de API permitidas em um período de tempo podem ser limitadas por usuário ou credencial.

- A limitação de solicitações pode ser precisa para dia, hora, minuto ou segundo.

Restrições

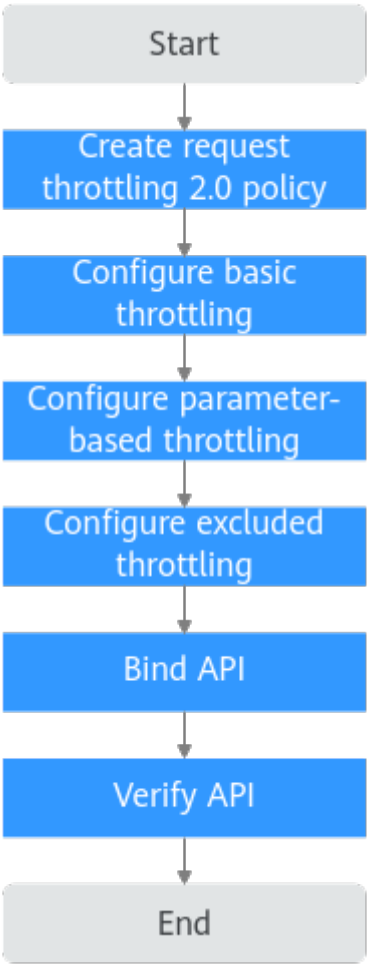
- Adicionar uma política de limitação de solicitações 2.0 a uma API significa vinculá-las. Uma API pode ser vinculada a apenas uma dessas políticas em um ambiente, mas cada política pode ser vinculada a várias APIs. As APIs vinculadas às políticas de limitação de solicitações 2.0 devem ter sido publicadas.
- Para APIs não vinculadas a uma política de limitação de solicitação 2.0, o limite de limitação é o valor de **ratelimit_api_limits** definido na página **Parameters** do gateway.
- Uma política tradicional de limitação de solicitações torna-se inválida se uma política de limitação de solicitações 2.0 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 65.535 caracteres.
- Se o gateway não suportar a limitação de solicitações 2.0, entre em contato com o suporte técnico.

6.2 Procedimento geral

Suponha que você tenha os seguintes requisitos de limitação de solicitação para uma API:

1. A API pode ser chamada até 10 vezes por 60s, mas pode ser chamada por um usuário apenas 5 vezes por 60s.
2. Apenas 10 solicitações contendo o campo de cabeçalho **Host=www.abc.com** são permitidas em 60s.
3. Apenas 10 solicitações com método **GET** e caminho **reqPath = /list** são permitidas em 60s.
4. Apenas 10 solicitações com caminho **reqPath = /fc** são permitidas em 60s.
5. Cada locatário excluído só pode chamar a API 5 vezes por 60 segundos.

Siga esse procedimento para criar uma política de limitação de solicitações 2.0 e vinculá-la a uma API.



1. **Crie uma política.**

   Insira as informações básicas da política de limitação de solicitações 2.0.
2. **Configure a limitação básica.**

   Defina as configurações de limitação básica.
3. **Configure a limitação baseada em parâmetros.**

   Ative a limitação baseada em parâmetros e defina parâmetros e regras.
4. **Configure a limitação excluída.**

   Ative a limitação excluída e configure os locatários e as credenciais excluídos.
5. **Vincule a política a uma API.**

   Vincule a política de limitação de solicitações 2.0 à API.
6. **Verifique a API.**

   Chame a API e verifique se a política de limitação de solicitações 2.0 entrou em vigor.

6.3 Procedimento de implementação

Passo 1 Crie uma política.

Faça logon no console do APIG e crie uma política de limitação de solicitações 2.0. Para obter detalhes, consulte **Limitação de solicitações 2.0** no *Guia de usuário do API Gateway*.

No painel de navegação, escolha **API Management** > **API Policies**. Clique em **Create Policy** e selecione **Request Throttling 2.0**.

Configure as informações básicas da política para atender às suas demandas.

Tabela 6-1 Informações básicas da política

Parâmetro	Descrição
Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Throttling	Selecione **High-performance**.
Policy Type	Selecione **API-specific**, o que significa medir e limitar solicitações de uma única API.
Period	Período de limitação. Defina esse parâmetro como 60s.

Passo 2 Configure a limitação básica.

Conforme exigido em **1**, defina **Max. API Requests** para 10 vezes por 60s e **Max. User Requests** para 5 vezes por 60s.

Tabela 6-2 Limitação básica

Parâmetro	Descrição
Max. API Requests	10
Max. User Requests	5

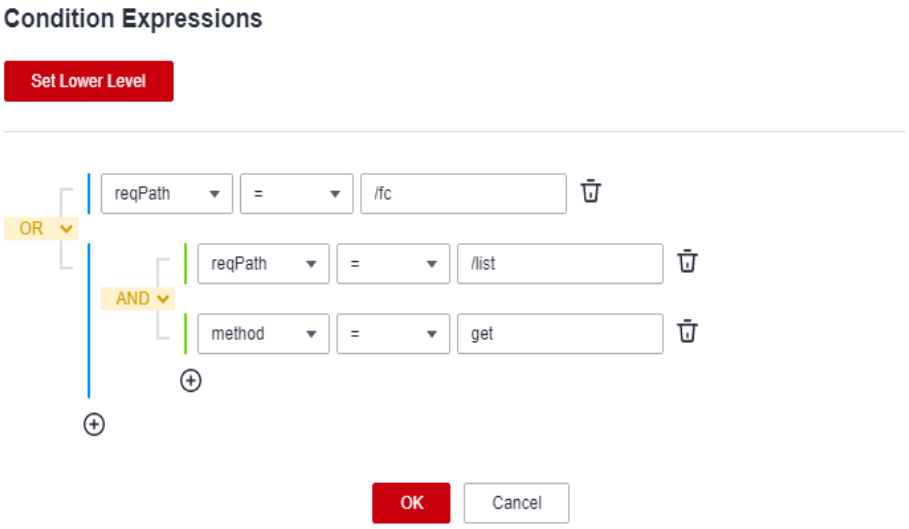
Passo 3 Configure a limitação baseada em parâmetros.

1. Conforme exigido em **2**, ative a limitação baseada em parâmetros e defina o cabeçalho e a regra.
   a. Clique em **Add Parameter**, selecione **header** para **Parameter Location** e insira **Host** para **Parameter**.
   b. Na área **Rules**, clique em **Add Rule** e defina **Max. API Requests** como **10** e **Period** como **60 seconds**. Em seguida, clique em  e defina a condição correspondente **Host = www.abc.com**.
   c. Clique em **OK**. A regra de correspondência de cabeçalho **Host = www.abc.com** é gerada, indicando que uma API vinculada a essa política só pode ser chamada 10 vezes a cada 60s por solicitações cujo cabeçalho **Host** é **www.abc.com**.
2. Conforme necessário em **3** e **4**, defina várias regras com o parâmetro **Path**.
   a. Na área **Rules**, clique em **Add Rule** e defina **Max. API Requests** como **10** e **Period** como **60 seconds**. Em seguida, clique em  para abrir a caixa de diálogo **Condition Expressions**.
   b. Adicione estas três expressões de condição: **reqPath = /fc**, **reqPath = /list** e **method = get**.

c. Clique em **Set Lower Level**.

d. Coloque as duas expressões **reqPath** em uma relação **OR**. Isso significa que a condição é atendida quando um dos dois caminhos é correspondido.

e. Selecione **reqPath = /list** e **method = get**, clique em **Set Lower Level** e selecione **AND**.



f. Clique em **OK**. Indica que APIs com caminho **/list** e método **GET** ou APIs com caminho **/fc** vinculado a essa política só podem ser chamadas 10 vezes por 60s.

Passo 4 Configure a limitação excluída.

Conforme necessário em **5**, ative a limitação excluída. Adicione um locatário excluído com um limite de 5 solicitações por 60s.

Tabela 6-3 Limitação excluída

Parâmetro	Descrição
Account ID	ID do locatário
Threshold	5

Passo 5 Clique em **OK**. A política de limitação de solicitações 2.0 está configurada.

Passo 6 Vincule essa política a uma API.

1. Clique no nome da política para acessar a página de detalhes da política.
2. Na área **APIs**, selecione ambiente **RELEASE** e clique em **Bind to APIs**. Selecione uma API e clique em **OK**.

Passo 7 Verifique a API.

Chame a API e verifique se a política de limitação de solicitações 2.0 entrou em vigor.

----Fim

7 Autenticação de dois fatores com um gateway dedicado

7.1 Introdução

Cenário

O APIG fornece modos de autenticação flexíveis e permite que você configure um autorizador personalizado para autenticação de dois fatores. Esta seção descreve como criar uma API que usa autenticação de dois fatores (aplicação + personalizada).

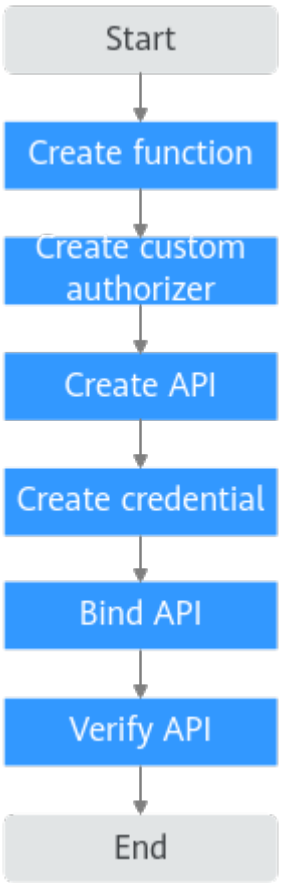
Vantagens

Além da autenticação segura da aplicação, você pode usar um autorizador personalizado para garantir a segurança da API.

Restrições

A autenticação personalizada depende do FunctionGraph.

7.2 Procedimento geral



1. **Crie uma função**.

   A função será usada para autenticação personalizada.

2. **Crie um autorizador personalizado**.

   Defina o tipo de autorizador como **Frontend** e selecione a função criada na etapa anterior.

3. **Crie uma API**.

   Defina o modo de autenticação como **App**, ative **Two-Factor Authentication** e selecione o autorizador personalizado criado na etapa anterior.

4. **Crie uma credencial**.

   As APIs que usam autenticação de aplicação exigem uma credencial para chamar. Crie uma credencial para gerar um ID e um par de chave/segredo.

5. **Vincule a credencial à API criada.**

   As APIs que usam autenticação de aplicação podem ser chamadas apenas com credenciais vinculadas.

6. **Verifique a API.**

   Chame a API para verificar se a autenticação de dois fatores foi configurada com sucesso.

7.3 Procedimento de implementação

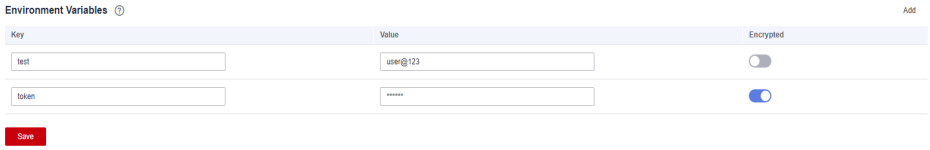
Passo 1 Efetue logon no console do FunctionGraph. Na página **Dashboard**, clique em **Create Function**. Para mais detalhes, consulte **Desenvolvimento de um autorizador personalizado com FunctionGraph**.

1. Defina os parâmetros de acordo com a tabela a seguir e clique em **Create Function**.

Tabela 7-1 Configuração da função

Parâmetro	Descrição
Function Type	Padrão: **Event Function**
Region	Selecione a mesma região que a do APIG.
Function Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Agency	Uma agência que delega FunctionGraph para acessar outros serviços em nuvem. Para este exemplo, selecione **Use no agency**.
Enterprise Project	A opção padrão é **default**.
Runtime	Selecione **Python 3.9**.

2. Na guia **Configuration**, escolha **Environment Variables** no painel esquerdo e clique em **Add**. **test** é um cabeçalho para autenticação de identidade, e **query** é para consulta de parâmetro. Se o **token** envolver dados confidenciais, ative a opção **Encrypted**.



3. Na guia **Code**, copie o seguinte código para **index.py** e clique em **Deploy**. Para obter detalhes sobre codificação, consulte **Criação de uma função para autenticação personalizada de front-end** no *Guia de desenvolvedor do API Gateway*.

```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
    testParameter = context.getUserData('test');
    userToken = context.getUserData('token');
    if event["headers"].get("token") == userToken and
event["queryStringParameters"].get("test") == testParameter:
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"allow",
                "context":{
                    "user":"auth success"
                }
            })
        }
    else:
        resp = {
            'statusCode': 401,
```



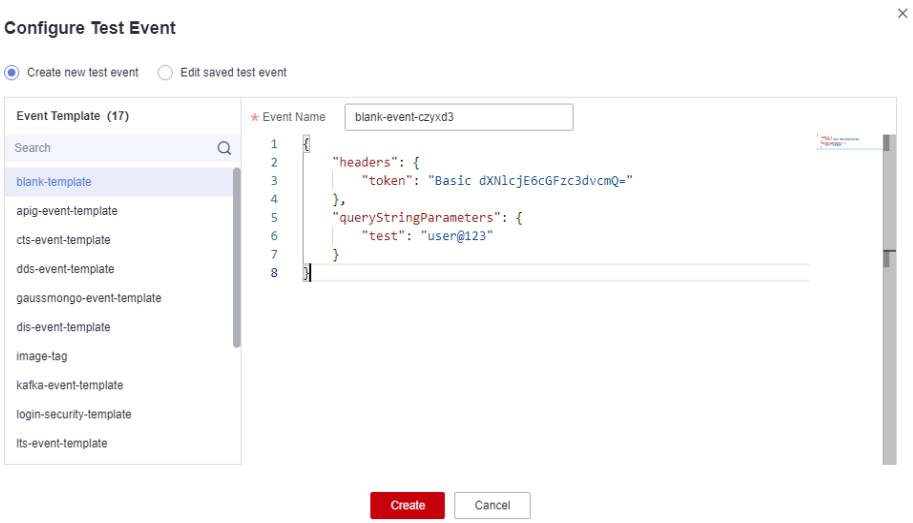
```
            'body': json.dumps({
                "status":"deny",
            })
        }
    return json.dumps(resp)
```

4. Configure um evento de teste para depurar o código.

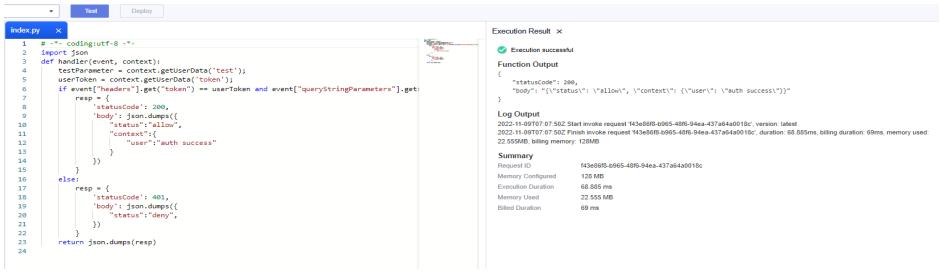
   a. Selecione **Configure Test Event** na lista suspensa e configure um evento de teste.

   NOTA

   Os valores dos parâmetros no evento de teste devem ser os mesmos das variáveis de ambiente.



   b. Clique em **Test**.



   c. Clique em **Deploy**.

Passo 2 Vá para o console do APIG e escolha **API Management** > **API Policies**.

Na guia **Custom Authorizers**, crie um autorizador personalizado.

Tabela 7-2 Configuração do autorizador personalizado

Parâmetro	Descrição
Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Type	Selecione **Frontend**.
Function URN	Clique em **Select** e selecione a **função criada**.

Parâmetro	Descrição
Version/Alias	**Version** é selecionada por padrão.
Max. Cache Age (s)	30
Identity Sources	Defina duas fontes de identidade: **token** de cabeçalho e **test** de cadeia de consulta.

Passo 3 Escolha **API Management** > **APIs** e clique em **Create API**.

1. Configure as informações do front-end de acordo com a tabela a seguir.

   Tabela 7-3 Configuração de front-end

Parâmetro	Descrição
API Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Group	A opção padrão é **DEFAULT**.
URL	**Method**: método de solicitação da API. Defina este parâmetro como **GET**. **Protocol**: protocolo de solicitação da API. Defina este parâmetro como **HTTPS**. **Subdomain Name**: o sistema aloca automaticamente um nome de subdomínio para cada grupo de APIs para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia. **Path**: caminho para solicitar a API. Digite **/api/two_factor_authorization**.
Gateway Response	Selecione uma resposta a ser exibida se o gateway falhar ao processar uma solicitação de API. A resposta de gateway padrão é **default**.
Authentication Mode	Modo de autenticação da API. Defina este parâmetro como **App**.
Two-Factor Authentication	Ative essa opção e selecione um **autorizador personalizado**.

2. Clique em **Next** e defina o tipo de back-end como **Mock**.

   Selecione um código de status, defina a resposta e clique em **Finish**.

3. Publique a API.

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

Clique em **Create Credential**, insira um nome de credencial e clique em **OK**.

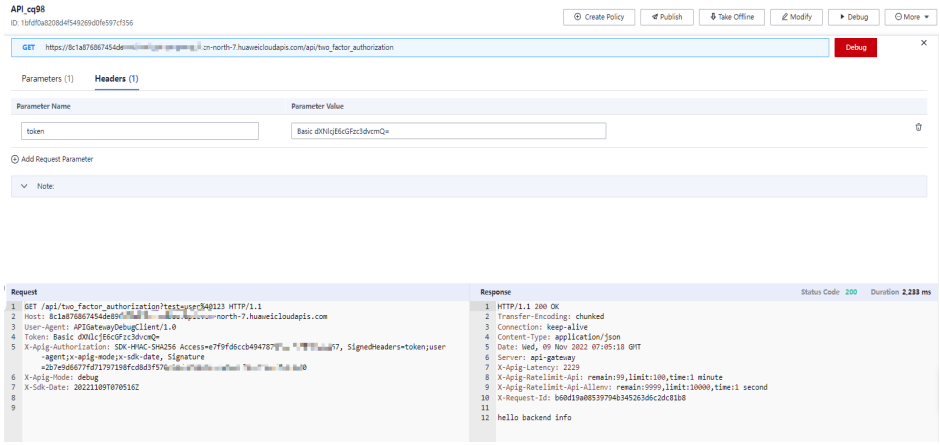
Passo 5 Vincule essa credencial à API.

Clique no nome da credencial para acessar a página de detalhes. Na área **APIs**, clique em **Bind to APIs**, selecione uma API e clique em **OK**.

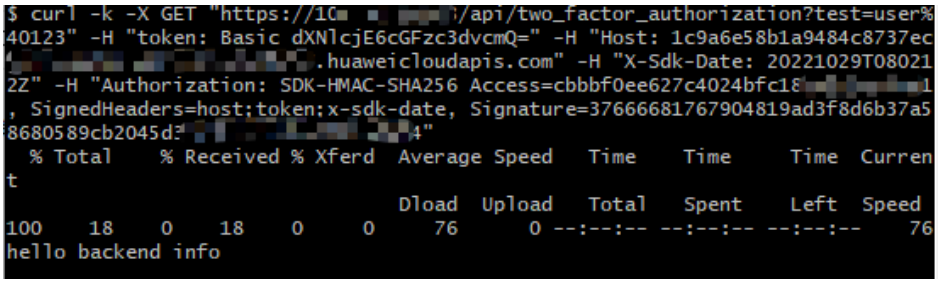
Passo 6 Verifique a API.

- Chame a API na página de depuração do APIG para verificar se a autenticação de dois fatores foi configurada com sucesso.

  Adicione **test** na guia **Parameters** e adicione **token** na guia **Headers**. Use os mesmos valores de parâmetros definidos para a função de autenticação personalizada. Se os valores dos parâmetros forem diferentes, o servidor retornará uma mensagem 401 indicando que a autenticação falha.



- Como alternativa, chame a API com um comando **curl**. Baixe o SDK do JavaScript primeiro. Para chamar a API, insira uma chave e um segredo, bem como o cabeçalho e a cadeia de consulta para gerar um comando **curl** e, em seguida, copie esse comando para a sua CLI para execução. Para obter detalhes, consulte **curl** no *Guia de desenvolvedor do API Gateway*.



----Fim

8 Redirecionamento automático de HTTP para HTTPS com um gateway dedicado

8.1 Introdução

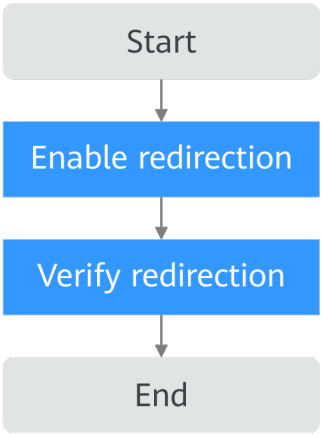
Cenário

O APIG suporta redirecionamento de HTTP para HTTPS. As APIs HTTP são inseguras na transmissão e autenticação. Você pode atualizá-las para acesso via HTTPS, garantindo a compatibilidade HTTP. Esta função é suportada por gateways criados após 30 de novembro de 2022.

Restrições

O redirecionamento é adequado apenas para solicitações GET e HEAD. Redirecionar outras solicitações pode causar perda de dados devido a restrições do navegador.

8.2 Procedimento geral



1. **Ative o redirecionamento**.

Verifique se a API para a qual você ativa o redirecionamento usa HTTPS ou HTTP&HTTPS para solicitações front-end.

2. **Verifique o redirecionamento**.

   Verifique se a função de redirecionamento está funcionando.

8.3 Procedimento de implementação

NOTA

Pré-requisitos

- Você criou uma API cujo protocolo de solicitação de front-end está definido como **HTTPS** ou **HTTP&HTTPS**.
- A API foi publicada.
- Um nome de domínio independente e um certificado SSL foram vinculados ao grupo de APIs ao qual a API pertence.

Para obter detalhes sobre essas operações, consulte o **Guia de usuário do APIG**

Ativação do redirecionamento

Passo 1 Faça logon no console do APIG e escolha **API Management** > **API Groups**.

Passo 2 Clique em um nome de grupo para acessar a página de detalhes.

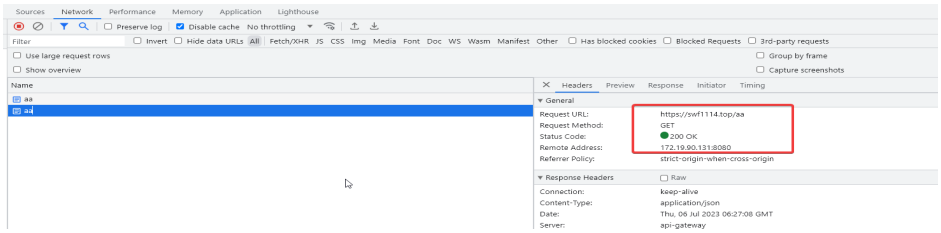
Passo 3 Na guia **Group Information**, localize o nome de domínio independente vinculado e ative o **HTTP-to-HTTPS Auto Redirection**.

----Fim

Verificação do redirecionamento

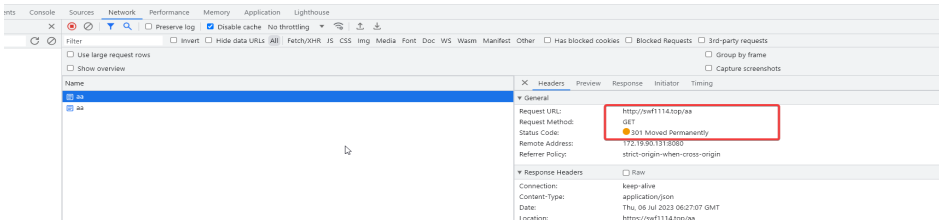
Passo 1 Use um navegador para chamar a API por meio de HTTPS.

1. Na barra de endereços do navegador, digite **https://***API request path* e pressione **Enter**.
2. Pressione **F12**.
3. Verifique o código de status exibido na guia **Network**. **200** significa que a chamada foi bem-sucedida.



Passo 2 Use um navegador para chamar a API por meio de HTTP.

1. Na barra de endereços do navegador, digite **http://***API request path* e pressione **Enter**.
2. Pressione **F12**.
3. Verifique o código de status exibido na guia **Network**. **301** significa que o redirecionamento foi bem-sucedido.



----Fim

9 Roteamento de solicitações de serviço gRPC usando um gateway dedicado

9.1 Introdução

Cenário

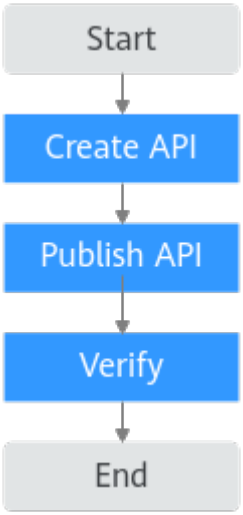
gRPC é uma estrutura moderna, de código aberto e de alto desempenho de Chamada de procedimento remoto (RPC) que pode ser executada em qualquer ambiente. Você só precisa definir a solicitação e a resposta de cada API e deixar que a estrutura gRPC cuide do resto. O gRPC usa buffers de protocolo (protobuf) como Linguagem de definição de interface (IDL) e para troca de mensagens na camada inferior.

Quando você usa um serviço de gRPC, pode criar uma API no APIG para rotear solicitações para o serviço.

Restrições

Devido às restrições do protocolo do gRPCs, as APIs do gRPC não podem ser importadas, exportadas ou depuradas e não são compatíveis com políticas de autenticação personalizadas ou de terceiros.

9.2 Procedimento geral



1. **Crie uma API**.

   Crie uma API gRPC com gRPCs como protocolos de front-end e back-end.

2. **Publique a API**.

   Publique a API gRPC em um ambiente.

3. **Verifique a API**.

   Use um cliente gRPC para testar o serviço gRPC. Se o servidor retornar uma resposta normalmente, o serviço gRPC estará disponível.

9.3 Procedimento de implementação

Pré-requisitos

- O cliente e o servidor são do tipo gRPC.
- O servidor tem um arquivo proto que define os parâmetros de solicitação e resposta da API. O arquivo proto é usado no gRPC para definir estruturas de dados e APIs de serviço. Ele descreve estruturas de dados e interações usando protobuf e serve como um contrato para a comunicação entre o cliente e o servidor.

Criação de uma API

Passo 1 Vá para o console do APIG.

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

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

Passo 4 Clique em **Create API** > **Create gRPC API**. Para obter detalhes, consulte **Criação de uma API de gRPC**.

Passo 5 Configure as informações de front-end e clique em **Next**.

Tabela 9-1 Configuração de front-end

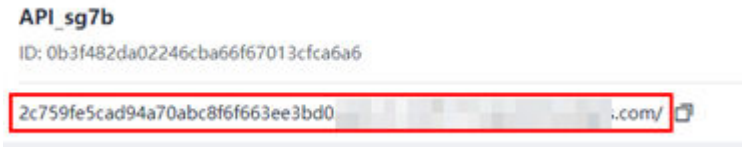
Parâmetro	Descrição
API Name	Insira um nome que esteja em conformidade com regras específicas para facilitar a pesquisa.
Group	A opção padrão é **DEFAULT**.
URL	**Method**: método de solicitação da API. Padrão: **POST**. **Protocol**: protocolo de solicitação da API. Padrão: **GRPCS**. **Subdomain Name**: o sistema aloca automaticamente um nome de subdomínio para cada grupo de APIs para testes internos. O nome do subdomínio pode ser acessado 1000 vezes por dia. **Path**: caminho para solicitar a API. Neste exemplo, insira **/helloworld.Greeter**. Para obter detalhes sobre o caminho da solicitação, consulte o **arquivo proto**. **helloworld** indica o nome do pacote e **Greeter** indica o nome do serviço.
Gateway Response	Selecione uma resposta a ser exibida se o gateway falhar ao processar uma solicitação de API. A resposta de gateway padrão é **default**.
Matching	Selecione **Prefix match**.
Authentication Mode	Modo de autenticação da API. Selecione **None**.

Passo 6 Configure as informações de back-end e clique em **Next**.

Tabela 9-2 Configuração de back-end

Parâmetro	Descrição
Load Balance Channel	Determine se o serviço de back-end será acessado usando um canal de balanceamento de carga. Para este exemplo, selecione **Skip**.
URL	**Method**: método de solicitação da API. Padrão: **POST**. **Protocol**: protocolo de solicitação do serviço de back-end. Padrão: **GRPCS**. **Backend Address**: endereço e porta do serviço de back-end. **Path**: caminho do serviço de back-end. Neste exemplo, insira **/**.

Passo 7 Clique em **Finish**.

> **NOTA**
>
> Na página **APIs**, o URL da API mostra apenas o nome e o caminho do domínio. Ele não mostra o método de solicitação ou protocolo. Ao enviar uma solicitação gRPC, insira o nome do domínio.
>
> 
>

----Fim

Publicação da API

Passo 1 Na guia **APIs**, selecione a API criada e clique em **Publish**.

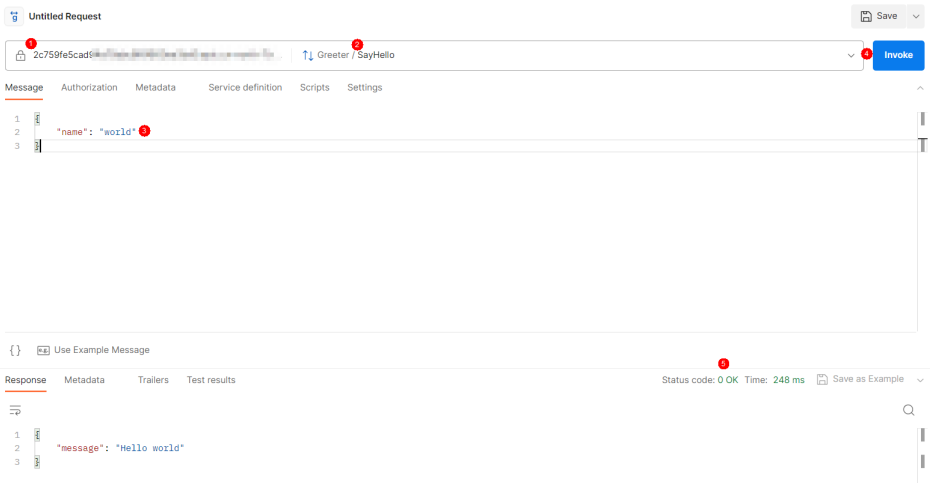
Passo 2 Selecione o ambiente onde a API será publicada e insira uma descrição.

Passo 3 Clique em **OK**. Depois que a API é publicada, o ponto de exclamação (!) vermelho no canto superior esquerdo do botão **Publish** desaparece.

----Fim

Verificação da API

Use a ferramenta de **teste da API** para chamar a API criada ou invoque essa API em um cliente.



Passo 1 Insira o nome de domínio de depuração do grupo da API.

Passo 2 Importe o arquivo proto do servidor.

O arquivo proto contém o seguinte conteúdo:

```
syntax = "proto3";
package helloworld;
// The greeting service definition.
service Greeter {
// Sends a greeting
rpc SayHello (HelloRequest) returns (HelloReply) {}
}
// The request message containing the user's name.
message HelloRequest {
```



```
string name = 1;
}
// The response message containing the greetings
message HelloReply {
string message = 1;
}
```

- **helloworld**: nome do pacote
- **Greeter**: nome do serviço
- **SayHello**: nome do método
- **HelloRequest**: corpo da solicitação
- **HelloReply**: corpo de resposta

Passo 3 Insira uma solicitação de API na área **message** de acordo com o arquivo proto.

```
{
    "name": "world"
}
```

Passo 4 Clique em **Invoke** para enviar a solicitação.

Passo 5 Veja a resposta na área **Response**. Se o código de status **0 OK** for exibido, a invocação será bem-sucedida.

----Fim

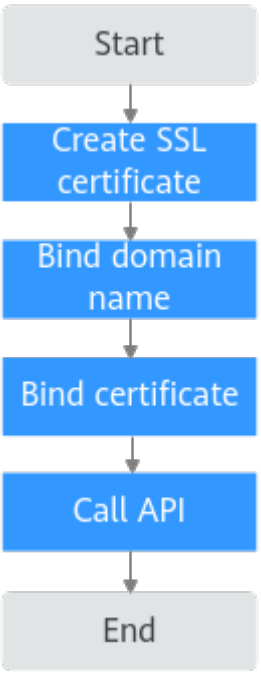
10 Autenticação de cliente com um gateway dedicado

10.1 Solução

Se o front-end da API oferecer suporte a HTTPS, será necessário adicionar um certificado SSL para o nome de domínio independente vinculado ao grupo de APIs. Um certificado SSL é usado para criptografia de dados e autenticação de identidade. Se um certificado SSL contiver um **certificado de AC**, a autenticação de cliente (autenticação bidirecional) será ativada por padrão. Ou autenticação unidirecional será usada.

- Autenticação unidirecional: quando um cliente se conecta a um servidor, o cliente verifica a validade do certificado SSl do servidor.
- Autenticação bidirecional: quando um cliente se conecta a um servidor, o cliente e o servidor verificam a validade do certificado SSl.

10.2 Procedimento geral



Gateways dedicados suportam autenticação unidirecional e bidirecional. Estes dois modos têm o mesmo procedimento. A seguir, a autenticação unidirecional será usada como exemplo. Para obter detalhes sobre a autenticação bidirecional, consulte **Autenticação bidirecional**.

1. **Crie um certificado SSL**.

   Um certificado SSL é usado para criptografia de dados e autenticação de identidade.
2. **Vincule um nome de domínio**.

   Vincule o grupo ao qual a API pertence com um nome de domínio independente licenciado e resolvido.
3. **Vincule um certificado**.

   Vincule o nome de domínio independente ao certificado SSL criado.
4. **Chame a API**.

   Verifique se a chamada da API foi bem-sucedida.

10.3 Procedimento de implementação

Autenticação unidirecional

Passo 1 Vá para o console do APIG.

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

Passo 3 Crie um certificado SSL.

1. No painel de navegação, escolha **API Management** > **API Policies**.
2. Na guia **SSL Certificates**, clique em **Create SSL Certificate**.

Tabela 10-1 Configuração de certificado para autenticação unidirecional

Parâmetro	Descrição
Name	Digite um nome de certificado que esteja em conformidade com regras específicas para facilitar a pesquisa.
Instances Covered	Selecione **Current**.
Content	-----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----
Key	-----Start RSA private key----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End RSA private key-----
CA	Nenhum certificado de AC é necessário para a autenticação unidirecional.

3. Clique em **OK**.

Passo 4 Vincule um nome de domínio.

1. No painel de navegação, escolha **API Management** > **API Groups**.
2. Clique no nome do grupo ao qual a API pertence. A página de detalhes do grupo é exibida.
3. Na página de guia **Group Information**, clique em **Bind Independent Domain Name**.

Tabela 10-2 Configuração de nome de domínio independente

Parâmetro	Descrição
Domain Name	Insira um nome de domínio licenciado.
Minimum TLS Version	Selecione **TLS1.2**.
HTTP-to-HTTPS Auto Redirection	Desativado por padrão.

4. Clique em **OK**.

Passo 5 Vincule um certificado.

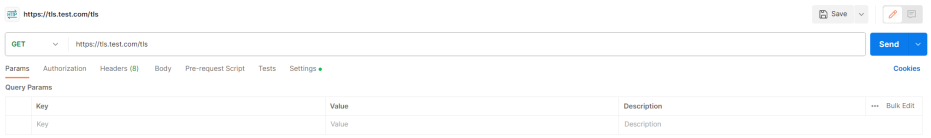
1. Na linha que contém o nome de domínio, clique em **Select SSL Certificate**.
2. Selecione o certificado criado e clique em **OK**.

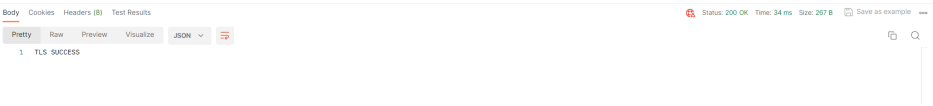
AVISO

A autenticação do cliente deve ser desativada para autenticação unidirecional.

Passo 6 Chame a API.

Use a ferramenta de teste da API para chamar a API. Se o código de status for **200**, a API é chamada com sucesso.





----Fim

Autenticação bidirecional

Passo 1 Na guia **SSL Certificates**, clique em **Create SSL Certificate**.

Tabela 10-3 Configuração do certificado para autenticação bidirecional

Parâmetro	Descrição
Name	Digite um nome de certificado que esteja em conformidade com regras específicas para facilitar a pesquisa.
Instances Covered	Selecione **Current**.
Content	Insira o conteúdo do certificado. -----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----
Key	Digite a chave. -----Start RSA private key----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End RSA private key-----

Parâmetro	Descrição
CA	Digite o conteúdo do certificado de AC. **Depois que o certificado de AC é configurado, a autenticação do cliente é ativada por padrão, desde que o nome de domínio independente esteja vinculado ao certificado SSL.** -----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----

Passo 2 Clique em **OK**.

Passo 3 Vincule um nome de domínio.

1. No painel de navegação, escolha **API Management** > **API Groups**.
2. Clique no nome do grupo ao qual a API pertence. A página de detalhes do grupo é exibida.
3. Na página de guia **Group Information**, clique em **Bind Independent Domain Name**.

   Tabela 10-4 Configuração de nome de domínio independente

Parâmetro	Descrição
Domain Name	Insira um nome de domínio licenciado.
Minimum TLS Version	Selecione **TLS1.2**.
HTTP-to-HTTPS Auto Redirection	Desativado por padrão.

4. Clique em **OK**.

Passo 4 Vincule um certificado.

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

AVISO

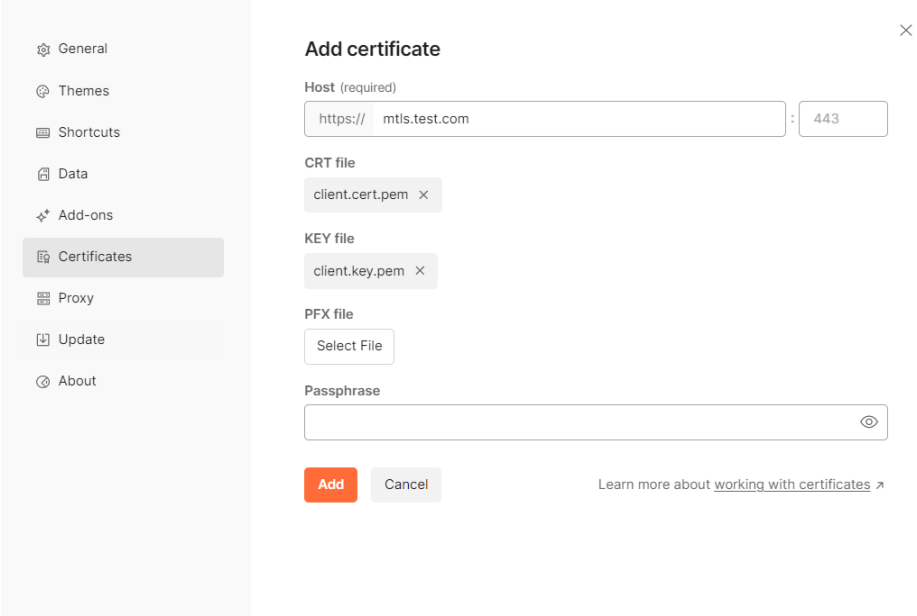
Depois de vincular um certificado SSL, a autenticação bidirecional é ativada automaticamente.

Passo 5 Chame a API.

Use a ferramenta de teste da API para chamar a API. Se o código de status for **200**, a API é chamada com sucesso.

Você precisa configurar o certificado do cliente ao acessar APIs.

Se o Postman for usado para chamar APIs, você precisará adicionar certificados de cliente a **Certificates** em **Setting** e carregar os certificados e a chave de cliente.



----Fim

