API Gateway

Best Practices

Issue 01

Date 2023-04-06

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Selectively Exposing CCE Workloads

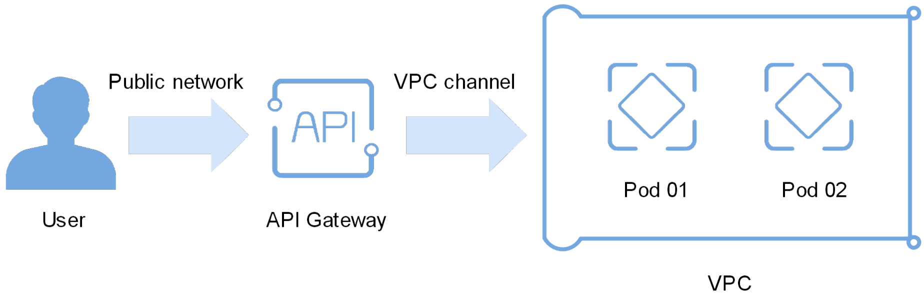
Overview

You can use APIG to selectively expose your workloads and microservices in Cloud Container Engine (CCE). Using APIG to expose containerized applications has the following benefits:

- You do not need to set elastic IP addresses, and this reduces network bandwidth costs.

  You can set up a VPC channel to access workloads in CCE.
- You can choose an authentication mode from multiple options to ensure access security.
- You can configure a request throttling policy to ensure secure access to your backend service.
- You can configure multiple pods for each workload for load balancing, optimizing resource utilization and increasing system reliability.

Figure 1-1 Accessing CCE workloads through APIG



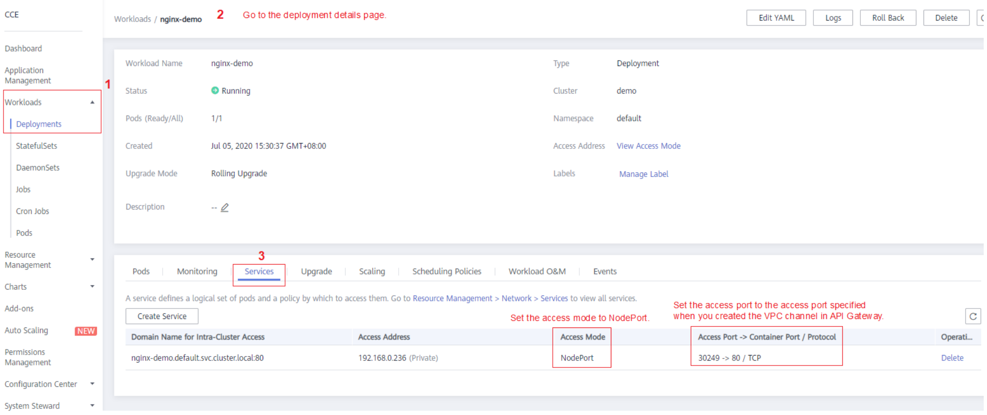
Preparing CCE Workloads

Create a cluster and workload in CCE, and add pods and containers to the workload. For more information, see .

View the workload details on the CCE console, and ensure that the service access mode is **NodePort** or **LoadBalancer**. For details, see NodePort or LoadBalancer.

- NodePort access

Figure 1-2 Viewing the access port



2 Go to the deployment details page.

Workload Name nginx-demo
Status Running
Pods (Ready/All) 1/1
Created Jul 05, 2020 15:30:37 GMT+08:00
Upgrade Mode Rolling Upgrade
Description --
Type Deployment
Cluster demo
Namespace default
Access Address View Access Mode
Labels Manage Label

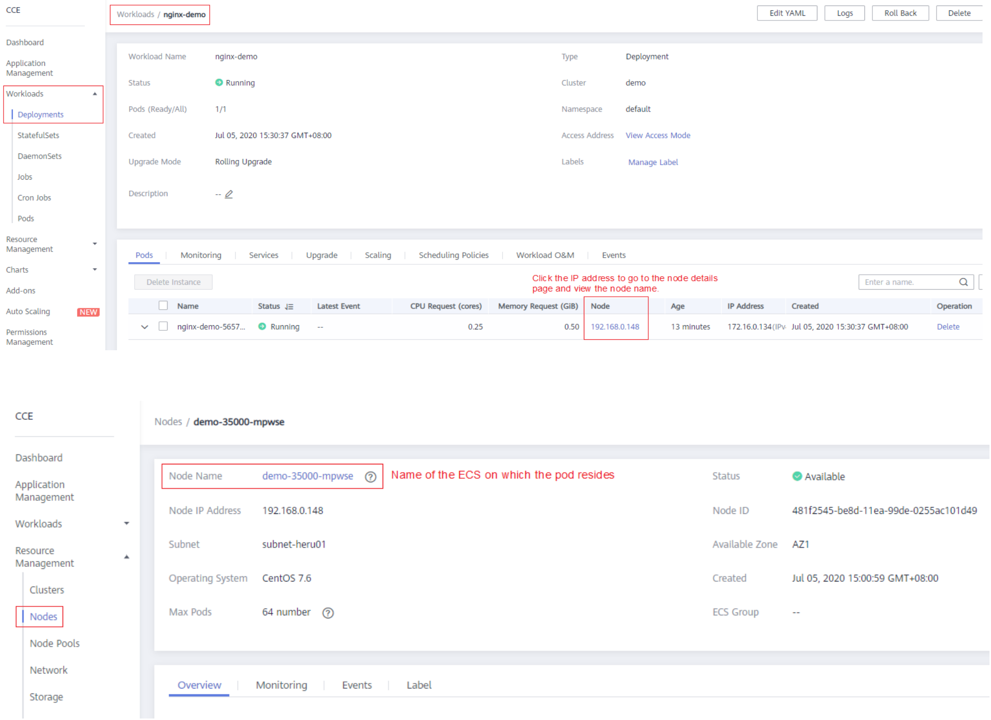
A service defines a logical set of pods and a policy by which to access them. Go to Resource Management > Network > Services to view all services.

Set the access mode to NodePort.

Set the access port to the access port specified when you created the VPC channel in API Gateway.

Domain Name for Intra-Cluster Access	Access Address	Access Mode	Access Port -> Container Port / Protocol	Operati...
nginx-demo.default.svc.cluster.local:80	192.168.0.236 (Private)	NodePort	30249 -> 80 / TCP	Delete

Figure 1-3 Viewing the name of the ECS on which the pod resides



Workload Name nginx-demo
Status Running
Pods (Ready/All) 1/1
Created Jul 05, 2020 15:30:37 GMT+08:00
Upgrade Mode Rolling Upgrade
Description --
Type Deployment
Cluster demo
Namespace default
Access Address View Access Mode
Labels Manage Label

Click the IP address to go to the node details page and view the node name.

	Name	Status	Latest Event	CPU Request (cores)	Memory Request (GiB)	Node	Age	IP Address	Created	Operation
□	nginx-demo-5657...	Running	--	0.25	0.50	192.168.0.148	13 minutes	172.16.0.134(IPv	Jul 05, 2020 15:30:37 GMT+08:00	Delete

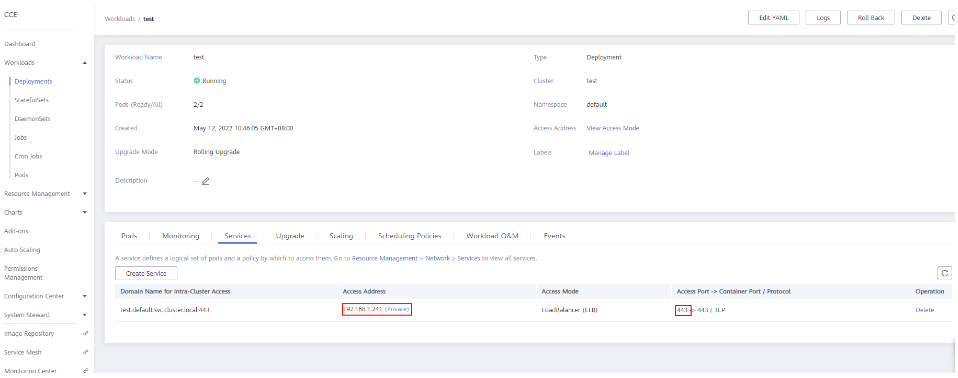
Nodes / demo-35000-mpwse

Node Name demo-35000-mpwse

Name of the ECS on which the pod resides

Node IP Address 192.168.0.148
Subnet subnet-heru01
Operating System CentOS 7.6
Max Pods 64 number
Status Available
Node ID 481f2545-be8d-11ea-99de-0255ac101d49
Available Zone AZ1
Created Jul 05, 2020 15:00:59 GMT+08:00
ECS Group --

- LoadBalancer access



Workload Name test
Status Running
Pods (Ready/All) 2/2
Created May 12, 2022 10:46:05 GMT+08:00
Upgrade Mode Rolling Upgrade
Description --
Type Deployment
Cluster test
Namespace default
Access Address View Access Mode
Labels Manage Label

A service defines a logical set of pods and a policy by which to access them. Go to Resource Management > Network > Services to view all services.

Domain Name for Intra-Cluster Access	Access Address	Access Mode	Access Port -> Container Port / Protocol	Operation
test.default.svc.cluster.local:443	192.168.1.241 (Private)	LoadBalancer (ELB)	443 -> 443 / TCP	Delete

Creating a VPC Channel

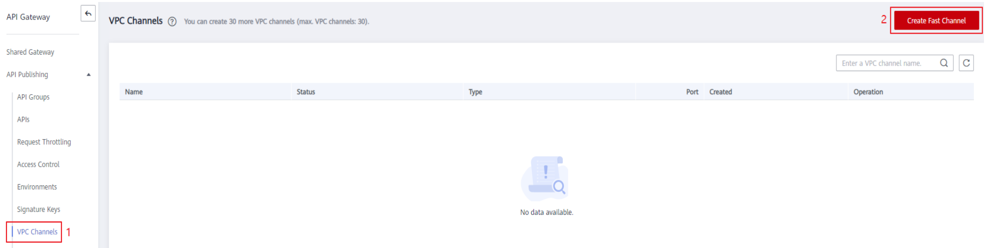
If the access mode of the target CCE workload is **LoadBalancer**, skip this procedure and go to **Opening an API**.

Step 1 Log in to the management console, select a region in the upper left corner, and choose **Service List** > **Application** > **API Gateway**.

Step 2 Create a VPC channel.

1. On the **VPC Channels** page, click **Create Fast Channel**.

Figure 1-4 VPC channel list



You can create 30 more VPC channels (max. VPC channels: 30).

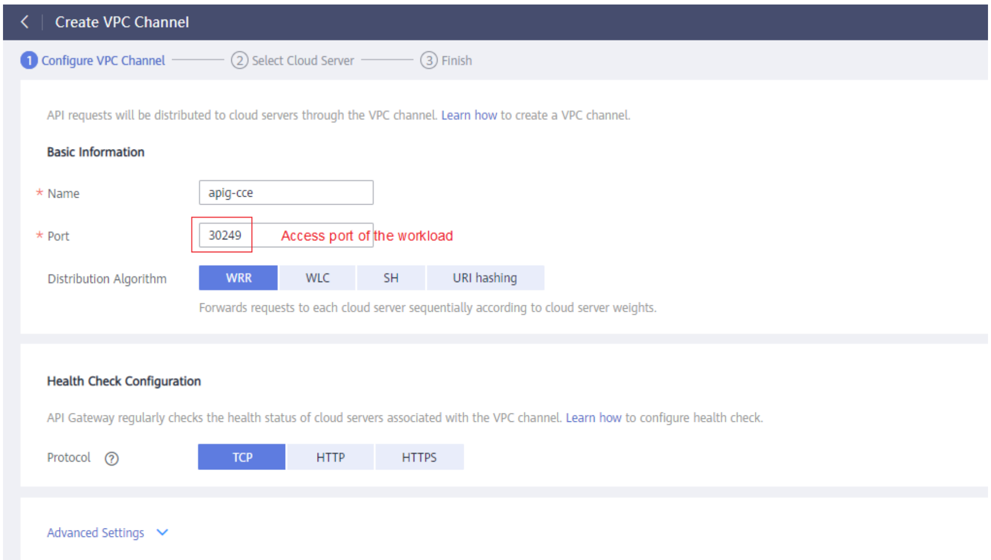
Name	Status	Type	Port	Created	Operation

No data available.

2. Set the parameters according to the following figure and retain the default values for other parameters.

   For details, see **API Gateway User Guide**.

Figure 1-5 Setting the basic VPC channel information



API requests will be distributed to cloud servers through the VPC channel. Learn how to create a VPC channel.

* Name: apig-cce

* Port: 30249 Access port of the workload

Distribution Algorithm: WRR | WLC | SH | URI hashing

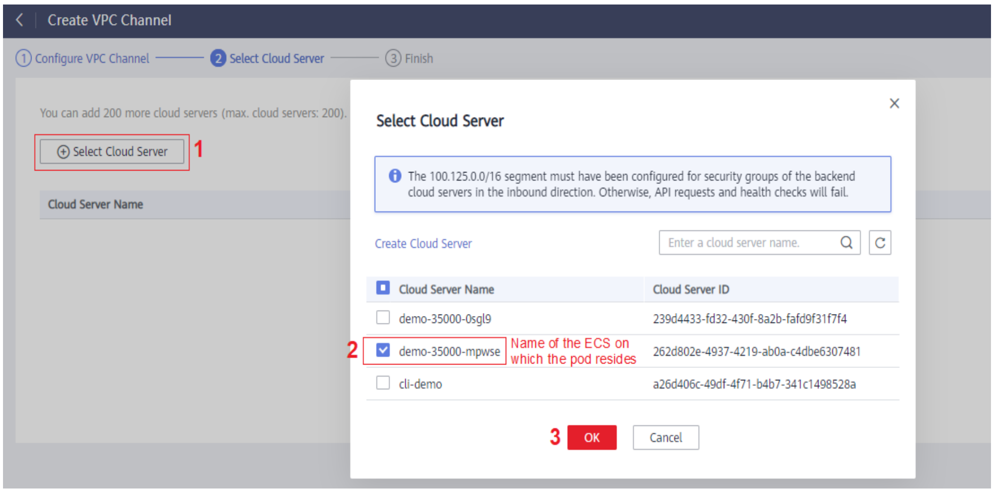
Forwards requests to each cloud server sequentially according to cloud server weights.

API Gateway regularly checks the health status of cloud servers associated with the VPC channel. Learn how to configure health check.

Protocol: TCP | HTTP | HTTPS

Step 3 Add the node that contains the CCE workload you want to access through APIG.

You can add multiple nodes for load balancing.



You can add 200 more cloud servers (max. cloud servers: 200).

Cloud Server Name

Select Cloud Server

The 100.125.0.0/16 segment must have been configured for security groups of the backend cloud servers in the inbound direction. Otherwise, API requests and health checks will fail.

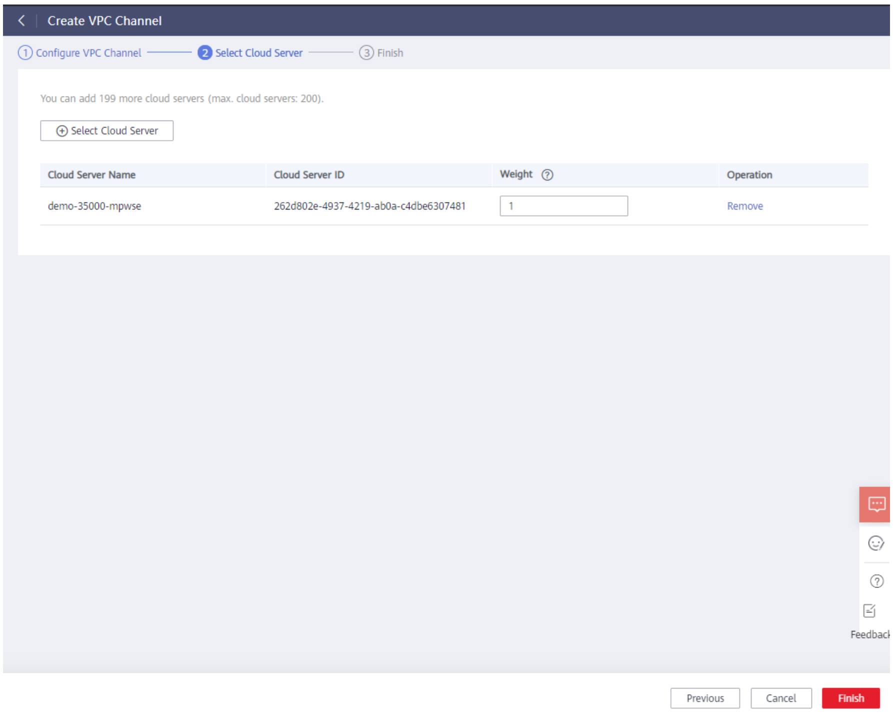
Create Cloud Server

Enter a cloud server name.

	Cloud Server Name	Cloud Server ID
□	demo-35000-0sgl9	239d4433-fd32-430f-8a2b-fafd9f31f7f4
☑	demo-35000-mpwse	262d802e-4937-4219-ab0a-c4dbe6307481
□	cli-demo	a26d406c-49df-4f71-b4b7-341c1498528a

Name of the ECS on which the pod resides

Step 4 Click **Finish**.



You can add 199 more cloud servers (max. cloud servers: 200).

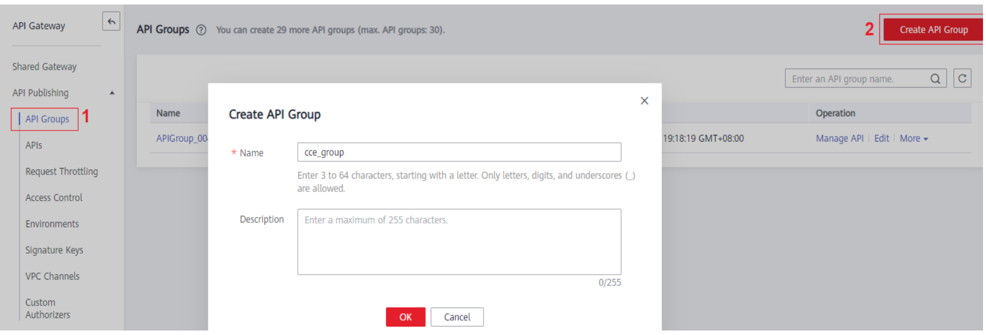
Cloud Server Name	Cloud Server ID	Weight	Operation
demo-35000-mpwse	262d802e-4937-4219-ab0a-c4dbe6307481	1	Remove

----End

Opening an API

Step 1 Create an API group, as shown in **Figure 1-6**.

Figure 1-6 Creating an API group



API Groups You can create 29 more API groups (max. API groups: 30).

Create API Group

* Name: cce_group

Enter 3 to 64 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.

Description: Enter a maximum of 255 characters.

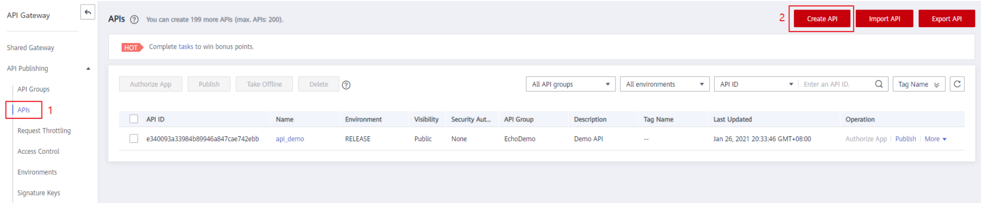
0/255

Step 2 Create an API.

For details, see **API Gateway User Guide**.

1. Click **Create API**.

Figure 1-7 API list



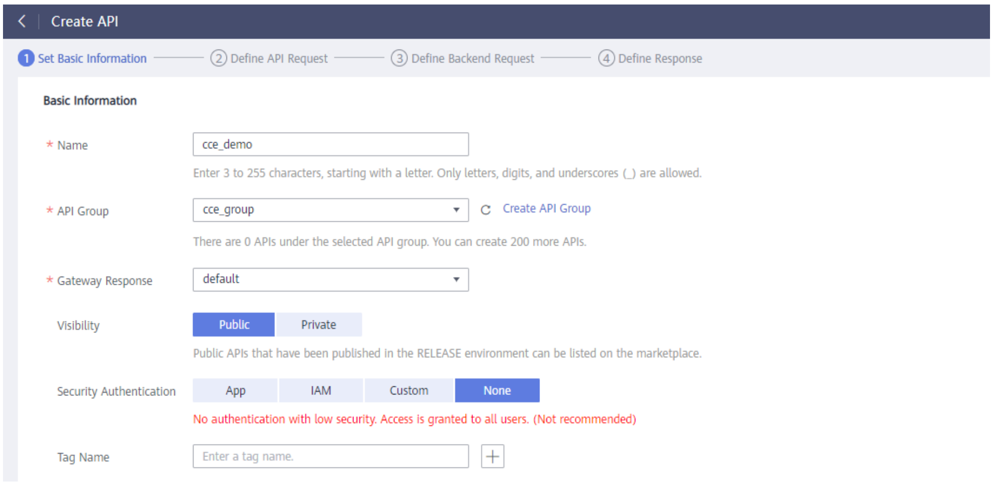
APIs You can create 199 more APIs (max. APIs: 200).

Complete tasks to win bonus points.

API ID	Name	Environment	Visibility	Security Aut...	API Group	Description	Tag Name	Last Updated	Operation
e340093a33984b89946a847cae742ebb	api_demo	RELEASE	Public	None	EchoDemo	Demo API	--	Jan 26, 2021 20:33:46 GMT+08:00	Authorize App | Publish | More

2. Set the basic information of the API.

Figure 1-8 Setting the basic API information



Basic Information

* Name: cce_demo

Enter 3 to 255 characters, starting with a letter. Only letters, digits, and underscores (_) are allowed.

* API Group: cce_group

There are 0 APIs under the selected API group. You can create 200 more APIs.

* Gateway Response: default

Visibility: Public

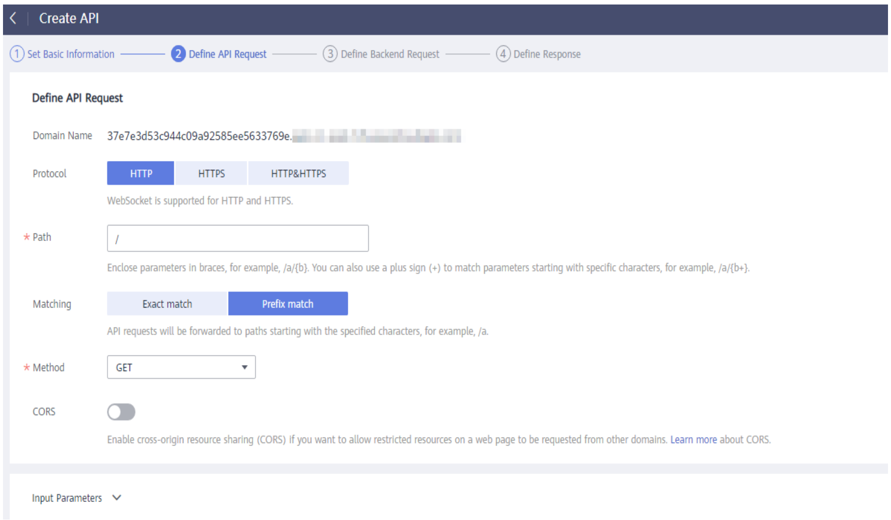
Public APIs that have been published in the RELEASE environment can be listed on the marketplace.

Security Authentication: None

No authentication with low security. Access is granted to all users. (Not recommended)

Tag Name: Enter a tag name.

3. On the **Define API Request** page, set the API request information.



Define API Request

Domain Name 37e7e3d53c944c09a92585ee5633769e.[redacted]

Protocol HTTP

WebSocket is supported for HTTP and HTTPS.

* Path /

Enclose parameters in braces, for example, /a/{b}. You can also use a plus sign (+) to match parameters starting with specific characters, for example, /a/{b+}.

Matching Prefix match

API requests will be forwarded to paths starting with the specified characters, for example, /a.

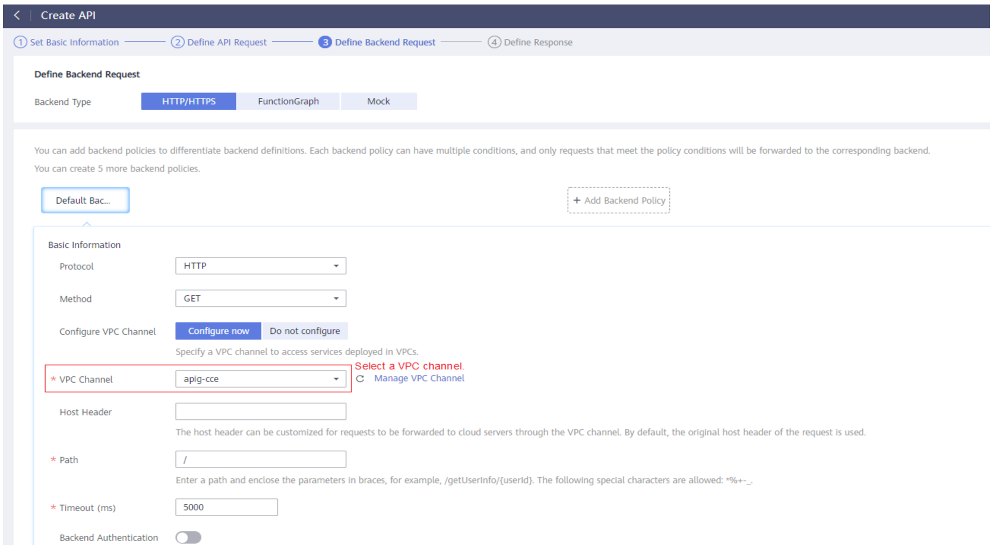
* Method GET

CORS

Enable cross-origin resource sharing (CORS) if you want to allow restricted resources on a web page to be requested from other domains. Learn more about CORS.

4. On the **Define Backend Request** page, set the backend request information.

   If the access mode of the target CCE workload is **NodePort**, select **Configure now**, and select the VPC channel created in **Creating a VPC Channel**. If the access mode is **LoadBalancer**, select **Do not configure**, and enter the **access address and port** of the load balancer. This step uses **NodePort** as an example.



Define Backend Request

Backend Type HTTP/HTTPS

You can add backend policies to differentiate backend definitions. Each backend policy can have multiple conditions, and only requests that meet the policy conditions will be forwarded to the corresponding backend.

You can create 5 more backend policies.

Basic Information

Protocol HTTP

Method GET

Configure VPC Channel Configure now

Specify a VPC channel to access services deployed in VPCs.

* VPC Channel apig-cce

Select a VPC channel.

Host Header

The host header can be customized for requests to be forwarded to cloud servers through the VPC channel. By default, the original host header of the request is used.

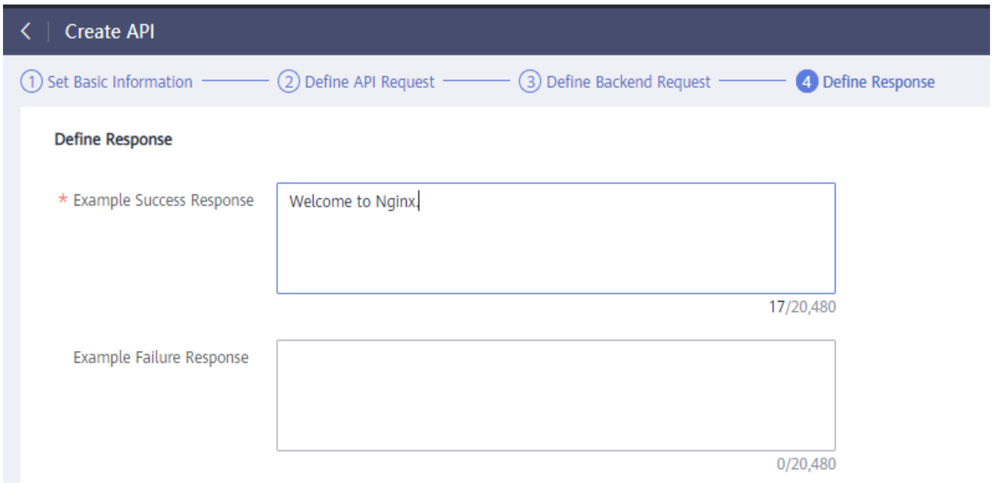
* Path /

Enter a path and enclose the parameters in braces, for example, /getUserInfo/{userId}. The following special characters are allowed: *%+-_.

* Timeout (ms) 5000

Backend Authentication

5. On the **Define Response** page, enter an example success response.



Define Response

* Example Success Response: Welcome to Nginx
17/20,480

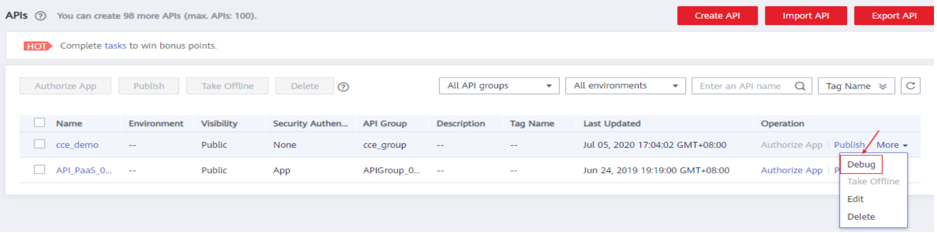
Example Failure Response:
0/20,480

6. Click **Finish**.

Step 3 Debug the API.

1. Click **Debug**.

Figure 1-9 API list



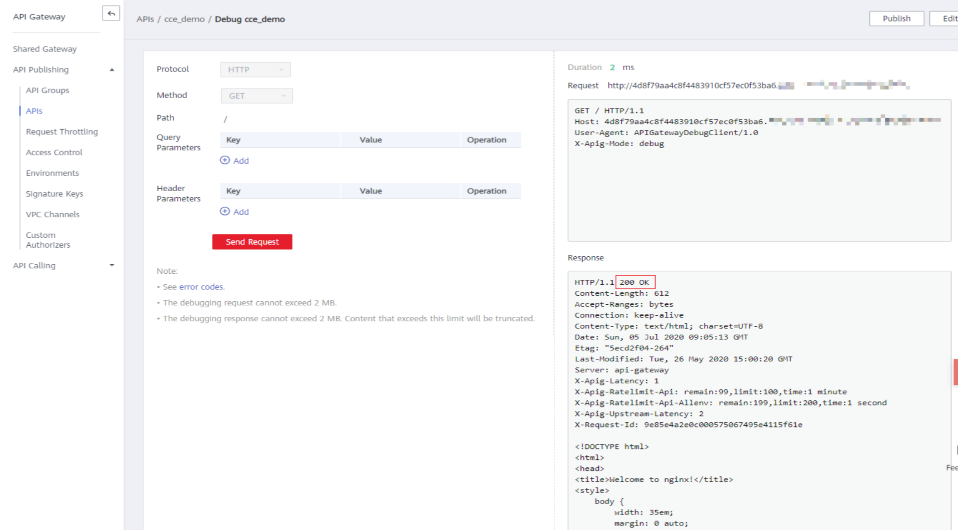
APIs You can create 98 more APIs (max. APIs: 100).

Complete tasks to win bonus points.

☐	Name	Environment	Visibility	Security Authen...	API Group	Description	Tag Name	Last Updated	Operation
☐	cce_demo	--	Public	None	cce_group	--	--	Jul 05, 2020 17:04:02 GMT+08:00	Authorize App | Publish | More
☐	API_PaaS_0...	--	Public	App	APIGroup_0...	--	--	Jun 24, 2019 19:19:00 GMT+08:00	Authorize App | P

2. Debug the API.

Figure 1-10 Debugging the API ("200" indicates that the API is called successfully.)



APIs / cce_demo / Debug cce_demo

Protocol: HTTP

Method: GET

Path: /

	Key	Value	Operation
Query Parameters			
Header Parameters			

Note:

- See error codes.
- The debugging request cannot exceed 2 MB.
- The debugging response cannot exceed 2 MB. Content that exceeds this limit will be truncated.

Duration 2 ms

Request http://4d8f79aa4c8f4483910cf57ec0f53ba6.[redacted]

```
GET / HTTP/1.1
Host: 4d8f79aa4c8f4483910cf57ec0f53ba6.[redacted]
User-Agent: APIGatewayDebugClient/1.0
X-Apig-Mode: debug
```

Response

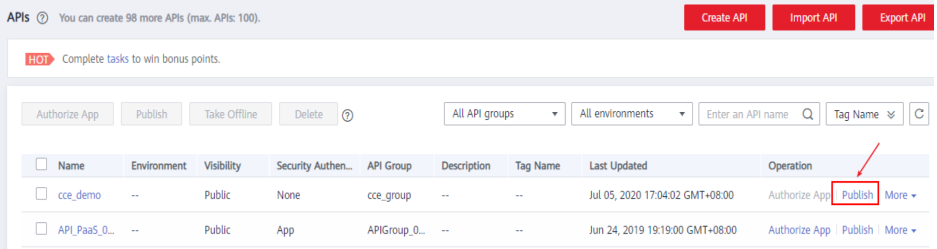
```
HTTP/1.1 200 OK
Content-Length: 612
Accept-Ranges: bytes
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Date: Sun, 05 Jul 2020 09:05:13 GMT
Etag: "5ecd2f04-264"
Last-Modified: Tue, 26 May 2020 15:00:20 GMT
Server: api-gateway
X-Apig-Latency: 1
X-Apig-Ratelimit-Api: remain:99,limit:100,time:1 minute
X-Apig-Ratelimit-Api-Allenv: remain:199,limit:200,time:1 second
X-Apig-Upstream-Latency: 2
X-Request-Id: 9e85e4a2e0c000575067495e4115f61e

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
```

Step 4 Publish the API.

1. Click **Publish**.

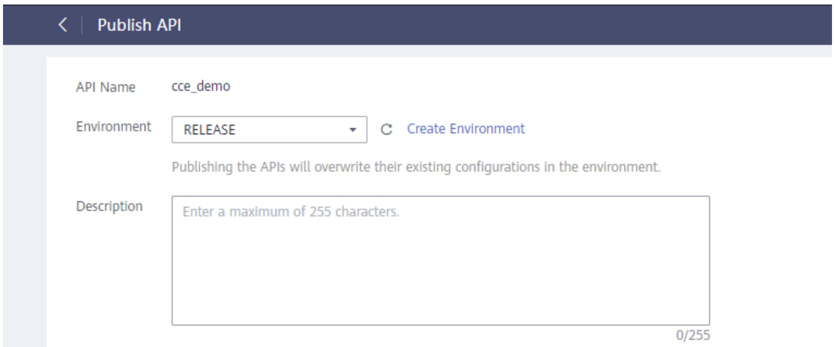
Figure 1-11 API list


APIs ⓘ You can create 98 more APIs (max. APIs: 100).

	Name	Environment	Visibility	Security Authen...	API Group	Description	Tag Name	Last Updated	Operation
□	cce_demo	--	Public	None	cce_group	--	--	Jul 05, 2020 17:04:02 GMT+08:00	Authorize App | Publish | More
□	API_PaaS_0...	--	Public	App	APIGroup_0...	--	--	Jun 24, 2019 19:19:00 GMT+08:00	Authorize App | Publish | More

2. Enter a description.

Figure 1-12 Publishing an API


Publish API

API Name cce_demo

Environment RELEASE

Publishing the APIs will overwrite their existing configurations in the environment.

Description Enter a maximum of 255 characters.

0/255

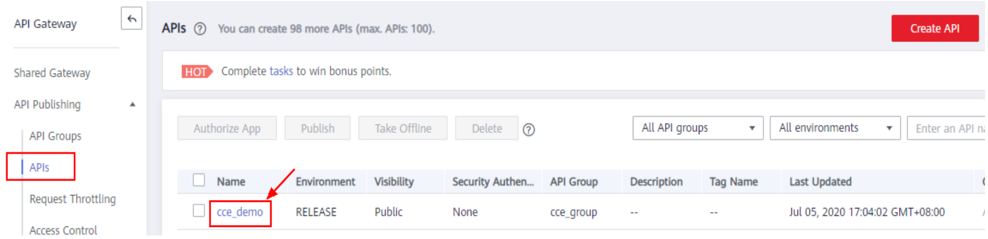
----End

Calling the API

Step 1 In the API list, click the API you created, and copy the URL on the displayed API details page.

1. Go to the API details page.

Figure 1-13 Clicking the name of an API

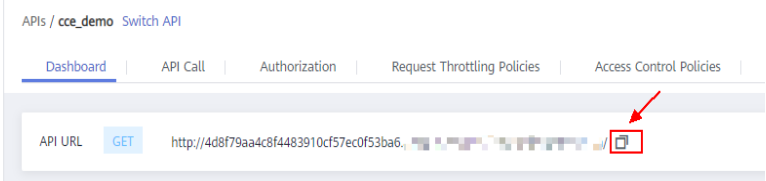


APIs ⓘ You can create 98 more APIs (max. APIs: 100).

	Name	Environment	Visibility	Security Authen...	API Group	Description	Tag Name	Last Updated
□	cce_demo	RELEASE	Public	None	cce_group	--	--	Jul 05, 2020 17:04:02 GMT+08:00

2. Copy the URL on the displayed API details page.

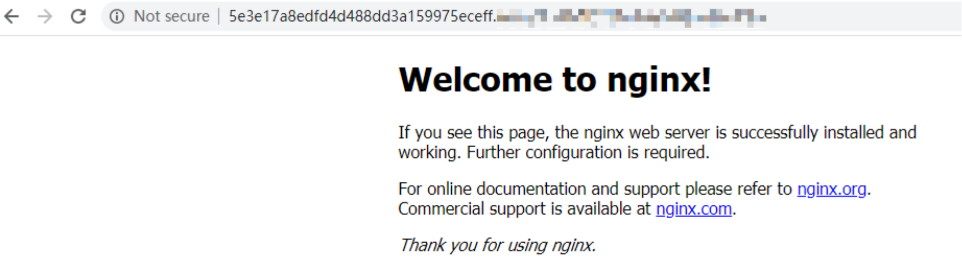
Figure 1-14 Copying the URL


APIs / cce_demo Switch API

API URL GET http://4d8f79aa4c8f4483910cf57ec0f53ba6.[redacted]/

Step 2 Paste the URL to the address bar of a browser. The following page will be displayed if the API request is successful.

To limit the number of API calls that will be received within a specific period, create a request throttling policy and bind it to the API. For more information, see **API Gateway User Guide**.



5e3e17a8edfd4d488dd3a159975eceff.[redacted]

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

----End

2 Selectively Exposing Service Capabilities of a Data Center

The backend services of APIG can be deployed in the following modes:

- Deployed in a VPC and accessible only using private IP addresses.

  You can create a VPC channel on APIG to enable network routing between APIG and the VPC.

- Deployed on the public network and accessible using a public IP address.
- Deployed in an on-premises data center and not accessible using a public IP address.

  If you use a dedicated API gateway, you can set up a connection between your on-premises data center and the gateway.

This section describes the precautions for using APIG to selectively expose APIs of backend services deployed in a local data center.

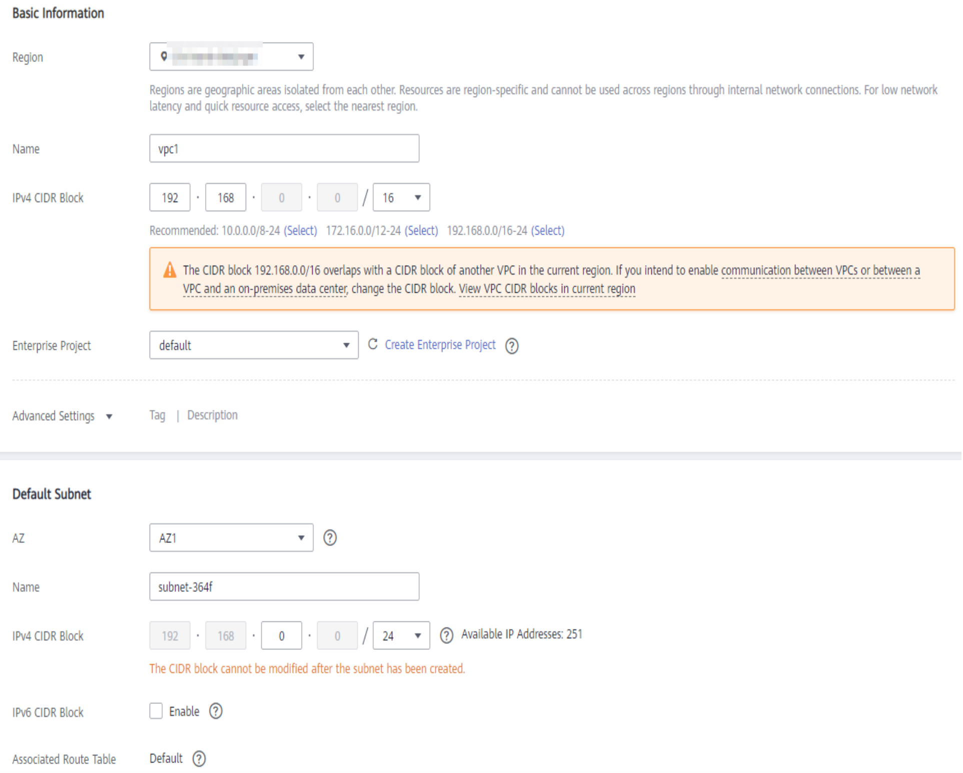
Connecting a Data Center to APIG

Step 1 Create a VPC.

For details, see the section "Creating a VPC" in the *Virtual Private Cloud User Guide*.

To allow APIG to access services in your on-premises data center, bind a VPC to your dedicated gateway, and establish a connection between the data center and VPC.

Figure 2-1 Creating a VPC



Basic Information

Region	[redacted] ▾ Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.
Name	vpc1
IPv4 CIDR Block	192 · 168 · 0 · 0 / 16 ▾ Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select) ⚠ The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you intend to enable communication between VPCs or between a VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region
Enterprise Project	default ▾ C Create Enterprise Project ?
Advanced Settings ▾	Tag | Description

Default Subnet

AZ	AZ1 ▾ ?
Name	subnet-364f
IPv4 CIDR Block	192 · 168 · 0 · 0 / 24 ▾ ? Available IP Addresses: 251 The CIDR block cannot be modified after the subnet has been created.
IPv6 CIDR Block	□ Enable ?
Associated Route Table	Default ?

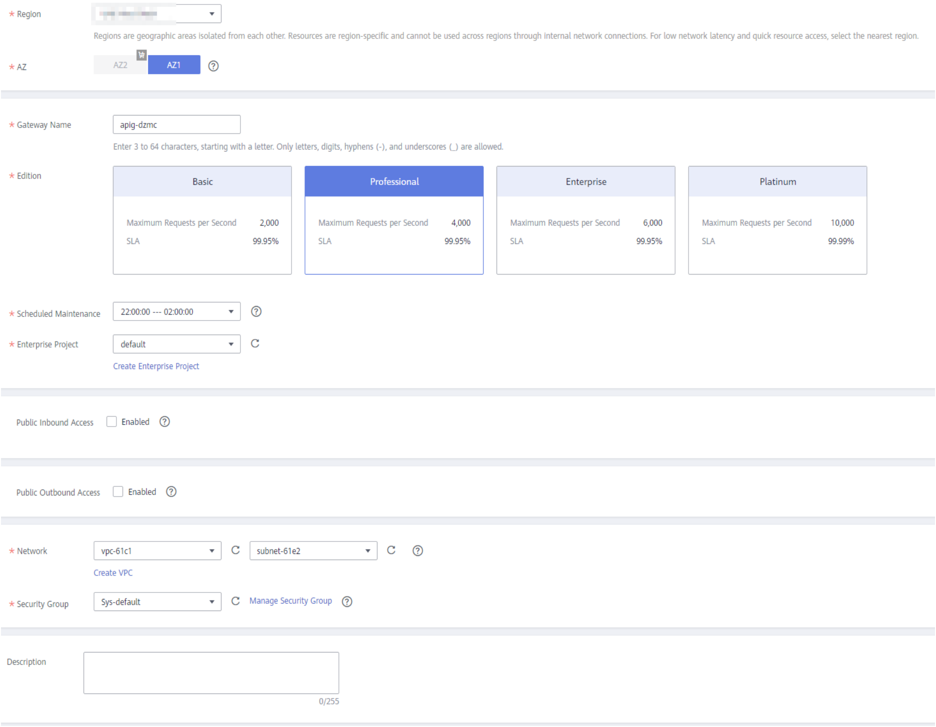
NOTE

- Specify a subnet for your dedicated gateway.
- A connection can be used to connect a local data center to only one VPC. You are advised to bind the same VPC to all your cloud resources to reduce costs.
- If a VPC already exists, you do not need to create a new one.

Step 2 Create a dedicated gateway.

For details, see section "Creating a Dedicated Gateway" in the *User Guide*.

Figure 2-2 Creating a dedicated gateway



* Region

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

* AZ: AZ2 | AZ1

* Gateway Name: apig-dzmc

Enter 3 to 64 characters, starting with a letter. Only letters, digits, hyphens (-), and underscores (_) are allowed.

* Edition

Basic	Professional	Enterprise	Platinum
Maximum Requests per Second 2,000	Maximum Requests per Second 4,000	Maximum Requests per Second 6,000	Maximum Requests per Second 10,000
SLA 99.95%	SLA 99.95%	SLA 99.95%	SLA 99.99%

* Scheduled Maintenance: 22:00:00 --- 02:00:00

* Enterprise Project: default

Create Enterprise Project

Public Inbound Access: □ Enabled

Public Outbound Access: □ Enabled

* Network: vpc-61c1 | subnet-61e2

Create VPC

* Security Group: Sys-default

Manage Security Group

Description:

0/255

Step 3 Enable Direct Connect by referring to the *Direct Connect User Guide*.

1. Create a connection.

   Apply for a connection from your account manager. If you do not have an account manager, contact technical support.

2. Create a virtual gateway.

   The virtual gateway is a logical gateway for accessing the VPC bound to the dedicated gateway.

   > **NOTE**
   >
   > Select the subnet that the dedicated gateway uses, to connect to the VPC. For details about the subnet, go to the gateway details page.

3. Create a virtual interface.

   The virtual interface links the connection with the virtual gateway, enabling connectivity between the connection and the VPC of the dedicated gateway.

   Configure the remote gateway and remote subnet as the gateway and subnet for accessing the open API of your on-premises data center. For example, if the API calling address of your data center is **http://192.168.0.25:80/***{URI}*, configure the remote gateway and remote subnet as those of **192.168.0.25**.

Step 4 Verify the network connectivity.

Create another pay-per-use ECS and select the same VPC, subnet, and security group as the dedicated gateway. If the data center can connect to the ECS, the data center can also connect to the dedicated gateway.

----End

Exposing APIs with the Dedicated Gateway

After you connect the data center to the dedicated gateway, you can expose APIs using the gateway. For details, see "API Opening" in the *User Guide*.

When creating an API, specify the backend address as the API calling address of your data center.

3 Exposing Backend Services Across VPCs

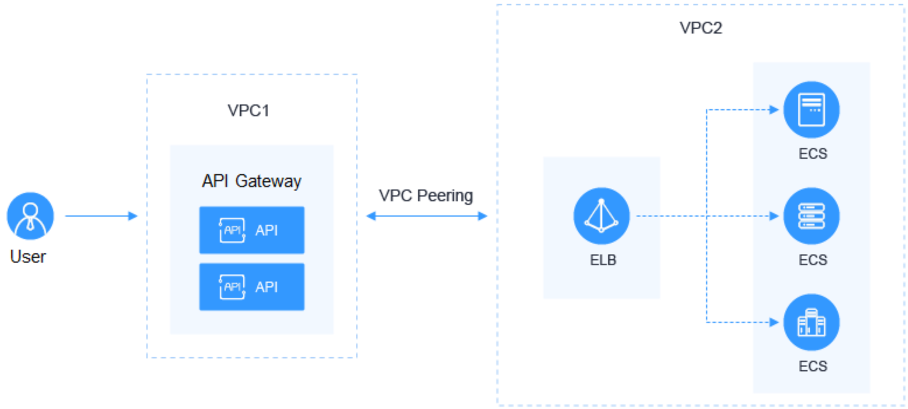
3.1 Introduction

Scenario

If the VPC of your backend server is different from that of your gateway, how do you configure cross-VPC interconnection? This section uses Elastic Load Balance (ELB) as an example to describe how to expose services in a private network load balancer using APIG.

Solution Architecture

Figure 3-1 Exposing backend services across VPCs



Advantages

Without modifying the existing network architecture, you can have all requests directly forwarded to your backend server through flexible configuration.

Restrictions

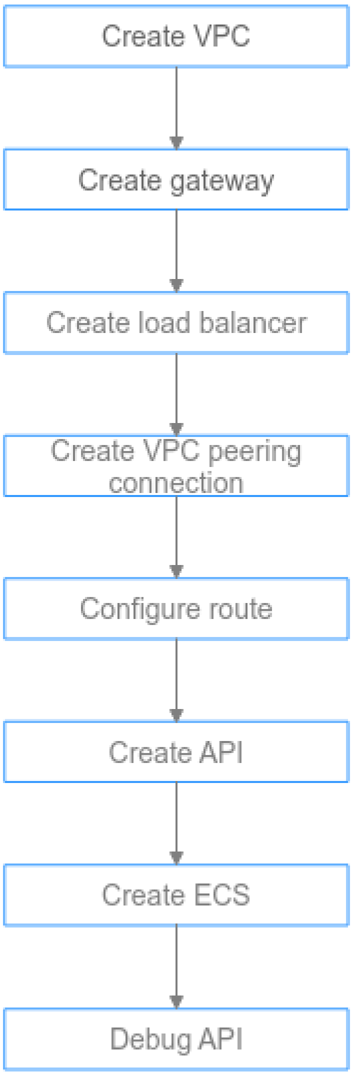
VPC 1, VPC 2, and the VPC CIDR block of your gateway cannot overlap. For details about the VPC CIDR block planning of the gateway, see **Table 3-3**.

3.2 Resource Planning

Table 3-1 Resource planning

Resource	Quantity
VPC	2
Dedicated gateway	1
Load balancer	1
ECS	1

3.3 General Procedure



1. **Create a VPC.**

   Create two VPCs, one for your gateway and the other for your backend service.

2. **Create a gateway.**

   Create a dedicated gateway in VPC 1.

3. **Create a load balancer.**

   Create a load balancer in VPC 2.

4. **Create a VPC peering connection.**

   Create a VPC peering connection to connect VPC 1 and VPC 2.

5. **Configure a route.**

   Configure a route for the dedicated gateway by setting the IP address to the IPv4 CIDR block of VPC 2 where the purchased load balancer is located.

6. **Create an API.**

   Create an API and set the backend service address to the IP address of the load balancer.

7. **Create an ECS.**

   Create an ECS in VPC 2, and deploy the backend service on the ECS.

8. **Debug the API.**

   Verify that the connection to the private network load balancer is successful.

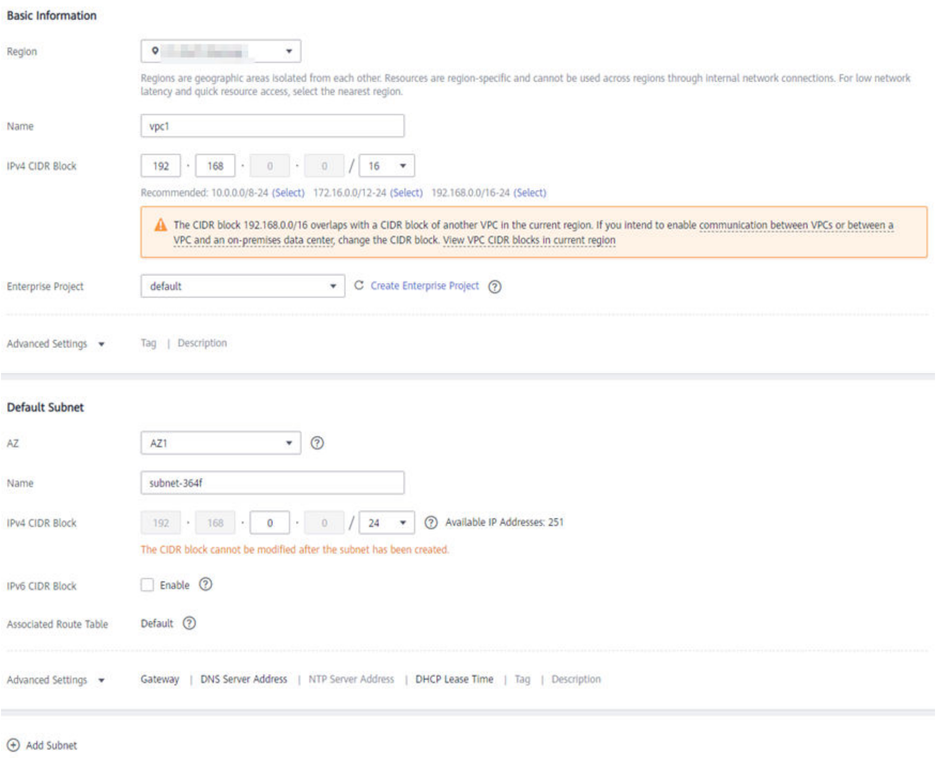
3.4 Implementation Procedure

Creating a VPC

Step 1 Log in to the network console.

Step 2 In the navigation pane, choose **Virtual Private Cloud** > **My VPCs**.

Step 3 On the **Virtual Private Cloud** page, click **Create VPC**, and configure the parameters by referring to **Table 3-2** and **Table 3-3**. For details, see sections "Creating a VPC" and "Creating a Subnet for the VPC" in the *Virtual Private Cloud User Guide*.



Basic Information

Region: [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

Name: vpc1

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)

The CIDR block 192.168.0.0/16 overlaps with a CIDR block of another VPC in the current region. If you intend to enable communication between VPCs or between a VPC and an on-premises data center, change the CIDR block. View VPC CIDR blocks in current region

Enterprise Project: default

Advanced Settings: Tag | Description

Default Subnet

AZ: AZ1

Name: subnet-364f

IPv4 CIDR Block: 192 . 168 . 0 . 0 / 24 Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

IPv6 CIDR Block: □ Enable

Associated Route Table: Default

Advanced Settings: Gateway | DNS Server Address | NTP Server Address | DHCP Lease Time | Tag | Description

Table 3-2 Configuration information

Parameter	Description
Region	Select a region.
Name	Enter **VPC1**. This VPC will be used to run a gateway.
Enterprise Project	Select **default**.
AZ	The AZ to which the subnet belongs. Select **AZ1**.
Name	A subnet is automatically created when you create a VPC.

Table 3-3 VPC CIDR block planning

VPC 1	VPC of APIG	VPC 2
10.X	172.31.0.0/16	Must be different from VPC 1 and the VPC of the gateway.
172.X	192.168.0.0/16	
192.X	172.31.0.0/16	

Step 4 Click **Create Now**.

Step 5 Repeat **Step 3** to **Step 4** to create **VPC2** for running your backend service.

----End

Creating a Gateway

Step 1 Log in to the APIG console.

Step 2 In the navigation pane, choose **Dedicated Gateways**.

Step 3 Click **Create Dedicated Gateway**.

Table 3-4 Gateway information

Parameter	Description
Billing Mode	Billing mode of the gateway. Select **Pay-per-use**.
Region	Select the region where the gateway is located. It must be the same as the region of VPC 1.
AZ	The AZ where the gateway is located. Select **AZ1**.
Gateway Name	Enter a name that conforms to specific rules to facilitate search.
Edition	Select **Professional**. The edition cannot be changed after the gateway is created.
Scheduled Maintenance	Select a time period when the gateway can be maintained by technical support engineers. A period with low service traffic is recommended. For this example, retain the default value **22:00:00---02:00:00**.
Enterprise Project	Select the enterprise project to which the gateway belongs. For this example, retain the default value **default**.
Network	Select **VPC 1** and a subnet.
Security Group	Click **Manage Security Groups** and create a security group. Ensure that you have selected **default** for **Enterprise Project**.
Description	Description of the gateway.

Step 4 Click **Next**.

Step 5 If the gateway configurations are correct, read and confirm your acceptance of the customer agreement and privacy statement, and click **Pay Now**.

----End

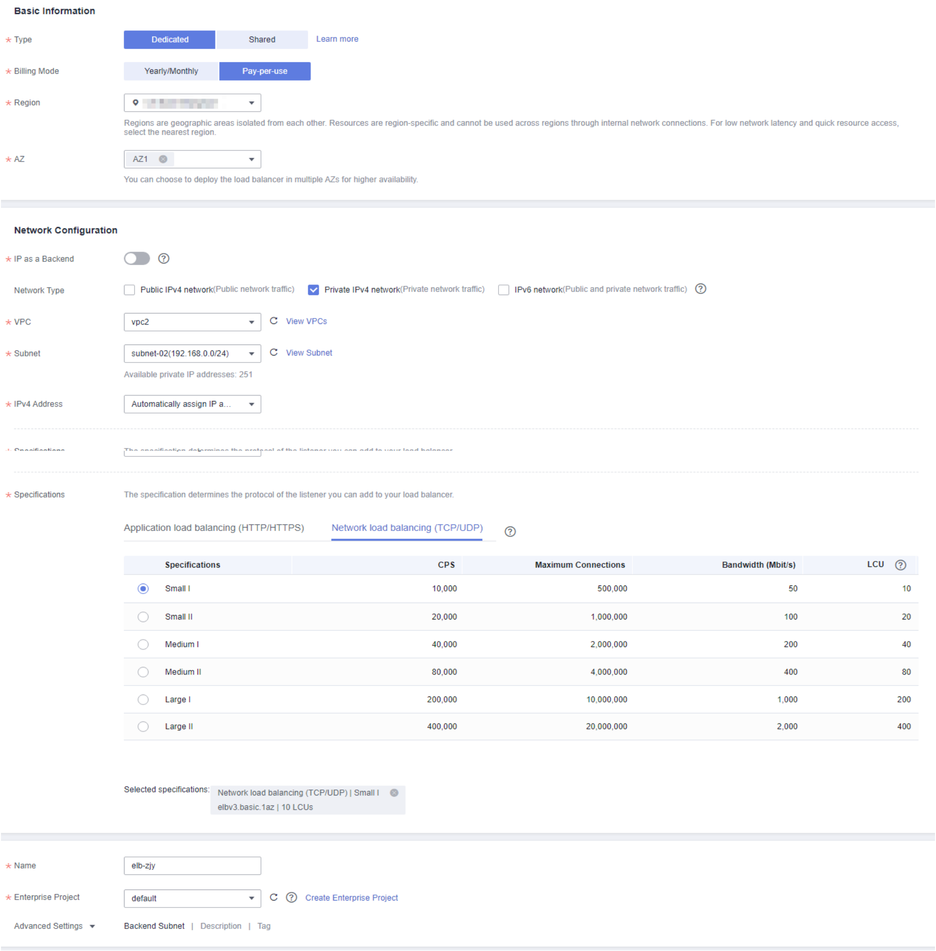
Buying a Load Balancer

Step 1 Log in to the network console.

Step 2 In the navigation pane, choose **Elastic Load Balance** > **Load Balancers**.

Step 3 Click **Buy Elastic Load Balancer**.

Step 4 Configure the load balancer information. For details, see section **Load Balancer** in the *Elastic Load Balance User Guide*.



Basic Information

- * Type: [✓ Dedicated] Shared — Learn more
- * Billing Mode: Yearly/Monthly [✓ Pay-per-use]
- * Region: Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.
- * AZ: AZ1 — You can choose to deploy the load balancer in multiple AZs for higher availability.

Network Configuration

- * IP as a Backend: off
- Network Type: ☐ Public IPv4 network(Public network traffic) ☑ Private IPv4 network(Private network traffic) ☐ IPv6 network(Public and private network traffic)
- * VPC: vpc2 — View VPCs
- * Subnet: subnet-02(192.168.0.0/24) — View Subnet — Available private IP addresses: 251
- * IPv4 Address: Automatically assign IP a...
- * Specifications: The specification determines the protocol of the listener you can add to your load balancer.

Application load balancing (HTTP/HTTPS) | [✓ Network load balancing (TCP/UDP)]

	Specifications	CPS	Maximum Connections	Bandwidth (Mbit/s)	LCU
●	Small I	10,000	500,000	50	10
○	Small II	20,000	1,000,000	100	20
○	Medium I	40,000	2,000,000	200	40
○	Medium II	80,000	4,000,000	400	80
○	Large I	200,000	10,000,000	1,000	200
○	Large II	400,000	20,000,000	2,000	400

Selected specifications: Network load balancing (TCP/UDP) | Small I
elbv3.basic.1az | 10 LCUs

- * Name: elb-zjy
- * Enterprise Project: default — Create Enterprise Project
- Advanced Settings: Backend Subnet | Description | Tag

Table 3-5 Load balancer parameters

Parameter	Description
Type	Type of the load balancer.
Billing Mode	By default, **Pay-per-use** is selected.
Region	Select the region where the load balancer is located. It must be the same as the region of VPC 2.
AZ	The AZ where the load balancer is located. Select **AZ1**.
Network Type	Select **Private IPv4 Network**.
VPC	Select **VPC 2**.
Subnet	Select a subnet.
Specification	Select **Network load balancing**.
Name	Enter a load balancer name that conforms to specific rules to facilitate search.

Parameter	Description
Enterprise Project	Select **default**.

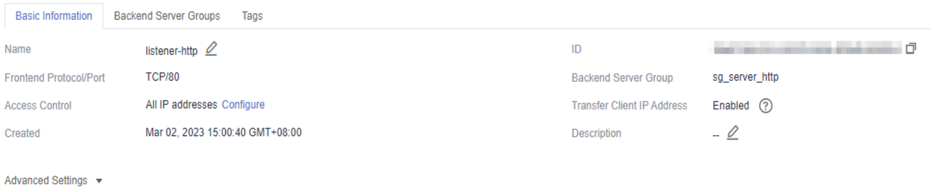
Step 5 Click **Next**.

Step 6 Confirm the configuration and click **Submit**.

Step 7 Add a listener.

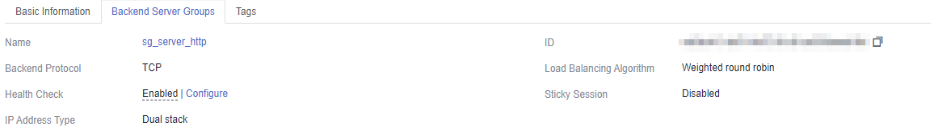
1. Click the name of the load balancer. On the **Listeners** tab page, click **Add Listener**.
2. Configure the listener name, frontend protocol, and port, and click **Next**.
3. Configure the backend server group name, backend protocol, and load balancing algorithm. Then click **Next**.
4. Add backend servers and click **Next**.
5. Click **Submit** The following figure shows the configuration.

Figure 3-2 Listener information



Name: listener-http
Frontend Protocol/Port: TCP/80
Access Control: All IP addresses Configure
Created: Mar 02, 2023 15:00:40 GMT+08:00
ID: [redacted]
Backend Server Group: sg_server_http
Transfer Client IP Address: Enabled
Description: --

Figure 3-3 Backend server group information



Name: sg_server_http
Backend Protocol: TCP
Health Check: Enabled | Configure
IP Address Type: Dual stack
ID: [redacted]
Load Balancing Algorithm: Weighted round robin
Sticky Session: Disabled

----End

Creating a VPC Peering Connection

Step 1 Log in to the network console.

Step 2 In the navigation pane, choose **Virtual Private Cloud** > **VPC Peering Connections**.

Step 3 Click **Create VPC Peering Connection** and configure the parameters.

Table 3-6 Configuring a VPC peering connection

Parameter	Description
Name	Enter a VPC peering connection name that conforms to specific rules to facilitate search.

Parameter	Description
Local VPC	Select **VPC 1**.
Account	By default, **My account** is selected.
Peer Project	Select a project
Peer VPC	Select **VPC 2**.

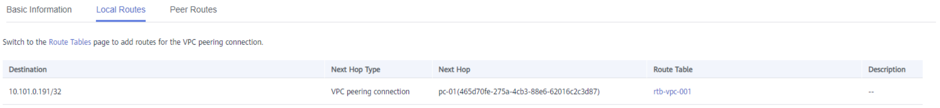
Step 4 Click **OK**.

Step 5 In the displayed dialog box, click **Add Route** to go to the VPC peering connection details page.

Step 6 On the **Local Routes** tab page, click **Route Tables**.

1. Under **Routes**, click **Add Route**.
2. In the displayed dialog box, enter the route information.
   - **Destination**: Enter the service address displayed on the details page of the **load balancer**.
   - **Next Hop Type**: Select **VPC peering connection**.
3. Click **OK**.

Figure 3-4 Local routes



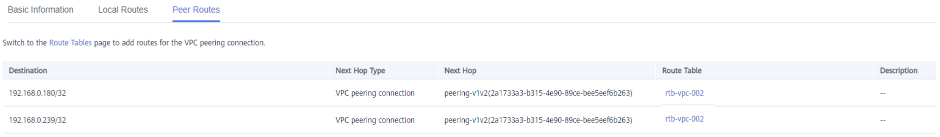
Switch to the Route Tables page to add routes for the VPC peering connection.

Destination	Next Hop Type	Next Hop	Route Table	Description
10.101.0.191/32	VPC peering connection	pc-01(465d70fe-275a-4cb3-88e6-62016c2c3d87)	rtb-vpc-001	--

Step 7 Go to the **Peer Routes** tab page, and click **Route Tables**.

1. Under **Routes**, click **Add Route**.
2. In the displayed dialog box, enter the route information.
   - **Destination**: Enter the private outbound address displayed on the details page of the **dedicated gateway**.
   - **Next Hop Type**: Select **VPC peering connection**.
3. Click **OK**.

Figure 3-5 Peer routes



Switch to the Route Tables page to add routes for the VPC peering connection.

Destination	Next Hop Type	Next Hop	Route Table	Description
192.168.0.180/32	VPC peering connection	peering-v1v2(2a1733a3-b315-4e90-89ce-bee5eef6b263)	rtb-vpc-002	--
192.168.0.239/32	VPC peering connection	peering-v1v2(2a1733a3-b315-4e90-89ce-bee5eef6b263)	rtb-vpc-002	--

----End

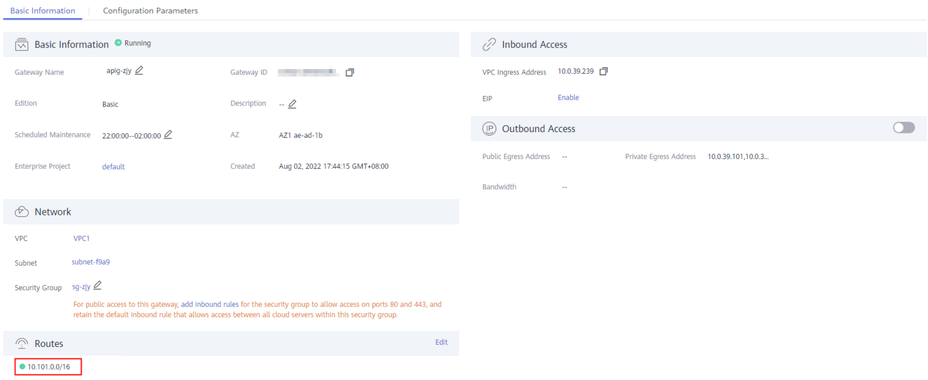
Configuring a Route

Step 1 Log in to the APIG console.

Step 2 In the navigation pane, choose **Dedicated Gateways**.

Step 3 Click the name of the created **dedicated gateway** or click **Access Console**.

Step 4 Click **Change** in the **Routes** area, enter the IPv4 CIDR block of VPC 2 where the load balancer you purchased is located.



Gateway Name apig-zjy
Gateway ID [redacted]
Edition Basic
Description --
Scheduled Maintenance 22:00:00--02:00:00
AZ AZ1 ae-ad-1b
Enterprise Project default
Created Aug 02, 2022 17:44:15 GMT+08:00

VPC Ingress Address 10.0.39.239
EIP Enable

Public Egress Address --
Private Egress Address 10.0.39.101,10.0.3...
Bandwidth --

VPC VPC1
Subnet subnet-f9a9
Security Group sg-zjy
For public access to this gateway, add inbound rules for the security group to allow access on ports 80 and 443, and retain the default inbound rule that allows access between all cloud servers within this security group.

10.101.0.0/16

Step 5 Click **Save**.

----End

Creating an API

Step 1 Log in to the APIG console.

Step 2 In the navigation pane, choose **Dedicated Gateways**. Then click a gateway name or click **Access Console**.

Step 3 In the navigation pane, choose **API Publishing** > **APIs**. Then click **Create API**.

Step 4 Configure the basic information and click **Next**.

Table 3-7 Frontend configuration

Parameter	Description
API Name	Enter a name that conforms to specific rules to facilitate search.
Group	The default option is **DEFAULT**.
Gateway Response	Select a response to be displayed if the gateway fails to process an API request. The default gateway response is **default**.
Authentication Mode	API authentication mode. Select **None**.

Step 5 Define the API request parameters and click **Next**.

Table 3-8 Parameters for defining API requests

Parameter	Description
Domain Name	The system automatically allocates a debugging domain name to each API group for internal testing. The domain name can be accessed 1000 times a day.
Protocol	Request protocol of the API. Set this parameter to **HTTPS**.
Path	Path for requesting the API.
Method	Request method of the API. Set this parameter to **GET**.

Step 6 Define the backend service parameters and click **Next**.

Table 3-9 Parameters for defining an HTTP/HTTPS backend service

Parameter	Description
Protocol	Set this parameter to **HTTP**.
Method	Request method of the API. Set this parameter to **GET**.
VPC Channel	Select **Skip**, and enter the service address of the load balancer you created.
Path	Path of the backend service.

Step 7 Define the response and click **Finish**.

----End

Buying an ECS

Step 1 Log in to the cloud server console.

Step 2 Click **Buy ECS**.

Step 3 Configure the basic settings and click **Next: Configure Network**.

Table 3-10 Basic settings

Parameter	Description
Billing Mode	Select **Pay-per-use**.
Region	Select the region where the ECS is located. It must be the same as the region of VPC 2.
AZ	Select the AZ where the ECS is located.
Specifications	Select specifications that match your service planning.

Parameter	Description
Image	Select an image that matches your service planning.

Step 4 Configure the network settings and click **Next: Configure Advanced Settings**.

Table 3-11 Network settings

Parameter	Description
Network	Select **VPC 2** and a subnet.
Security Group	Select the security group created for the **dedicated gateway**.
EIP	Select **Not required**.

Step 5 Configure advanced settings and click **Next: Confirm**.

Table 3-12 Advanced settings

Parameter	Description
ECS Name	Enter a name that conforms to specific rules to facilitate search.
Login Mode	Credential for logging in to the ECS. The default option is **Password**.
Username	The default user is **root**.
Password	Set a password for logging in to the ECS.
Confirm Password	Enter the password again.

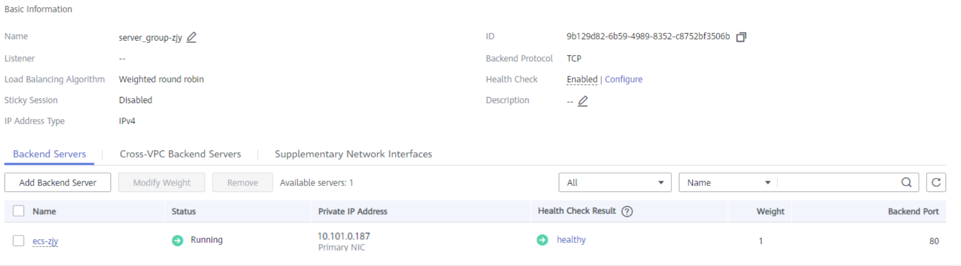
Step 6 Confirm the configuration and select enterprise project **default**.

Step 7 Read and confirm your acceptance of the agreement. Then click **Submit**.

----End

Debugging the API

Step 1 On the **Backend Server Groups** tab page of **the load balancer**, add **the ECS**.



Basic Information

Name	server_group-zjy	ID	9b129d82-6b59-4989-8352-c8752bf3506b
Listener	--	Backend Protocol	TCP
Load Balancing Algorithm	Weighted round robin	Health Check	Enabled | Configure
Sticky Session	Disabled	Description	--
IP Address Type	IPv4		

Available servers: 1

Name	Status	Private IP Address	Health Check Result	Weight	Backend Port
ecs-zjy	Running	10.101.0.187 Primary NIC	healthy	1	80

Step 2 Start the ECS.

Step 3 Go to the **APIs** page of the **dedicated gateway**, choose **API Publishing** > **APIs**, and then choose **More** > **Debug** in the row that contains **the API you created**.

Step 4 Enter the request parameters and click **Send Request**.

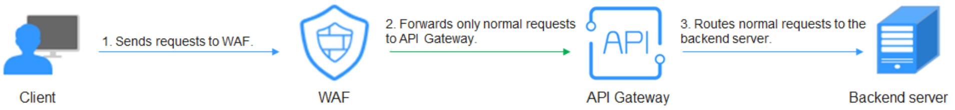
If the status code is **200**, the debugging is successful.

----End

4 Interconnecting with WAF

To protect API Gateway and your backend servers from malicious attacks, deploy Web Application Firewall (WAF) between API Gateway and the external network.

Figure 4-1 Access to a backend server

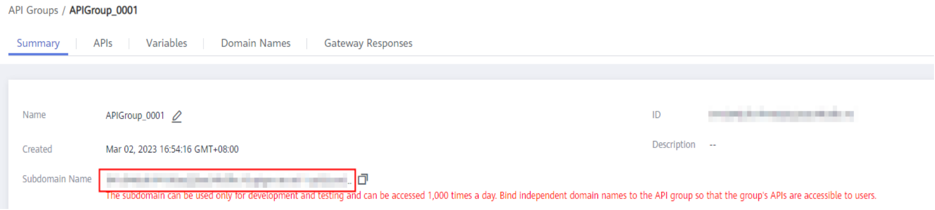

1. Sends requests to WAF.
2. Forwards only normal requests to API Gateway.
3. Routes normal requests to the backend server.
API
Client
WAF
API Gateway
Backend server

(Recommended) Solution 1: Register API Group Debugging Domain Name on WAF and Use the Domain Name to Access the Backend Service

API groups provide services using domain names for high scalability.

Step 1 Create an API group in a gateway, record the domain name, and create an API in the group.

Figure 4-2 Creating an API group and recording the subdomain name



Name APIGroup_0001

Created Mar 02, 2023 16:54:16 GMT+08:00

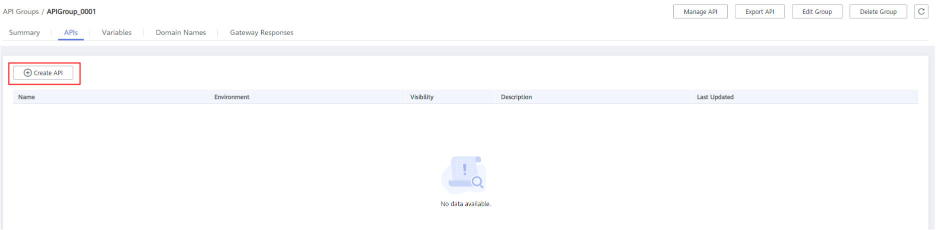
Subdomain Name [redacted]

The subdomain can be used only for development and testing and can be accessed 1,000 times a day. Bind independent domain names to the API group so that the group's APIs are accessible to users.

ID [redacted]

Description --

Figure 4-3 Creating an API



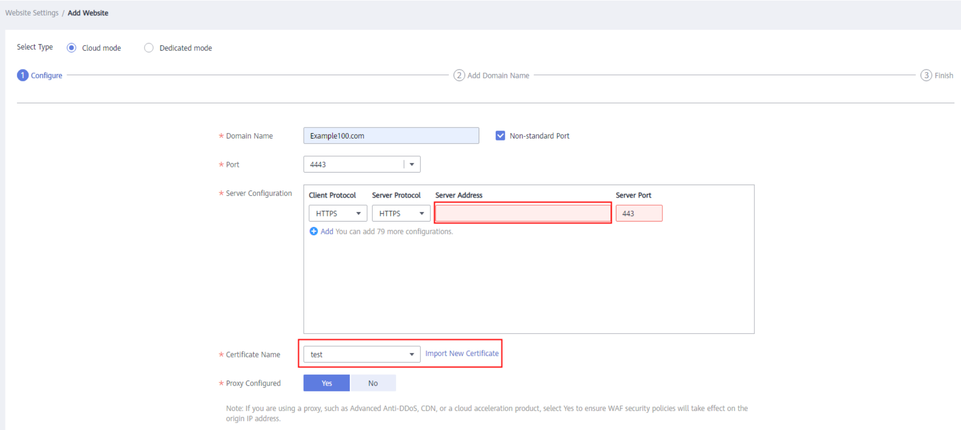
Name	Environment	Visibility	Description	Last Updated

No data available.

Step 2 Go to the WAF console, and add a domain name by configuring **Server Address** as the API group domain name and adding a certificate. For details, see section "Connection Process (Cloud Mode)" in the *Web Application Firewall User Guide*.

NOTE

You can use a public network client to access WAF with its domain name. WAF then uses the same domain name to forward your requests to API Gateway. There is no limit on the number of requests that API Gateway can receive for the domain name.



Website Settings / Add Website

Select Type ● Cloud mode ○ Dedicated mode

1 Configure — 2 Add Domain Name — 3 Finish

* Domain Name: Example100.com ☑ Non-standard Port

* Port: 4443

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port
HTTPS	HTTPS		443

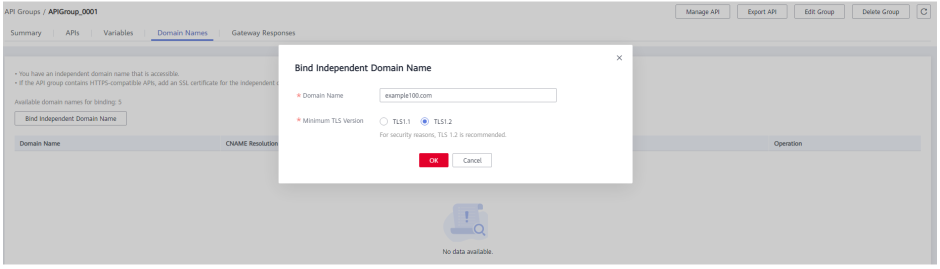
Add You can add 79 more configurations.

* Certificate Name: test Import New Certificate

* Proxy Configured: Yes No

Note: If you are using a proxy, such as Advanced Anti-DDoS, CDN, or a cloud acceleration product, select Yes to ensure WAF security policies will take effect on the origin IP address.

Step 3 On the gateway details page, bind the domain name to the API group.



API Groups / APIGroup_0001

- You have an independent domain name that is accessible.
- If the API group contains HTTPS-compatible APIs, add an SSL certificate for the independent

Available domain names for binding: 5

Domain Name	CNAME Resolution	Operation

No data available.

Bind Independent Domain Name

* Domain Name: example100.com

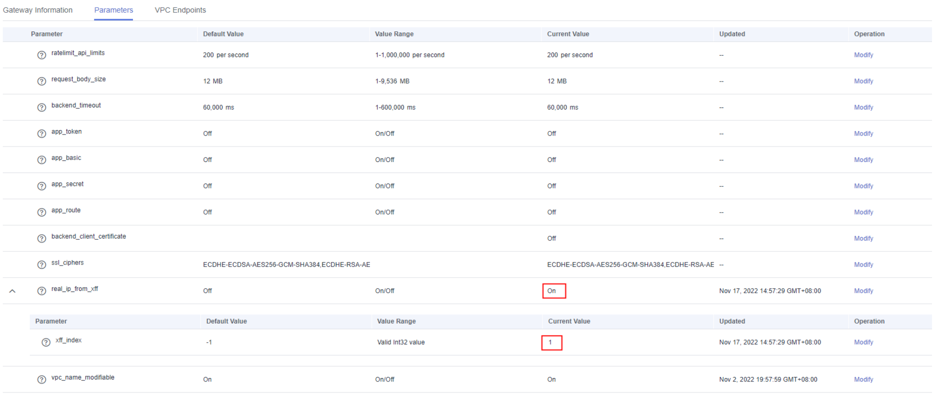
* Minimum TLS Version ○ TLS1.1 ● TLS1.2

For security reasons, TLS 1.2 is recommended.

Step 4 Enable **real_ip_from_xff** and set the parameter value to **1**.

NOTE

When a user accesses WAF using a public network client, WAF records the actual IP address of the user in the HTTP header **X-Forwarded-For**. API Gateway resolves the actual IP address of the user based on the header.



	Parameter	Default Value	Value Range	Current Value	Updated	Operation
	ratelimit_api_limits	200 per second	1-1,000,000 per second	200 per second	--	Modify
	request_body_size	12 MB	1-9,536 MB	12 MB	--	Modify
	backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	--	Modify
	app_token	Off	On/Off	Off	--	Modify
	app_basic	Off	On/Off	Off	--	Modify
	app_secret	Off	On/Off	Off	--	Modify
	app_route	Off	On/Off	Off	--	Modify
	backend_client_certificate			Off	--	Modify
	ssl_ciphers	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AE		ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AE	--	Modify
^	real_ip_from_xff	Off	On/Off	On	Nov 17, 2022 14:57:29 GMT+08:00	Modify
	vpc_name_modifiable	On	On/Off	On	Nov 2, 2022 19:57:59 GMT+08:00	Modify

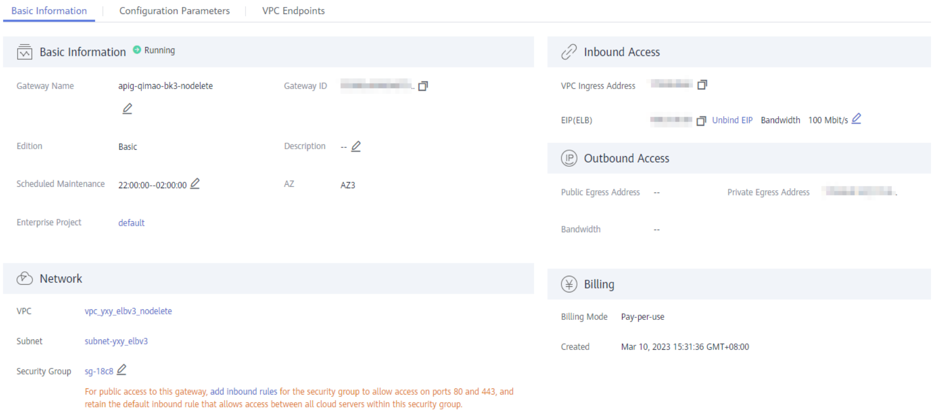
Parameter	Default Value	Value Range	Current Value	Updated	Operation
xff_index	-1	Valid Int32 value	1	Nov 17, 2022 14:57:29 GMT+08:00	Modify

----End

Solution 2: Forward Requests Through the DEFAULT Group and Use Gateway Inbound Access Address to Access the Backend Service from WAF

Step 1 View the inbound access addresses of your gateway. There is no limit on the number of times the API gateway can be accessed using an IP address.

- **VPC Ingress Address**: VPC access address
- **EIP**: public network access address



Basic Information Running

Gateway Name apig-qimao-bk3-nodelete

Gateway ID [redacted]

Edition Basic

Description --

Scheduled Maintenance 22:00:00--02:00:00

AZ AZ3

Enterprise Project default

Network

VPC vpc_yxy_elbv3_nodelete

Subnet subnet-yxy_elbv3

Security Group sg-18c8

For public access to this gateway, add inbound rules for the security group to allow access on ports 80 and 443, and retain the default inbound rule that allows access between all cloud servers within this security group.

Inbound Access

VPC Ingress Address [redacted]

EIP(ELB) [redacted] Unbind EIP Bandwidth 100 Mbit/s

Outbound Access

Public Egress Address --

Private Egress Address [redacted]

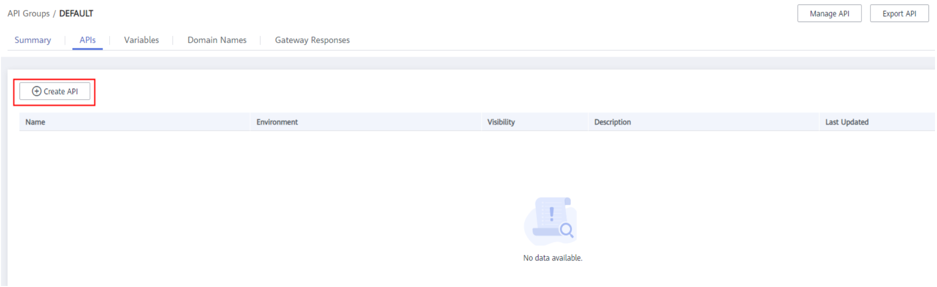
Bandwidth --

Billing

Billing Mode Pay-per-use

Created Mar 10, 2023 15:31:36 GMT+08:00

Step 2 Create an API in the **DEFAULT** group.



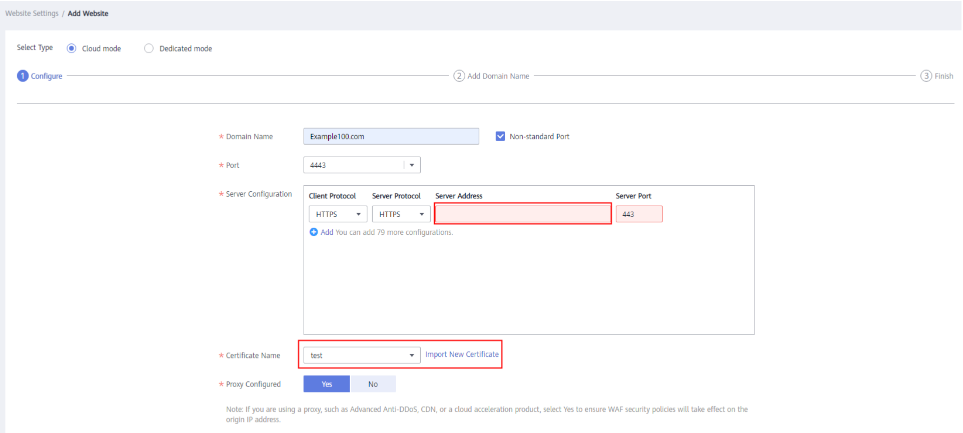
Name	Environment	Visibility	Description	Last Updated

No data available.

Step 3 Go to the WAF console, add a domain name by configuring **Server Address** as an **inbound access address** of your API gateway and adding a certificate, and then copy the WAF back-to-source IP addresses. For details, see .

NOTE

- If WAF and your gateway are in the same VPC, set **Server Address** to the VPC access address.
- If your gateway is bound with an EIP, set **Server Address** to the EIP.


Website Settings / Add Website

Select Type ● Cloud mode ○ Dedicated mode

1 Configure — 2 Add Domain Name — 3 Finish

* Domain Name: Example100.com ☑ Non-standard Port

* Port: 4443

* Server Configuration:

Client Protocol	Server Protocol	Server Address	Server Port
HTTPS	HTTPS		443

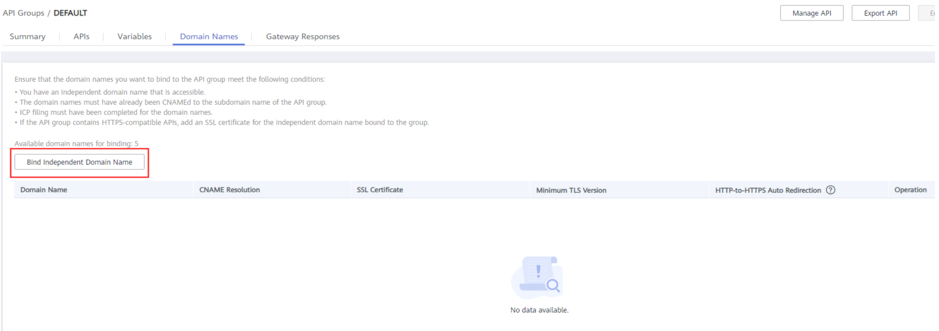
Add You can add 79 more configurations.

* Certificate Name: test Import New Certificate

* Proxy Configured: Yes No

Note: If you are using a proxy, such as Advanced Anti-DDoS, CDN, or a cloud acceleration product, select Yes to ensure WAF security policies will take effect on the origin IP address.

Step 4 On the gateway details page, bind the domain name to the **DEFAULT** group.


API Groups / DEFAULT

Ensure that the domain names you want to bind to the API group meet the following conditions:
- You have an independent domain name that is accessible.
- The domain names must have already been CNAMEd to the subdomain name of the API group.
- ICP filing must have been completed for the domain names.
- If the API group contains HTTPS-compatible APIs, add an SSL certificate for the independent domain name bound to the group.

Available domain names for binding: 5

Bind Independent Domain Name

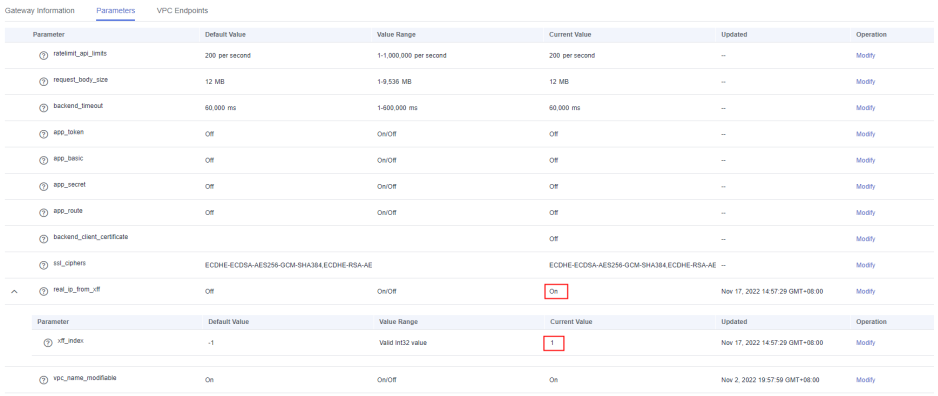
Domain Name	CNAME Resolution	SSL Certificate	Minimum TLS Version	HTTP-to-HTTPS Auto Redirection	Operation

No data available.

Step 5 Enable **real_ip_from_xff** and set the parameter value to **1**.

NOTE

When a user accesses WAF using a public network client, WAF records the actual IP address of the user in the HTTP header **X-Forwarded-For**. API Gateway resolves the actual IP address of the user based on the header.



Parameter	Default Value	Value Range	Current Value	Updated	Operation
ratelimit_api_limits	200 per second	1-1,000,000 per second	200 per second	--	Modify
request_body_size	12 MB	1-9,536 MB	12 MB	--	Modify
backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	--	Modify
app_token	Off	On/Off	Off	--	Modify
app_basic	Off	On/Off	Off	--	Modify
app_secret	Off	On/Off	Off	--	Modify
app_route	Off	On/Off	Off	--	Modify
backend_client_certificate			Off	--	Modify
ssl_ciphers	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AE		ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AE	--	Modify
real_ip_from_xff	Off	On/Off	On	Nov 17, 2022 14:57:29 GMT+08:00	Modify
vpc_name_modifiable	On	On/Off	On	Nov 2, 2022 19:57:59 GMT+08:00	Modify

Parameter	Default Value	Value Range	Current Value	Updated	Operation
xff_index	-1	Valid Int32 value	1	Nov 17, 2022 14:57:29 GMT+08:00	Modify

----End