API Gateway

Cloud Native Gateway

Product Documentation

Contents

Cloud Native Gateway
Creating Cloud Native Gateway

Last updated：2022-07-11 11:05:53

Overview

Cloud Native Gateway is an API gateway hosting product incubated by Tencent Cloud that is 100% compatible with the open source Kong gateway. It is currently in beta test.

This document describes how to create a Cloud Native Gateway instance in the console.

Directions

1. Log in to the API Gateway console and click **Cloud Native Gateway** on the left sidebar.
2. Click **Create** to enter the Cloud Native Gateway instance creation page.

Parameter	Required	Description
Region	Yes	Select the region of the Cloud Native Gateway instance.
Availability Zone	Yes	Select the AZ of the Cloud Native Gateway instance in the selected region. Unavailable AZs have insufficient resources.
Gateway Name	Yes	Enter the name of the Cloud Native Gateway instance.
Gateway Type	Yes	Currently, only Kong gateway is supported.
Gateway Version	Yes	Open-source version of the selected gateway type.
Cluster Node Specifications	Yes	Select the specification of each node. A Cloud Native Gateway cluster consists of multiple nodes.
Number of Cluster Nodes	Yes	Select the number of cluster nodes. A Cloud Native Gateway cluster consists of multiple nodes.
Network	Yes	Select the VPC where the Cloud Native Gateway instance is deployed.
Subnet	Yes	Select the subnet where the Cloud Native Gateway instance is deployed in the selected VPC.

Parameter	Required	Description
Description	No	Enter the description of the current Cloud Native Gateway instance.

3. Click **Save** and wait for the instance to be created.

Notes

- To create a Cloud Native Gateway instance, your account must be granted with the `ApiGateWay_QCSRole` role, and the role must be associated with the `QcloudAccessForApiGateWayRoleInCloudNativeAPIGateway` policy. If your account doesn't have such role and policy, grant them in the pop-up authorization window during creation.
- The log feature of Cloud Native Gateway relies on CLS. Make sure that you have activated CLS in the CLS console before creating a Cloud Native Gateway instance.
- Currently, Cloud Native Gateway is in beta and free of charge.

Interconnecting with CVM via Cloud Native Gateway

Last updated：2022-07-11 11:05:53

Overview

This document describes how to open up a service deployed in a CVM instance to a third-party business through Cloud Native Gateway.

Prerequisites

- You have created a CVM instance as instructed in Guidelines for Creating Instances and deployed it in the VPC as the backend service. The CVM instance is referred to as "backend CVM instance" in this document.
- You have created a Cloud Native Gateway instance in Kong type as instructed in Creating Cloud Native Gateway Instance. The Cloud Native Gateway instance must be in the same region and VPC as the backend CVM instance.

Directions

Step 1. Open the private network IP range of the Cloud Native Gateway instance

1. Log in to the CVM console and click **Security Group** on the left sidebar to enter the security group list.
2. Select a region and click **Create**. In the pop-up window, configure parameters to create a security group.
3. Click **OK** to enter the security group details page. Select **Security Group Rules** > **Inbound Rule** to enter the inbound rule list.
4. Click **Add Rules**. In the pop-up window, add three VPC private network IP ranges in sequence: `10.0.0.0/8`, `192.168.0.0/16`, and `172.16.0.0/12`. Enter `ALL` for all protocol ports, set all policies to **Allow**, and click **OK**.
5. Return to the security group details page. Select **Associated Instance** > **CVM** > **Add Association** and associate the newly created security group to the backend CVM instance. At this point, the VPC private network IP range has been opened.

Step 2. Configure a service and route in the Cloud Native Gateway console

1. Log in to the Cloud Native Gateway console.

2. Select a created Cloud Native Gateway instance in the instance list and click its ID to enter the instance details page.

3. On the topbar on the instance details page, select **Configuration management**, find the address and admin account/password of the Kong console, and log in to the Kong console with the account and password.

4. On the left sidebar of the Kong console, click **Services** to enter the service list.

5. Click **ADD NEW SERVICE**. In the pop-up window, configure parameters to create a service.

   When creating the service, enter the private IP of the backend CVM instance for the URL and enter 80 for the port in the format of `protocol://CVM private network IP:80`. Other fields are optional.

6. In the service list, click the name of the created service to enter its details page.

7. On the left sidebar of the service details page, click **Routes** to enter the route list.

8. Click **ADD ROUTE**. In the pop-up window, configure parameters to create a route.

   Paths is required, while other fields are optional. A path must start with "/". You can use the proxy address plus path to access the backend service.

> Note：
>
> Due to the restrictions of the Kong console, when creating a route, you must press **Enter** after entering a path to confirm the path; otherwise, the route will fail to be created.

Step 3. Access the backend service via Cloud Native Gateway

1. Log in to the Cloud Native Gateway console.

2. Select a created Cloud Native Gateway instance in the instance list and click its ID to enter the instance details page.

3. On the topbar on the instance details page, select **Configuration management** and find the Kong proxy addresses. Here, the public network proxy address is used for access over the public network, and the private network proxy address is used for access in a VPC.

4. Enter the **public network address + route path in step 2** in a browser to access the service deployed in the CVM instance.