

# **Tencent Kubernetes Engine Container Instance Guide Product Documentation**



## Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Container Instance Guide

### Network

- Accessing Public Network by Binding an EIP

### OPS

- Viewing Logs and Events

- Enabling Log Collection

### Access Management

- Binding a Role to a Container Instance

### Contact Us

# Container Instance Guide

## Network

### Accessing Public Network by Binding an EIP

Last updated : 2022-03-31 16:39:56

## 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	<p>Elastic IP (EIP) is a fixed public IP address under a certain region and can be purchased and held independently.</p> <p>Use cases: a single instance or a few instances need to interconnect with a public network, for example, the Nginx service.</p>	<p>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 <a href="#">Billing for Elastic Public IP</a>.</p>
Binding a NAT Gateway	<p>A NAT Gateway is a IP address translation service. It provides secure and high-performance Internet access service for the resources in a VPC.</p> <p>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.</p>	<p>NAT Gateway service fees consists two parts: gateway fees (bill on an hourly basis) and network fees (bill by traffic). For more information, see <a href="#">Billing Overview</a>.</p>

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. The steps are as follows:

## 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 : 2022-03-31 16:39:56

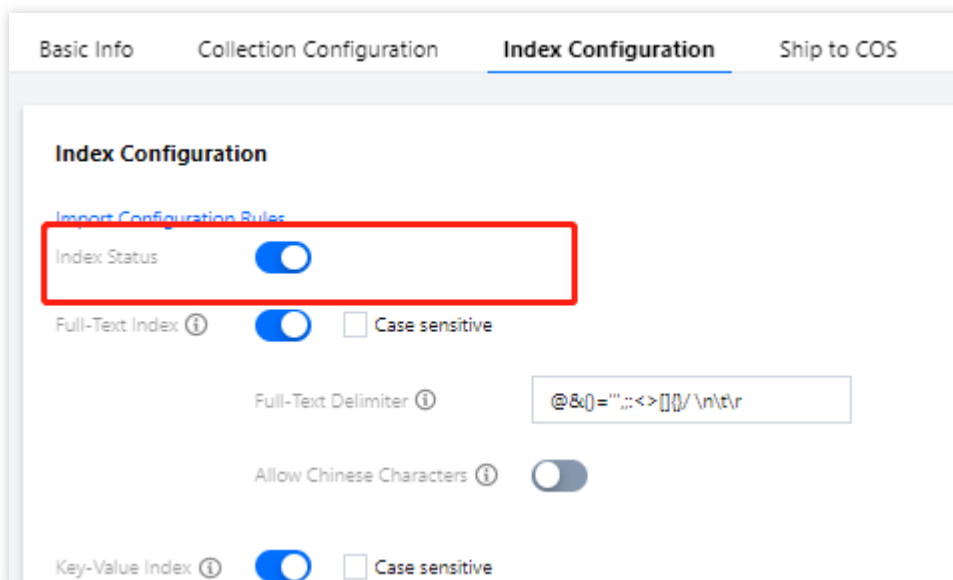
## Overview

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 users 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". 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.

## 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 : 2022-03-31 16:39:56

### 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. Click **Next**.
5. Select the role you have created in advance to complete the binding process.

If 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.cloud.tencent.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.