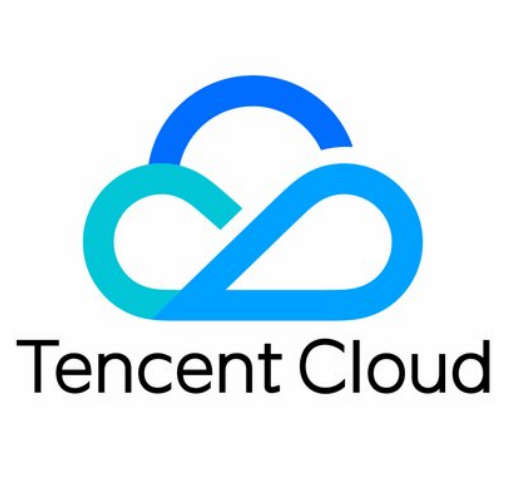
Tencent Kubernetes Engine

TKE Container Instance Guide

Product Documentation



Contents

TKE Container Instance Guide
Container Instance Management
Creating a Container Instance

Last updated：2022-12-26 16:17:57

Overview

This document describes how to create and edit a container instance, and how to view events and logs.

If you are creating a container instance for the first time, we recommend that you refer to Creating a Container Instance.
If you want to use advanced features such as container group and log collection, please refer to Creating a Container Instance.

The configuration supported by the two modes are as follows:

Supported Item	Quick Creation	Complete Creation
All regions	✓	✓
All specifications	✓	✓
Volume	✓	✓
Container environment variables	✓	✓
Number of instances	✓	✓
Multi-container	×	✓
Advanced configuration of a container (such as running command and init container)	×	✓
Restart policy (it defaults to Always)	×	✓
Log collection	×	✓
Binding a role	×	✓
Binding an EIP	×	✓

Note：
Container instances are under beta test currently. To use them, please submit a ticket.

Directions

Authorizing at the first time

You need to authorize permissions to the current account for TKE to operate cloud resources when you use an EKSCI for the first time. For details, see Service Authorization. If you have authorized the permissions to TKE, please skip this step.

You can log in to the CAM console to check if there is a TKE_QCSRole role.

Creating a container instance

1. Log in to the **TKE console**.
2. On the list page of container instances, select the region where the instance is located.
3. Click **Create instance** on the top of the instance list.
4. On the **Create instance** page, configure the basic information of the instance.

Configuration Item	Description
Instance name	Enter the name of the instance to be created.
Region	Select a closest region. For example, if you are located in Shenzhen, please select "Guzhangzhou" for the region.
Container network	Assign an IP address within the IP range of the container network to the container instance. Subnet determines the availability zone. Each availability zone supports different type of resources, such as AMD, GPU-T4 and GPU-V100. Please select a subnet which supports the desired type of resources according to the prompts.
Security group	Security group has the capability of a firewall and can limit the network communication of the instance. Default value is default.

<table>
<tr><td>Instance specification</td><td>For specifications supported by an instance, see Resource Specifications.</td></tr>
<tr><td>Volume (optional)</td><td>Provides storage for the container. Currently, it supports NFS and CBS. Also, it needs to be mounted to the specified path of the container.
<table>
<tr><th>Volume Type</th><th>Description</th></tr>
<tr><td>Cloud Block Storage (CBS)</td><td>You can mount a Tencent Cloud CBS disk to a specified path of the container. When the container is migrated, the cloud disk will be migrated along with it. CBS volumes are suitable for the persistent storage of data and can be used for stateful services such as MySQL. For a service for which a CBS volume is configured, the maximum number of Pods is 1.</td></tr>
<tr><td>Network File System (NFS)</td><td>You only need to enter the NFS path. You can use a CFS or NFS for file storage. NFS volumes are suitable for the persistent storage of data that is read and written many times. They can also be used in scenarios such as big data analysis, media processing, and content management.</td></tr>
</table></td></tr>
<tr><td>Containers in the Pod</td><td>You can add multiple containers.
Name: (optional) enter a custom name. If it is left empty, the image name will be used.
Image: you can select an image from TCR Enterprise Edition, TCR Personal Edition, Dockerhub or a third-party image repository.
Image tag: it defaults to `latest` if it is left empty.
Environment variable: you can configure the environment variables for the container.
CPU limit: It is left empty by default and the container can use all instance resources. You can set the maximum amount of CPU resources that the container can use.
Memory limit: It is left empty by default and the container can use all instance resources. You can set the maximum amount of memory resources that the container can use.
Health check: For details, see Health Check for Containers.
Running commands and parameters: For details, see Running Commands and Parameters for Containers.
Init container: You can set the container to init container. Note that there must be a business container other than the init container.
</td></tr>
<tr><td>Image repository</td><td>When you select an image from Docker Hub or a third-party image repository, you must</td></tr>
</table>

credential	enter the image credential, i.e., access address, username and password of the repository.
Number of instances	You can create multiple instances at a time. You can create only one replica if you select CBS as the volume type.

5. Click **Confirm** to go to the "Confirm configuration" page.
6. On this page, confirm the resource specification and configuration cost. Click **Create instance** to complete the creation.

You can set the advanced configuration on **Other configurations** page.

- Restart policy
- Log collection
- Role authorization
- EIP

You can select a restart policy from the following three policies. It defaults to `Always` .

- **Always**: Auto-restart the container if it is in any status other than `running` .
- **Never**: Regardless of the status, never restart the container.
- **OnFailure**: Auto-restart the container when the container terminates of the operation and the exit code is not 0. Restart policy is actually the behavior that acts on containers in the Pod. It does not means the container instance will be restarted.

Editing a container instance

1. Log in to the TKE console.
2. On the list page of container instances, select the region where the instance is located.
3. Click **More** > **Edit** on the right of the instance to be edited.
4. Modify the parameters of the instance on **Edit instance** page.
5. Click **Update instance** when you finished the modification.

Note
- Previous configuration will be cleared when you update the container instance. You need to recreate it.
- You cannot modify the following parameters for the container instance. Please recreate them if you want to modify.
  - Region
  - Network
  - Security group

- Resource specification

Container Instance Lifecycle

Last updated：2022-06-22 11:32:31

This document describes the statuses of a container instance and whether it is billed from its creation to deletion. You can determine whether your current business runs normally based on the status.

Container Instance Status

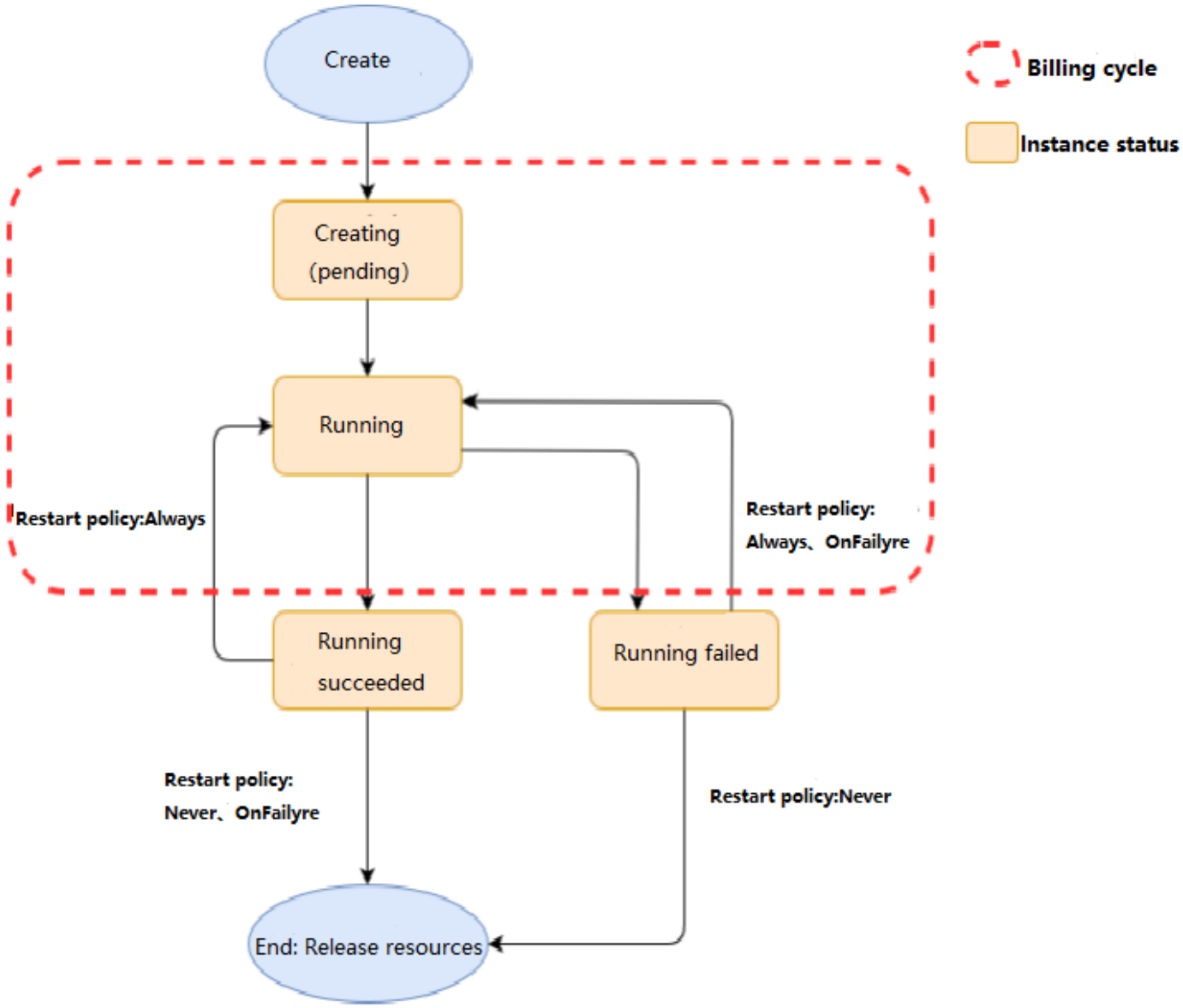
All the statuses of a container instance are as described below:

Instance Status	Description
Pending	The instance is being created.
Running	Indicates that all containers have been created successfully and at least one container is running.
Succeeded	Indicates that all containers have finished running and exited successfully (the `exitCode` of all containers is `0`) and the restart policy is `never` or `onFailure`.
Failed	Indicates that all containers have exited with an exception (the `exitCode` is not `0`) and the restart policy is `never`.

Note：
A restart policy is a behavior performed on the container in an instance. It doesn't mean that the container instance will be restarted. There are three restart policies as described below:

- **Always**: Auto-restarts the container if it is in any status other than `Running`.
- **Never**: Never restarts the container regardless of its status.
- **OnFailure**: Auto-restarts the container when it exits and the `exitCode` is not `0`.

The billing details for each status are as shown below:



Container Status

Container Status	Description
Created	The container was created successfully.
Running	The container runs successfully.

Container Status	Description
Exited	The container exits after successful or failed (`exitCode` is not `0`) running.
Unknown	The container status is unknown; for example, when the init container hasn't been terminated for a long time.

Network
Accessing Public Network by Binding an EIP

Last updated：2022-12-23 14:49:04

Overview

You need to bind an EIP or configure a NAT Gateway for the container instance and pay additional network fees when the EKSCI needs to connect to a public network, such as deploying a Nginx service, pulling a private image etc. There are two methods for this.

Method	Description and Use Cases	Cost
Binding an EIP	Elastic IP (EIP) is a fixed public IP address under a certain region and can be purchased and held independently. Use cases: a single instance or a few instances need to interconnect with a public network, for example, the Nginx service.	When EIP has not been bound with cloud resource, only IP resource fees are charged. When EIP has been bound with cloud resource, only public network fees are charged. For more information, see Billing for Elastic Public IP.
Binding a NAT Gateway	A NAT Gateway is a IP address translation service. It provides secure and high-performance Internet access service for the resources in a VPC. Use cases: multiple instances under a VPC need to communicate with a public network. For example, multiple instances need to pull images from a third-party image repository.	NAT Gateway service fees consists two parts: gateway fees (bill on an hourly basis) and network fees (bill by traffic). For more information, see Billing Overview.

This document describes how to bind an EIP to a container instance, so as to enable the container instance to interconnect with a public network.

Directions

Note

You need to bind an EIP when creating the container instance.

1. Log in to the TKE console to go to the container instance page.
2. Click **Create Instance**.
3. Configure the parameters of the container instance based on actual needs. For more information, see Creating a Container Instance. Click **Next**.
4. Enable "Binding an EIP". You can use one of the two methods to bind.
   - Auto-creating an EIP
   - Using an existing EIP

   A container instance supports auto-creating an EIP and binding with it. The attributes are as follows:

   - Peak bandwidth, which needs to be customized by you. It will affect billing. Please check the details and select appropriate peak bandwidth based on your needs.
   - Lifecycle, which is consistent with the container instance. When you delete the container instance, the lifecycle is deleted simultaneously.
5. Click **Confirm** to complete the process.

OPS
Viewing Logs and Events

Last updated：2022-04-21 18:36:00

Overview

Events and logs can help you troubleshoot the issues occur during using container instances. This document describes how to view the logs and events of container instances in the TKE console.

Viewing Container Logs

You can view the logs of init containers and business containers.

- Method 1
- Method 2

1. Log in to the TKE console.
2. On the container instance list page, click **Logs** on the right of the instance for which you want to view the events.

Viewing Container Instance Events

You can view all events corresponding to the current instance. For common events, see Event List.

- Method 1
- Method 2

1. Log in to the TKE console.
2. On the container instance list page, click **More** > **View Events** on the right of the instance for which you want to view the events.

Event List

The common events and solutions are as follows:

Content	Level	Description and Solution

Content	Level	Description and Solution
RestartedEksCi	normal	Restart EKSCI successfully.
AllocatedEip	normal	Assign an EIP successfully.
AssociatedEip	normal	Bind an EIP successfully.
ResourceInsufficient	warning	The resource with the specification corresponding to EKSCI of the current region and availability zone has been sold out. Please select another specification for creation or change to another availability zone.
RecreatingPodSandbox	warning	PodSandbox recreate after timeout.
FailedMountVolume	warning	Failed to mount a CBS disk or NFS.
FailedAllocateEip	warning	Failed to assign an EIP.
FailedAssociateEip	warning	Failed to bind an EIP.

Enabling Log Collection

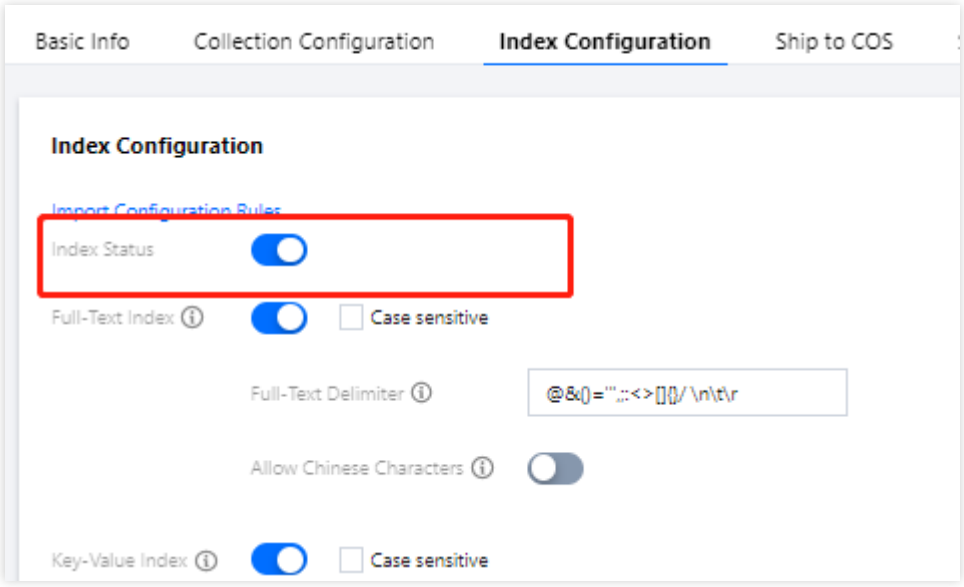
Last updated：2022-07-18 10:13:07

Overview

EKSCI provides log collection capability and supports sending the standard output logs and file logs of the containers in the cluster to CLS. It is applicable for uses who want to store and analyze the service logs in EKSCI.

Prerequisites

- Prepare a log topic of CLS to be used as the log reporting terminal. You can view and search the logs under the log topic after reporting the logs. If there is no appropriate log topic, see Creating Logset and Log Topic.
- Enable the **Log Index** for the selected log topic. Index configuration is required for CLS log search and analysis. If it is not enabled, you cannot view and search the logs. For how to configure index, see Configuring Index.
  You can go to the **CLS console** > **Log Topic** page, select a log topic name, and enable the index in the **Index Configuration** tab, as shown in the figure below:



Directions

Enabling log collection when creating a container instance

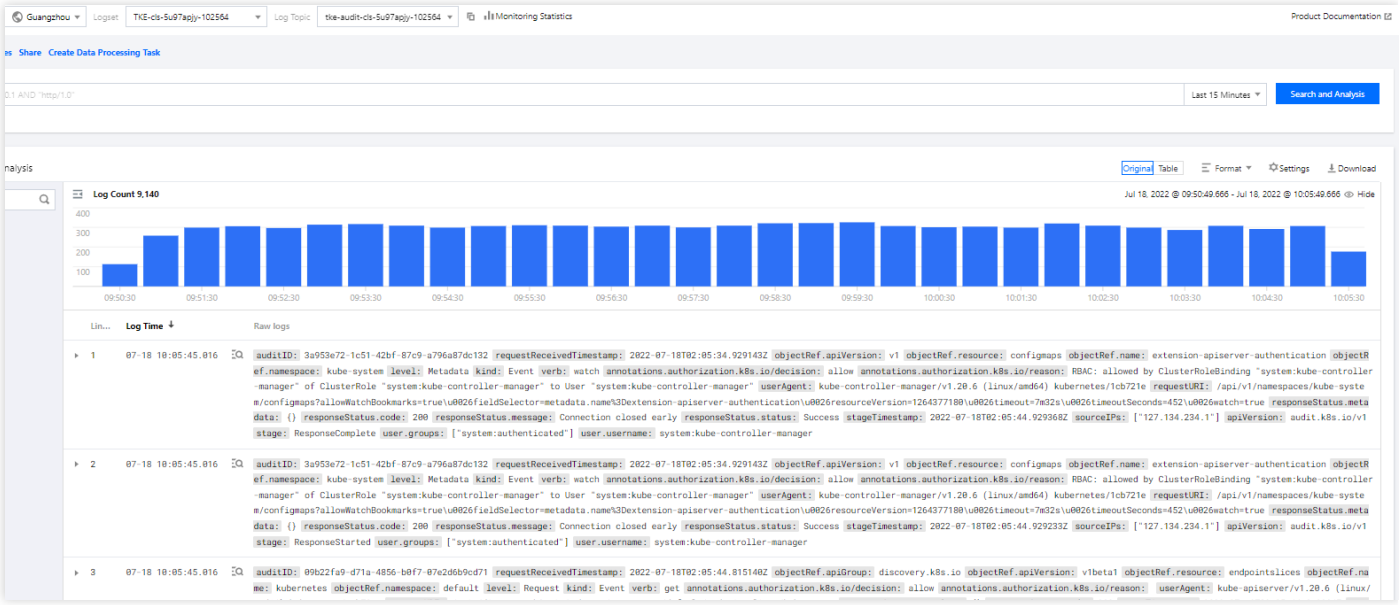
Note：
You need to enable log collection when creating the container instance.

1. Log in to the TKE console. Click **Create Instance**.
2. Set the parameters of the container instance based on actual needs. Click **Next**.
3. Enable log collection on **Other Configurations** page.
   Authorization is required when the log collection feature is enabled for the first time. The role TKE_QCSLinkedRoleInEKSLog will be bound to your account by default, and the default policy configured for this role is QcloudAccessForTKELinkedRoleInEKSLog. The role will have permissions such as log uploading. Select the following parameters after the feature is enabled:
   - Select the logset and log topic.
   - Select the container and configure the collection path. It supports "stdout" (indicating standard output) and absolute path, and supports `*`. If there are more than one collection path, separate them with `,`.

Note
If role authorization capability is required when enabling log collection feature, the role bound to the instance must have write permission of "cls:pushLog". For details, see Creating a Container Instance. Only one role can be bound to the container instance.

Viewing the collected logs

1. Log in to the CLS console and click **Search and Analysis** in the left sidebar.
2. On the **Search and Analysis** page, select the region, log set, and log topic to view logs, enable full-text index to search and analyze logs, as shown in the figure below:



FAQs

What can I do if logs are not displayed?

If you confirm that you have reported logs but they are not displayed, please check the following:

1. Log in to the CAM console to check if there is a TKE_QCSLinkedRoleInEKSLog role.
2. Check if full-text index has been enabled for the log topic.
3. If role authorization has been enabled, check if the role bound to the container instance has the permission to report logs. For specific configuration, see "Role Authorization".
4. Check if the entity selected for the role bound to the instance is CVM.

If the problem persists, please submit a ticket to contact us.

Access Management
Binding a Role to a Container Instance

Last updated：2022-12-23 14:42:55

Overview

EKSCI supports binding a role to the instance to authorize corresponding permissions to the instance. It is applicable to be used in the scenarios where you need to access other Tencent Cloud services through containers, such as uploading logs to CLS and modifying CLS topic permissions. This document describes how to bind a role to a container instance to authorize permissions.

In the following, we take uploading logs to CLS as an example. The steps are as follows:

Directions

You need to bind a role when creating the container instance. The steps are as follows:

1. Log in to the TKE console.
2. On the list page of container instances, select the region where the instance is located.
3. Click **Create Instance** at the top of the instance list.
4. Configure the parameters of the container instance based on actual needs. For more information, see Creating a Container Instance. Click **Next**.
5. Select the role you have created in advance to complete the binding process.
   It there is no appropriate role, click **Create CAM Role**. For directions, see the following:

Creating a policy

You need to create a policy before creating a role. This policy determines what permissions your role has.

1. Log in to the CAM console and select **Policies** in the left sidebar.
2. On the **Polices** page, click **Create Custom Policy**.
3. Select **Create by Policy Generator** in **Select Policy Creation Method** pop-up.
4. Select the permissions that need to be authorized to the instance. For example, select write operation of "cls:pushLog". Click **Next**.
5. Confirm the policy name and click **Done**.

Creating a role

You need to bind the policy to a role after creating the policy, so as to make the role have the permissions corresponding to the policy. You can bind multiple policies to one role based on your needs and unbind them at any time.

1. Log in to the CAM console, and select **[Roles]**(https://console.tencentcloud.com/cam/role) in the left sidebar.
2. On the **Roles** page, click **Create Role**.
3. In the **Select role entity** window that appears, select **Tencent Cloud Product Service** to go to the **Create Custom Role** page.
4. On the **Enter role entity info** tab, select **Cloud Virtual Machine (cvm)** and click **Next**.
5. On the **Configure role policy** tab, select the name of the policy created in the previous step and click **Next**.
6. On the **Review** tab, enter the role name to review the role information, and then click **Done**. For more information, see Creating a Role.

> Note
> You must select **Cloud Virtual Machine (cvm)** as the role entity. Authorization cannot be completed if you select any other entity.

7. After creating an appropriate role, select it in step 4.
8. Click **Next** to confirm the configuration and complete instance creation. You can verify if the role has been bound properly by performing the actions corresponding to the permissions.

Contact Us

Last updated：2022-04-25 15:41:16

Customer Service

If you have any questions about Tencent Cloud products, please contact our customer service for assistance.

- Hong Kong (China): +852 800-964-163 (toll-free)
- US: +1 888-652-2736 (toll-free)
- Other regions: +86 4009100100

Submitting a Ticket

If you encounter any OPS or technical problems when using our products, you can log in to the Tencent Cloud console and follow the on-screen prompts to submit a ticket. We will get back to you as soon as possible.
Ticket links:

- Submitting a ticket: Submit a ticket
- Querying ticket state: Ticket list

A ticket can have the following status:

- Pending processing: the ticket is just submitted or has been received but not reviewed by the technical support team. You can submit more information for or close the ticket at this stage.
- Processing: the technical support team has received and reviewed the ticket and is taking an action. You can submit more information for or close the ticket at this stage.
- More information required: the technical support team has received and reviewed the ticket, but more information is required for processing it. You can close the ticket at this stage.

> Note：
> The ticket will revert to "pending processing" status after you re-submit the ticket with more information.

- Closed: the ticket has been resolved, or you closed the ticket before it was processed.