

# Cloud Application Engine

## User Guide

**Issue** 01  
**Date** 2024-07-01



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **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.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

<b>1 Overview.....</b>	<b>1</b>
<b>2 Permissions Management.....</b>	<b>4</b>
2.1 Creating a User and Granting Permissions.....	4
2.2 Creating a Custom CAE Policy.....	5
<b>3 Environment Management.....</b>	<b>7</b>
3.1 Creating an Environment.....	7
3.2 Deleting an Environment.....	10
3.3 Hibernating an Environment.....	10
<b>4 Application Management.....</b>	<b>13</b>
<b>5 Component Management.....</b>	<b>15</b>
5.1 Component Overview.....	15
5.2 Creating a Component.....	16
5.3 Managing Components.....	21
5.3.1 Editing a Component.....	21
5.3.2 Deleting a Component.....	24
5.3.3 Stopping a Component.....	25
5.3.4 Starting a Component.....	25
5.3.5 Restarting a Component.....	26
5.3.6 Upgrading a Component.....	26
5.3.7 Rolling Back a Component.....	30
5.3.8 Manually Scaling Component Instances.....	31
5.3.9 Related Operations.....	32
<b>6 Instance Management.....</b>	<b>34</b>
6.1 Viewing an Instance.....	34
6.2 Deleting an Instance.....	34
6.3 Logging In to a Container Using CloudShell.....	35
<b>7 Component Configurations.....</b>	<b>37</b>
7.1 Overview.....	37
7.2 Configuring RDS.....	37
7.3 Configuring CSE.....	39
7.4 Configuring Environment Variables.....	43

7.5 Configuring the Access Mode.....	47
7.5.1 Configuring Access Ports in the Environment.....	47
7.5.2 Configuring Load Balancing.....	51
7.5.3 Configuring Load Balancing and Route.....	58
7.6 Configuring an AS Policy.....	67
7.6.1 Configuring a Metric AS Policy.....	67
7.6.2 Configuring a Time AS Policy.....	71
7.6.3 Configuring a Hybrid AS Policy.....	74
7.6.4 Editing an AS Policy.....	79
7.6.5 Disabling an AS Policy.....	87
7.7 Configuring Cloud Storage.....	88
7.7.1 Cloud Storage Description.....	88
7.7.2 Configuring a Parallel File System.....	89
7.7.3 Configuring a Bucket.....	91
7.7.4 Editing a Cloud Storage Mounting Configuration.....	93
7.7.5 Deleting a Cloud Storage Mounting Configuration.....	95
7.8 Configuring Health Check.....	96
7.9 Configuring Lifecycle.....	100
7.10 Configuring Log Collection.....	103
7.11 Configuring Performance Management.....	107
7.12 Configuring Custom Metrics.....	110
<b>8 Component O&amp;M.....</b>	<b>114</b>
8.1 Viewing Component Events.....	114
8.2 Viewing Component Monitoring.....	116
8.3 Viewing Component Logs.....	118
<b>9 System Settings.....</b>	<b>120</b>
9.1 Authorizing Cloud Storage.....	120
9.2 Authorizing a Source Code Repository.....	122
9.3 Configuring a Domain Name.....	124
9.4 Configuring Certificates.....	125
9.5 Configuring Start/Stop Policies.....	127
9.6 Configuring System Network.....	130
9.6.1 Configuring Network Bandwidth.....	130
9.6.2 Configuring VPC to Access the CAE Environment.....	132
9.6.3 Configuring the CAE Environment to Access VPC.....	133
9.7 Configuring Event Notification Rules.....	135
9.8 Configuring the Monitoring System.....	139
9.9 Configuring a DEW Secret.....	143
<b>10 Key Operations Recorded by CTS.....</b>	<b>149</b>
10.1 CAE Operations That Can Be Recorded by CTS.....	149
10.2 Querying Archived Traces.....	151

---

**11 Change History..... 154**

# 1 Overview

---

Cloud Application Engine (CAE) is a serverless PaaS platform that provides simplified hosting for applications. It helps users migrate microservice applications to the cloud without O&M IaaS on a pay-per-use basis, effectively reducing costs and improving efficiency.

CAE provides the following capabilities:


- Fast deployment in minutes based on source code, software packages, or container images
- Mainstream languages and runtime systems such as Java, Node.js, and Tomcat
- Seamless hosting for web, microservice, and API applications
- Pay-per-use auto scaling based on resources or custom service indicators, coping with unpredictable user access traffic
- Standard pluggable runtime systems, allowing you to focus on application development
- Built-in application governance, implementing self-healing and quick recovery of large-scale cloud-native applications

## Prerequisites

1. You have [registered a Huawei account and enabled Huawei Cloud services](#).
2. Your account has permission to use CAE. For details, see [Creating a Custom CAE Policy](#).

## Logging In to the CAE Console

**Step 1** Log in to the [management console](#).

**Step 2** Click  and select a region.

**Step 3** Click  in the upper left corner and click **Cloud Application Engine**.

- If you log in for the first time, click **Authorize** on the displayed service authorization page to authorize CAE to use the services on which it depends. Then, the **Cloud Application Engine** console is displayed.

**Figure 1-1** Authorization

**i Grant Permissions to CAE**

Cloud Application Engine (CAE) requests permission to access SoftWare Repository for Container (SWR) so that CAE can use container images to create components.

- To use Cloud Application Engine (CAE), assign permissions to access these cloud services: Virtual Private Cloud (VPC), Elastic Load Balance (ELB), Log Tank Service (LTS), SoftWare Repository for Container (SWR), and Application Operations Management (AOM)

CAE uses these cloud services to provide network connection, cloud log management, image pulling, and monitoring analysis functions for containers in a cluster.

Once authorized, an agency named `cae_trust` will be created in IAM. To ensure service running, do not delete or modify this agency when using CAE.



- If this is not your first login, the **Cloud Application Engine** console is displayed directly.

----End

## Console Description

**Table 1-1** describes the CAE console.

**Table 1-1** CAE console description

Item	Description
Overview	Provides overall CAE dashboard information, including the application health status, CPU usage, number of concurrent connections, memory usage, traffic, network inbound speeds, engine information, and latest features.
Components	Provides capabilities such as creating, deploying, and upgrading components. A component is a self-owned package or public middleware that can be deployed and provides services externally.
Instance List	Allows you to view instance information, delete instances, and log in to containers using CloudShell.
Component Configurations	Provides component-based middleware configuration and O&M management for RDS databases, CSE engines, environment variables, access modes, AS policies, cloud storage configuration, performance management, and custom monitoring metrics.
Component Events	Displays events that occur during component deployment and running.

Item	Description
Component Monitoring	Provides component monitoring, including visualized real-time monitoring of uplink and downlink speeds (BPS), uplink and downlink rates (PPS), file system write/read rate, CPU usage, and memory usage.
Component Logs	Provides instance-level running logs to help locate faults.
System Settings	Provides cloud storage authorization, domain name configuration, and certificate configuration. You can view and unbind authorized object storage, and configure domain names, certificates, start/stop policies, microservice gateways, and event notification rules.



# 2 Permissions Management

---

## 2.1 Creating a User and Granting Permissions

This section describes how to use [Identity and Access Management \(IAM\)](#) for fine-grained permissions management on your CAE resources. With IAM, you can:

- Create IAM users for employees from different departments of your enterprise. In this way, each IAM user has a unique security credential to use CAE resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei account or cloud service to perform efficient O&M on your CAE resources.

If your Huawei account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions, as shown in [Figure 1](#).

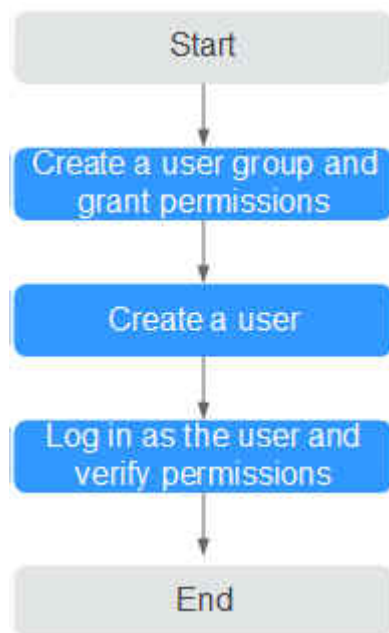
### Prerequisites

Learn about the permissions (see [Permissions Management](#)) supported by CAE and choose policies or roles according to your requirements.

For details about the permissions of other services, see [System Permissions](#).

## Process Flow

Figure 2-1 Process for granting CAE permissions



1. **Create a user group and grant permissions to it.**  
Create a user group on the CAE console, and grant the **CAE ReadOnlyAccess** policy to the group.
2. **Create an IAM user.**  
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.  
Log in to the CAE console as the created user, and verify that the user only has read permissions for CAE.
  - In **Service List**, choose **Cloud Application Engine**. On the CAE console, choose **Components** > **Create Component**. If a message appears indicating insufficient permissions after you click **Create and Deploy Component**, the **CAE ReadOnlyAccess** policy has taken effect.
  - Choose any other service in **Service List**. If a message appears indicating insufficient permissions, the **CAE ReadOnlyAccess** policy has taken effect.

## 2.2 Creating a Custom CAE Policy

Custom policies supplement the system-defined policies of CAE.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details, see [Creating a Custom Policy](#). This section provides examples of common custom CAE policies.

## Example Custom Policy

This procedure creates a policy that an IAM user is prohibited to delete components.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "cae:*:*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "cae:application:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

After authorization, users in the group can verify their permissions using the console or REST APIs.

The following uses the custom policy as an example to describe how to log in to the CAE console to verify that a user is not allowed to delete components.

1. Log in to Huawei Cloud as an IAM user.
  - Tenant name: Name of the account used to create the IAM user
  - IAM username and password: Username and password specified during the IAM user creation using the tenant name
2. On the **Components** page, create a component for test, and click **More > Delete** in the **Operation** column of the component. If a message is displayed indicating that you do not have the operation permissions, the permissions configuration is correct and has taken effect.

# 3 Environment Management

## 3.1 Creating an Environment

You can create application components in different environments to isolate them.

### NOTE

By default, only one environment can be created under an account. [Submit a service ticket](#) to increase the quota.

### Prerequisites

A CAE runs on a VPC. Before creating an environment, ensure that VPCs and subnets are available.

For details, see [Creating a VPC](#).

If the engine is created using an account with the minimum permission for creating engines, for example, `cae:environment:create` in the [fine-grained permission dependencies of CAE](#), the default VPC security group `cae-default-sg` needs to be preset by the primary account and the rules listed in [Table 3-1](#) need to be added.

For details, see [Adding a Security Group Rule](#).

**Table 3-1** cae-default-sg rules

Direction	Priority	Policy	Protocol and Port	Type	Source Address
Inbound	1	Allow	TCP: 3000–65535	IPv4	0.0.0.0/0
	1	Allow	All	IPv6	cae-default-sg
	1	Allow	All	IPv4	cae-default-sg
Outbound	100	Allow	All	IPv4	0.0.0.0/0

Direction	Priority	Policy	Protocol and Port	Type	Source Address
	100	Allow	All	IPv6	::/0

**NOTICE**

Do not modify or delete the default security group. Otherwise, the system may run abnormally.

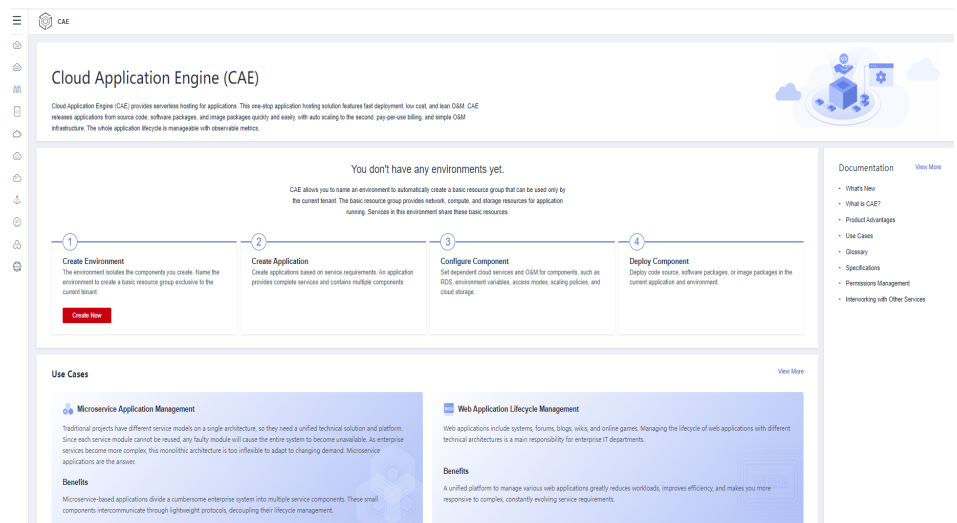
**Procedure**

**Step 1** [Log in to CAE.](#)

**Step 2** Use either of the following methods to create an environment:

- If you use CAE for the first time, a message is displayed indicating that no environment has been created.
  - a. Click **Create Now** in the **Create Environment** card.

**Figure 3-1** Creating an environment




- b. In the displayed dialog box, set the parameters by referring to [Table 3-2](#).

**Table 3-2** Creating an environment

Parameter	Description
Environment	Enter an environment name.

Parameter	Description
Enterprise Project	<p>Select an enterprise project.</p> <p>An enterprise project facilitates project-level management and grouping of cloud resources and users. The default project is <b>default</b>.</p> <p>It is available after the <b>enterprise project function</b> is enabled.</p>
Virtual Private Cloud	<p>Select the VPC to which the environment resource belongs from the drop-down list.</p> <p>To create a VPC, click <b>Create VPC</b>. For details, see <b>Creating a VPC</b>.</p> <p><b>NOTE</b> The VPC cannot be modified after the environment is created.</p>
Subnet	<p>Select a subnet from the drop-down list.</p> <p>If no subnet is available, click <b>Create Subnet</b> to access the network console and create a subnet. For details, see <b>Creating a Subnet for the VPC</b>.</p> <p><b>NOTE</b> Keep at least two available network IP addresses for CAE configuration and optimization.</p>
Security Group	<p>You can select <b>Auto generate</b> or <b>Use existing</b>.</p> <p><b>NOTE</b> This group must allow access from the selected subnet to both the subnet gateway address and the access addresses and ports of middleware such as RDS and CSE instances.</p>
Organization	<p>If you use CAE for the first time, select <b>Create Organization</b> from the drop-down list and enter an organization name.</p>

- If this is not your first time using CAE, choose **Components**.
  - a. Click  next to **Environment** in the upper part of the page.
  - b. In the displayed **Create Environment** dialog box, enter an environment name.

**Step 3** Click **OK**.


----End

## 3.2 Deleting an Environment

### NOTE

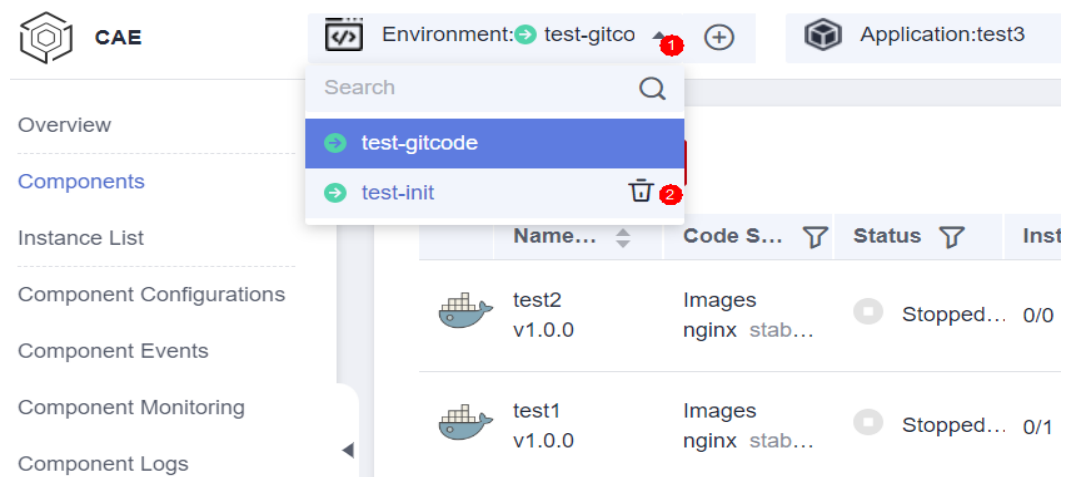
- Before deleting an environment, ensure that no component is deployed in the environment or the deployed components have been deleted. For details, see [Deleting a Component](#).
- Hibernated environments cannot be deleted. Wake up the environment before deleting it.

**Step 1** [Log in to CAE](#).

**Step 2** In **Environment** in the upper part of the page, click  to expand the environment list.

**Step 3** Move the mouse pointer to the target environment and click the displayed .

**Figure 3-2** Deleting an environment



**Step 4** In the displayed dialog box, click **OK**.

----End

## 3.3 Hibernating an Environment

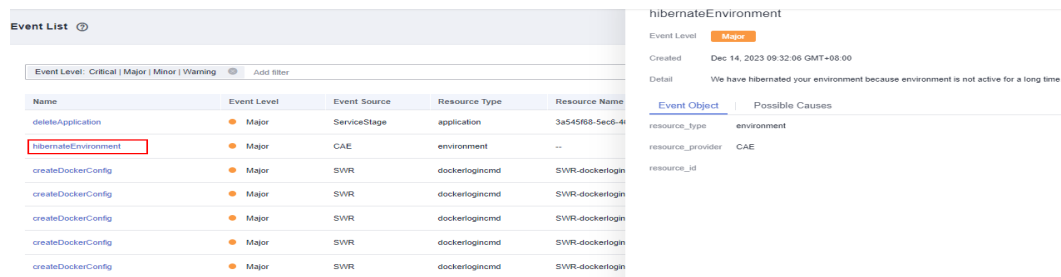
### Prerequisites

You have [created an environment](#).

### Hibernating an Environment

All CAE environments in the same region under your account will automatically enter the hibernation state if no component is deployed within 12 hours or components have been running for less than 5 minutes within three days. Then, the system will generate an event. You can view the event details on the AOM console.

Figure 3-3 Viewing event details



## Restrictions After Environment Hibernation

After hibernation, you can wake up the environment and view the applications, components, and system configurations in the environment, but cannot modify them.

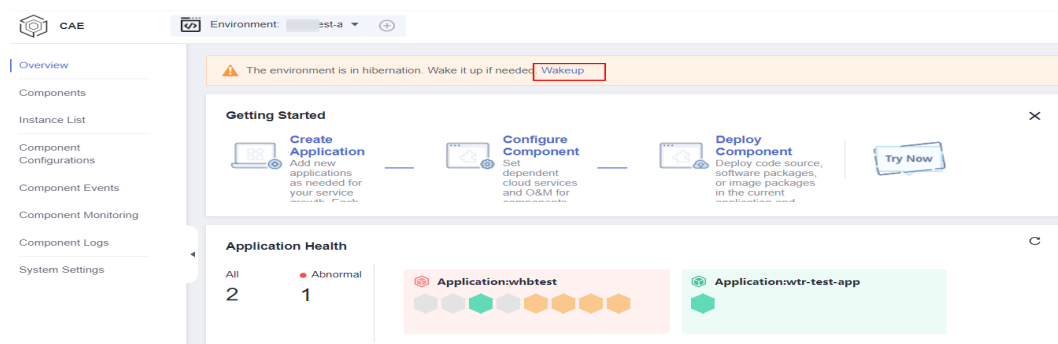
## Waking Up an Environment

Wake up the environment before deleting it or deploying components in it.

**Step 1** Log in to CAE.

**Step 2** Click **Wakeup** in the upper part of the page.

Figure 3-4 Wakeup page



**Step 3** In the displayed dialog box, confirm the environment information, click **OK**, and wait until the environment is woken up.



Figure 3-5 Confirming information

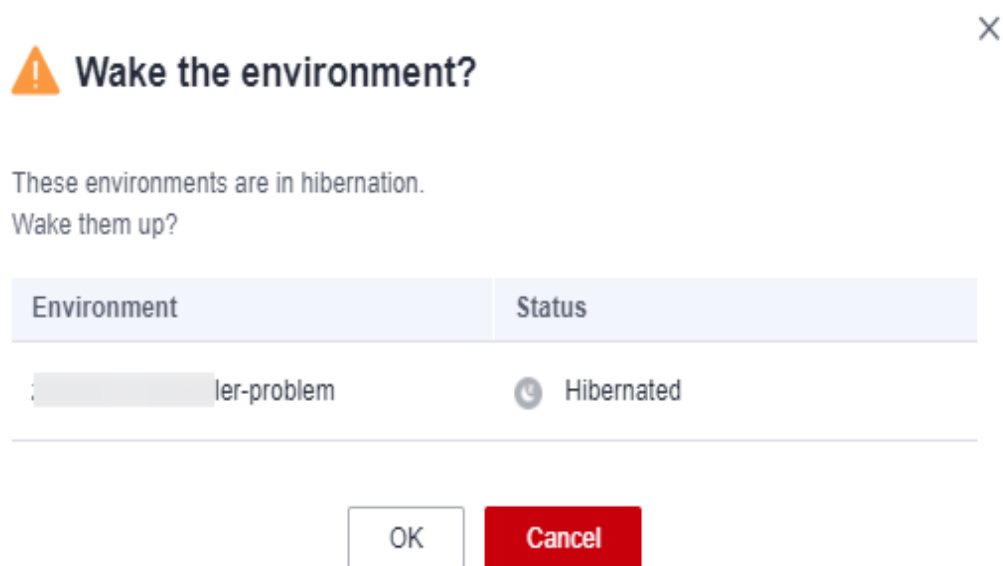
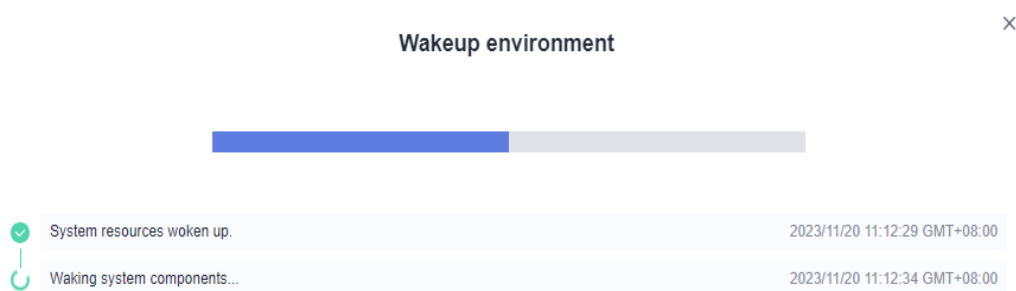


Figure 3-6 Waking up environment



----End

# 4 Application Management

You can create applications and components under an application to provide services externally.


## Prerequisites

You have [created an environment](#).

## Creating an Application

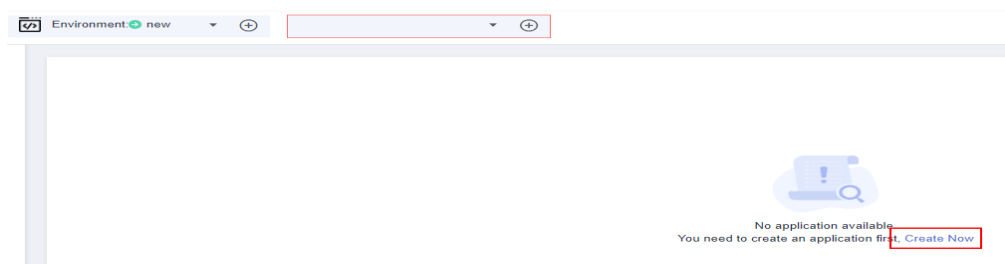
**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components** and use either of the following methods to create an application:

- Click  next to **Application** in the upper part of the page.
- Click **Create Now** on the **Components** page.

This method is available only when you create the first application.

**Figure 4-1** Creating an application



**Step 3** In the displayed **Create Application** dialog box, enter an application name.

**Step 4** Click **OK**.

----End


## Deleting an Application

### NOTICE

- Deleted applications cannot be restored. Exercise caution when performing this operation.
- Before deleting an application, delete all components of the application. For details, see [Deleting a Component](#).

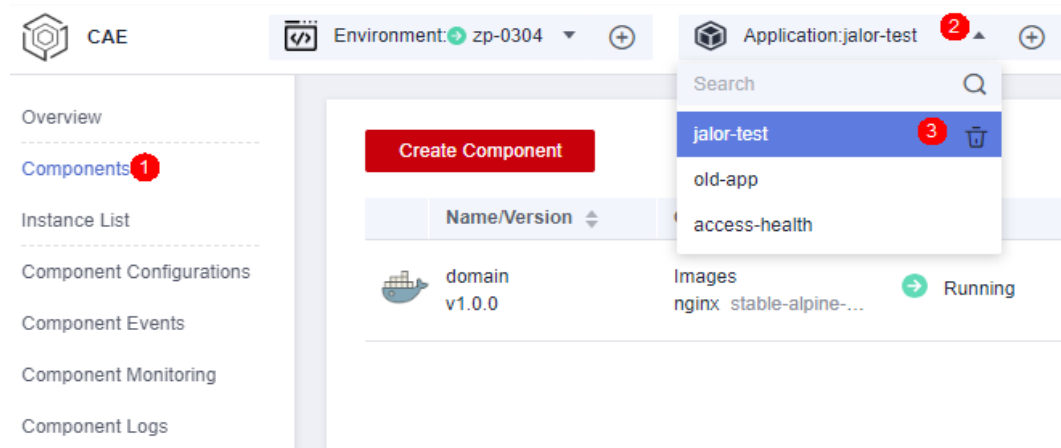
**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Click  in the **Application** column to expand the application list.

**Step 4** Move the mouse pointer to the target application and click the displayed .

**Figure 4-2** Deleting an application



**Step 5** In the displayed dialog box, click **OK**.

----End

# 5 Component Management

## 5.1 Component Overview

An application component implements a service feature of an application. It is in the form of code or software packages and can be deployed independently.

After creating an application on CAE, you can create components in the application.

### Component Description

**Table 5-1** lists the languages and runtime systems supported by CAE components.

**Table 5-1** Supported languages and runtime systems

Runtime System	Component Source
Java 8, Java 11, Java 17	Source code repository, JAR package
Tomcat 8, Tomcat 9	Source code repository, WAR package
Node.js 8, Node.js 14, Node.js 16	Source code repository, ZIP package
PHP 7	Source code repository, ZIP package
Docker	Image package
Python 3	Source code repository, ZIP package
.net core	Source code repository

## Component Source

Component Source	Description
Source code repository	GitHub, GitCode, GitLab, and Bitbucket code can be identified.
Image	<p>If you use a private image to create your containerized application, upload the private image to the image repository. The following upload modes are supported:</p> <ol style="list-style-type: none"> <li>1. Upload the image package by <b>Upload Through Client</b> or <b>Upload Through Page</b>.</li> <li>2. Go to the Software Repository for Container (SWR) console and upload the image to the image repository. For details, see <a href="#">Uploading an Image</a>.</li> </ol>
Software package	<p>The following upload modes are supported:</p> <ol style="list-style-type: none"> <li>1. Select the corresponding software package from the CodeArts software release repository. Upload the software package to the software release repository in advance. For details, see <a href="#">Uploading a Software Package</a>.</li> <li>2. Select the corresponding software package from OBS. Upload the software package to the OBS bucket in advance. For details, see <a href="#">Uploading an Object</a>.</li> </ol>

## 5.2 Creating a Component

### NOTE

A maximum of 50 application components can be created in an environment.

### Prerequisites

1. You have created an environment. For details, see [Creating an Environment](#).
2. You have created an application. For details, see [Creating an Application](#).

### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the created application and environment from the drop-down lists in the upper part of the page, and click **Create Component**.

**Step 4** Configure the component by referring to [Table 5-2](#).

**Table 5-2** Basic component information

Parameter	Item	Description
Component	-	Component name.
Version	-	Component version. The format is A.B.C or A.B.C.D. A, B, C, and D are natural numbers, for example, 1.0.0 or 1.0.0.0.
Specifications	-	Select the instance specifications, for example, 0.5 Core, 1 GiB; 1 Core, 1 GiB; 1 Core, 2 GiB; 2 Core, 4 GiB.
Instances	-	Value range: 1 to 99. Default value: 2.

Parameter	Item	Description
Code Source	Source code repository	<ol style="list-style-type: none"> <li>1. Select a code source. GitHub, GitCode, GitLab, and Bitbucket code can be identified.</li> <li>2. Complete the code information. <ul style="list-style-type: none"> <li>- <b>Authorization:</b> Select the corresponding source code authorization from the drop-down list. If you use this function for the first time, click <b>Create Authorization</b> and set <b>Authorization</b> and <b>Mode</b>, and click <b>OK</b>. Click <b>Authorization List</b> to view the created authorization. Select the check box on the left to <b>Re-authorize</b> or <b>Delete</b> the authorized source code.</li> <li>- <b>Username/Organization:</b> Select a user or organization to manage code in the current project.</li> <li>- <b>Repository:</b> Select a repository to manage code of each module in the current project.</li> <li>- <b>Branch:</b> Select a branch to manage code.</li> </ul> </li> <li>3. <b>Language/Runtime System:</b> Select a language of the source code from the drop-down list. For details, see <a href="#">Component Description</a>.</li> <li>4. <b>Custom Build:</b> Select <b>Default</b> or <b>Custom</b>. <p><b>NOTE</b> The authorization mode varies depending on the code source.</p> <ul style="list-style-type: none"> <li>- <b>Default command or script:</b> preferentially executes <b>build.sh</b> in the <b>root</b> directory. If <b>build.sh</b> does not exist, the code will be built using the common method of the selected language. Example: <b>mvn clean package</b> for Java.</li> <li>- <b>Custom command:</b> Commands are customized using the selected language. Alternatively, the default command or script is used after <b>build.sh</b> is modified.</li> </ul> </li> <li>5. <b>Dockerfile:</b> Set this parameter if the component source is <b>Source code repository</b>. You can select <b>Custom</b> or <b>Default</b>. <p><b>NOTE</b> You can select <b>Default</b> to change the name of the Maven artifact file specified in the default Dockerfile only when <b>Language/Runtime System</b> is set to Java.</p> </li> <li>6. <b>Dockerfile Address:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Custom</b>. <ul style="list-style-type: none"> <li>- <b>Dockerfile Address</b> is the directory where the Dockerfile is located relative to the root directory (./) of the project. The Dockerfile is used to build an image.</li> <li>- The Docker program reads the Dockerfile file to generate a custom image.</li> </ul> </li> </ol>

Parameter	Item	Description
		<ul style="list-style-type: none"> <li>- The Dockerfile address contains 1 to 255 characters, including letters, digits, periods (.), hyphens (-), underscores (_), and slashes (/).</li> <li>- If the file name is Dockerfile, you can only enter a directory address and this address must end with a slash (/).</li> </ul> <p>7. <b>Artifact File:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Default</b>. Select and run the specified JAR package from multiple JAR packages generated during Maven build. The JAR package ends with <b>.jar</b>. Fuzzy match is supported. Examples: demo-1.0.jar and demo*.jar.</p>
	Image	<ol style="list-style-type: none"> <li>1. Upload the image package by <b>Upload Through Client</b> or <b>Upload Through Page</b>.</li> <li>2. On the <b>My Images</b>, <b>Open Source Images</b>, or <b>Shared Images</b> page, select an image package for deployment. You can search for an image by name. <ul style="list-style-type: none"> <li>- <b>My Images:</b> image packages uploaded by users.</li> <li>- <b>Open Source Images:</b> images provided by SWR.</li> <li>- <b>Shared Images:</b> image packages shared by different accounts.</li> </ul> </li> <li>3. (Optional) You can also click the link next to <b>Code Source</b> to go to the SWR console and perform more image management operations.</li> </ol> <p><b>NOTE</b> When you select <b>Upload Through Page</b>, only one image package can be added at a time. The file size cannot exceed 2 GB (after decompression). The image package can be in .tar or .tar.gz format. Only the image package created by the container engine client of version 1.11.2 or later can be uploaded. For details, see <a href="#">Creating an Image Package</a>. To upload a file larger than 2 GB, select <b>Upload Through Client</b>.</p>

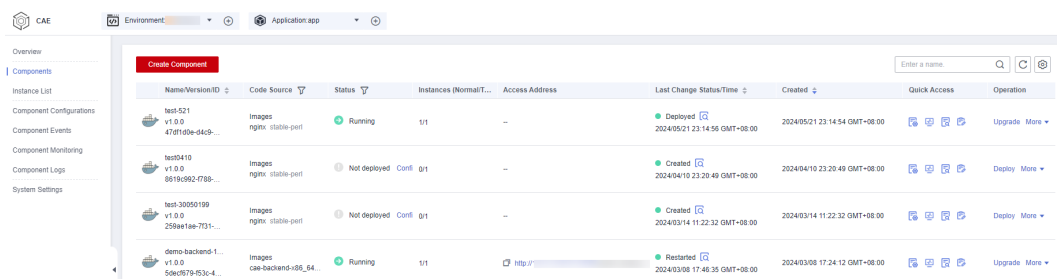


Parameter	Item	Description
	Software package	<ol style="list-style-type: none"> <li>Select <b>CodeArts Release Repo</b> or <b>OBS</b> where the software packages are located.                             <ul style="list-style-type: none"> <li>If you select <b>CodeArts Release Repo</b>, upload the software package to the software release repository in advance. For details, see <a href="#">Uploading a Software Package</a>.</li> <li>If you select <b>OBS</b>, upload the software package to the OBS bucket in advance. For details, see <a href="#">Uploading an Object</a>.</li> </ul> </li> <li><b>Language/Runtime System</b>: Select a language of the software package from the drop-down list. For details, see <a href="#">Component Description</a>.</li> <li><b>Build Type</b>: Select <b>System default</b> or <b>Custom Dockerfile</b>.                             <ul style="list-style-type: none"> <li><b>System default</b>: Use the default Dockerfile based on the selected language or runtime system.</li> <li><b>Custom Dockerfile</b>: Customize the Dockerfile based on the selected language.</li> </ul> </li> </ol>


**Step 5** Create a component.

- Click **Configure Component**. For details, see [Component Configurations](#).
- Click **Create and Deploy Component**. In the displayed dialog box, click **Deploy Now**.
- After the component is created or deployed, you can view the environment ID, application ID, component ID, component name, code source, status, number of instances, and creation time on the **Components** page.

**Figure 5-1** Component list



**NOTE**

- If a component is in the **Not deployed** state, click **Configure** in the **Status** column to configure and deploy it.
- If a component is in the **Running** state, click  in the **Quick Access** column to reconfigure it and make the configurations take effect.

----End

## 5.3 Managing Components

### 5.3.1 Editing a Component

You can modify the name, version number, number of instances, instance specifications, code source, and custom build commands of components.

 **NOTE**

Only component in the **Not deployed** state can be edited.

#### Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Components**.
- Step 3** Select the target component and click **More > Edit** in the **Operation** column.
- Step 4** Configure the component again by referring to the following table.

Parameter	Item	Description
Component	-	Component name.
Version	-	Component version. The format is A.B.C or A.B.C.D. A, B, C, and D are natural numbers, for example, 1.0.0 or 1.0.0.0.
Specifications	-	Select the instance specifications, for example, 0.5 Core, 1 GiB; 1 Core, 1 GiB; 1 Core, 2 GiB; 2 Core, 4 GiB.
Instances	-	Value range: 1 to 99. Default value: 2.

Parameter	Item	Description
Code Source	Source code repository	<ol style="list-style-type: none"> <li>1. Select a code source. GitHub, GitCode, GitLab, and Bitbucket code can be identified.</li> <li>2. Complete the code information. <ul style="list-style-type: none"> <li>- <b>Authorization:</b> Select the corresponding source code authorization from the drop-down list. If you use this function for the first time, click <b>Create Authorization</b> and set <b>Authorization</b> and <b>Mode</b>, and click <b>OK</b>. Click <b>Authorization List</b> to view the created authorization. Select the check box on the left to <b>Re-authorize</b> or <b>Delete</b> the authorized source code.</li> <li>- <b>Username/Organization:</b> Select a user or organization to manage code in the current project.</li> <li>- <b>Repository:</b> Select a repository to manage code of each module in the current project.</li> <li>- <b>Branch:</b> Select a branch to manage code.</li> </ul> </li> <li>3. <b>Language/Runtime System:</b> Select a language of the source code from the drop-down list.</li> <li>4. <b>Custom Build:</b> Select <b>Default</b> or <b>Custom</b>. <p><b>NOTE</b> The authorization mode varies depending on the code source.</p> <ul style="list-style-type: none"> <li>- <b>Default command or script:</b> preferentially executes <b>build.sh</b> in the <b>root</b> directory. If <b>build.sh</b> does not exist, the code will be built using the common method of the selected language. Example: <b>mvn clean package</b> for Java.</li> <li>- <b>Custom command:</b> Commands are customized using the selected language. Alternatively, the default command or script is used after <b>build.sh</b> is modified.</li> </ul> </li> <li>5. <b>Dockerfile:</b> Set this parameter if the component source is <b>Source code repository</b>. You can select <b>Custom</b> or <b>Default</b>. <p><b>NOTE</b> You can select <b>Default</b> only when <b>Language/Runtime System</b> is set to Java.</p> </li> <li>6. <b>Dockerfile Address:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Custom</b>. <ul style="list-style-type: none"> <li>- <b>Dockerfile Address</b> is the directory where the Dockerfile is located relative to the root directory (./) of the project. The Dockerfile is used to build an image.</li> <li>- The Docker program reads the Dockerfile file to generate a custom image.</li> <li>- The Dockerfile address contains 1 to 255 characters, including letters, digits, periods (.), hyphens (-), underscores (_), and slashes (/).</li> </ul> </li> </ol>

Parameter	Item	Description
		<ul style="list-style-type: none"> <li>- If the file name is Dockerfile, you can only enter a directory address and this address must end with a slash (/).</li> </ul> <p>7. <b>Artifact File:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Default</b>. Select and run the specified JAR package from multiple JAR packages generated during Maven build. The JAR package ends with <b>.jar</b>. Fuzzy match is supported. Examples: demo-1.0.jar and demo*.jar.</p>
	Image	<ol style="list-style-type: none"> <li>1. Upload the image package by <b>Upload Through Client</b> or <b>Upload Through Page</b>.</li> <li>2. On the <b>My Images</b>, <b>Open Source Images</b>, or <b>Shared Images</b> page, select an image package for deployment. You can search for an image by name. <ul style="list-style-type: none"> <li>- <b>My Images:</b> image packages uploaded by users.</li> <li>- <b>Open Source Images:</b> images provided by SWR.</li> <li>- <b>Shared Images:</b> image packages shared by different accounts.</li> </ul> </li> <li>3. (Optional) You can also click the link next to <b>Code Source</b> to go to the SWR console and perform more image management operations.</li> </ol> <p><b>NOTE</b> When you select <b>Upload Through Page</b>, only one image package can be added at a time. The file size cannot exceed 2 GB (after decompression). The image package can be in .tar or .tar.gz format. Only the image package created by the container engine client of version 1.11.2 or later can be uploaded. For details, see <a href="#">Creating an Image Package</a>. To upload a file larger than 2 GB, select <b>Upload Through Client</b>.</p>

Parameter	Item	Description
	Software package	<ol style="list-style-type: none"> <li>1. Select <b>CodeArts Release Repo</b> or <b>OBS</b> where the software packages are located. <ul style="list-style-type: none"> <li>- If you select <b>CodeArts Release Repo</b>, upload the software package to the software release repository in advance. For details, see <a href="#">Uploading a Software Package</a>.</li> <li>- If you select <b>OBS</b>, upload the software package to the OBS bucket in advance. For details, see <a href="#">Uploading an Object</a>.</li> </ul> </li> <li>2. <b>Language/Runtime System</b>: Select a language of the software package from the drop-down list.</li> <li>3. <b>Build Type</b>: Select <b>System default</b> or <b>Custom Dockerfile</b>. <ul style="list-style-type: none"> <li>- <b>System default</b>: Use the default Dockerfile based on the selected language or runtime system.</li> <li>- <b>Custom Dockerfile</b>: Customize the Dockerfile based on the selected language.</li> </ul> </li> </ol>

**Step 5** Click **Complete**.

----End

## 5.3.2 Deleting a Component

You can delete a component that is no longer used.

### NOTICE

- Deleted components cannot be restored. Exercise caution when performing this operation.
- Only components that have no available instances can be deleted. [Stop the component](#) before deleting it.

### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **More > Delete** in the **Operation** column.

Figure 5-2 Deleting a component

Name/Version/ID	Code Source	Status	Instances (NormalIT...	Access Address	Last Change Status/Time	Created	Quick Access	Operation
test-521 v1.0.0 47df1d0e-d4c9...	Images nginx_stable-perf	Running	1/1	--	Deployed 2024/05/21 23:14:56 GMT+08:00	2024/05/21 23:14:54 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More
test0410 v1.0.0 6819-c92-4789...	Images nginx_stable-perf	Not deployed Conf 0/1		--	Created 2024/04/10 23:20:49 GMT+08:00	2024/04/10 23:20:49 GMT+08:00	[Refresh] [Refresh] [Refresh]	Deploy More
test-30050199 v1.0.0 259aa1ae-7f31...	Images nginx_stable-perf	Not deployed Conf 0/1		--	Created 2024/03/14 11:22:32 GMT+08:00	2024/03/14 11:22:32 GMT+08:00	[Refresh] [Refresh] [Refresh]	Roll back Start Stop Restart Edit Delete
demo-backend-1... v1.0.0 5de6f979-f53c-4...	Images cae-backend-x86_64...	Running	1/1	http://	Restarted 2024/03/08 17:46:35 GMT+08:00	2024/03/08 17:24:12 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More

**Step 4** In the displayed dialog box, enter **DELETE** and click **OK**.

----End

### 5.3.3 Stopping a Component

You can stop a component that is not used. A stopped component will not be charged and its application cannot be used.

#### NOTE

- Components in the **Not deployed** and **Not ready** states cannot be stopped.
- Do not stop a component when it is being scaled. Disable the AS policy before the operation. For details, see [Disabling an AS Policy](#).
- When a component is being stopped, AS policies cannot be added or enabled for the component.

#### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **More > Stop** in the **Operation** column.

Figure 5-3 Stopping a component

Name/Version/ID	Code Source	Status	Instances (NormalIT...	Access Address	Last Change Status/Time	Created	Quick Access	Operation
test-521 v1.0.0 47df1d0e-d4c9...	Images nginx_stable-perf	Running	1/1	--	Deployed 2024/05/21 23:14:56 GMT+08:00	2024/05/21 23:14:54 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More
demo-backend-1... v1.0.0 5de6f979-f53c-4...	Images cae-backend-x86_64...	Running	1/1	http://	Restarted 2024/03/08 17:46:35 GMT+08:00	2024/03/08 17:24:12 GMT+08:00	[Refresh] [Refresh] [Refresh]	Roll back Start Stop Restart Edit Delete
demo-frontend-1... v1.0.0 7049a99a-49e1...	Images cae-frontend-x86_64...	Running	1/1	http://	Deployed 2024/03/08 17:24:27 GMT+08:00	2024/03/08 17:24:12 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More

**Step 4** In the displayed dialog box, click **OK**.

----End

### 5.3.4 Starting a Component

You can start a stopped component.

#### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **More > Start** in the **Operation** column.

**Figure 5-4** Starting a component

Name/Version/ID	Code Source	Status	Instances (Normal/T...	Access Address	Last Change Status/Time	Created	Quick Access	Operation
test v1.0.0 045d8c-63e3...	Software Packages weather-1.0.0.jar	Stopped	0/1	-	Stopped 2024/01/29 19:26:02 GMT+08:00	2024/01/29 19:25:00 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More Start Stop Restart Edit Delete
umask v1.0.0 f715d9-2ae5...	Images withmetric v1	Stopped	0/2	-	Stopped 2024/01/22 11:53:24 GMT+08:00	2024/01/17 18:17:07 GMT+08:00	[Refresh] [Refresh] [Refresh]	

**Step 4** In the displayed dialog box, click **OK**.

----End

### 5.3.5 Restarting a Component

Only components in the **Running** and **Not ready** states can be restarted.

**NOTE**

When a component is being started, AS policies cannot be added or enabled for the component.

#### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **More > Restart** in the **Operation** column.

**Figure 5-5** Restarting a component

Name/Version/ID	Code Source	Status	Instances (Normal/T...	Access Address	Last Change Status/Time	Created	Quick Access	Operation
test-521 v1.0.0 47d1d0e-d4c9...	Images nginx: stable-perf	Running	1/1	-	Deployed 2024/05/21 23:14:56 GMT+08:00	2024/05/21 23:14:54 GMT+08:00	[Refresh] [Refresh] [Refresh]	Upgrade More Roll back Start Stop Restart Edit Delete
test0410 v1.0.0 8619-592-f789...	Images nginx: stable-perf	Not deployed	Conf: 0/1	-	Created 2024/04/10 23:20:49 GMT+08:00	2024/04/10 23:20:49 GMT+08:00	[Refresh] [Refresh] [Refresh]	
test-30050199 v1.0.0 259e4f6e-7031...	Images nginx: stable-perf	Not deployed	Conf: 0/1	-	Created 2024/03/14 11:22:32 GMT+08:00	2024/03/14 11:22:32 GMT+08:00	[Refresh] [Refresh] [Refresh]	

**Step 4** In the displayed dialog box, click **OK**.

----End

### 5.3.6 Upgrading a Component

If a component fails to be deployed, you can upgrade it for redeployment.

#### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **Upgrade** in the **Operation** column.

**Step 4** Configure the component again by referring to the following table.

Parameter	Item	Description
Component	-	The value cannot be changed during upgrade.
Version	-	Component version. The format is A.B.C or A.B.C.D. A, B, C, and D are natural numbers, for example, 1.0.0 or 1.0.0.0.
Specifications	-	Select the instance specifications, for example, 0.5 Core, 1 GiB; 1 Core, 1 GiB; 1 Core, 2 GiB; 2 Core, 4 GiB.



Parameter	Item	Description
<p>Code Source</p> <p><b>NOTE</b> During upgrade, the code source format is restricted. For example, components deployed using images, JAR, or WAR can only be upgraded using images, JAR, or WAR respectively.</p>	<p>Source code repository</p>	<ol style="list-style-type: none"> <li>1. Select a code source. GitHub, GitCode, GitLab, and Bitbucket code can be identified.</li> <li>2. Only <b>Branch</b> can be modified during upgrade. <b>Branch:</b> Select a branch to manage code.</li> <li>3. <b>Build Type:</b> Select <b>Default</b> or <b>Custom</b>. <b>NOTE</b> The authorization mode varies depending on the code source. <ul style="list-style-type: none"> <li>- <b>Default command or script:</b> preferentially executes <b>build.sh</b> in the <b>root</b> directory. If <b>build.sh</b> does not exist, the code will be built using the common method of the selected language. Example: <b>mvn clean package</b> for Java.</li> <li>- <b>Custom command:</b> Commands are customized using the selected language. Alternatively, the default command or script is used after <b>build.sh</b> is modified.</li> </ul> </li> <li>4. <b>Dockerfile:</b> Set this parameter if the component source is <b>Source code repository</b>. You can select <b>Custom</b> or <b>Default</b>. <b>NOTE</b> You can select <b>Default</b> to configure artifact files only when <b>Language/Runtime System</b> is set to Java.</li> <li>5. <b>Dockerfile Address:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Custom</b>. <ul style="list-style-type: none"> <li>- <b>Dockerfile Address</b> is the directory where the Dockerfile is located relative to the root directory (./) of the project. The Dockerfile is used to build an image.</li> <li>- The Docker program reads the Dockerfile file to generate a custom image.</li> <li>- The Dockerfile address contains 1 to 255 characters, including letters, digits, periods (.), hyphens (-), underscores (_), and slashes (/).</li> <li>- If the file name is Dockerfile, you can only enter a directory address and this address must end with a slash (/).</li> </ul> </li> <li>6. <b>Artifact File:</b> Set this parameter if <b>Dockerfile</b> is set to <b>Default</b>. Select and run the specified JAR package from multiple JAR packages generated during Maven build. The JAR package ends with <b>.jar</b>. Fuzzy match is supported. Examples: demo-1.0.jar and demo*.jar.</li> </ol>

Parameter	Item	Description
	Image	<ol style="list-style-type: none"> <li>1. Upload the image package by <b>Upload Through Client</b> or <b>Upload Through Page</b>.</li> <li>2. On the <b>My Images</b>, <b>Open Source Images</b>, or <b>Shared Images</b> page, select an image package for deployment. You can search for an image by name. <ul style="list-style-type: none"> <li>- <b>My Images</b>: image packages uploaded by users.</li> <li>- <b>Open Source Images</b>: images provided by SWR.</li> <li>- <b>Shared Images</b>: image packages shared by different accounts.</li> </ul> </li> <li>3. (Optional) You can also click the link next to <b>Code Source</b> to go to the SWR console and perform more image management operations.</li> </ol> <p><b>NOTE</b> When you select <b>Upload Through Page</b>, only one image package can be added at a time. The file size cannot exceed 2 GB (after decompression). The image package can be in .tar or .tar.gz format. Only the image package created by the container engine client of version 1.11.2 or later can be uploaded. For details, see <a href="#">Creating an Image Package</a>. To upload a file larger than 2 GB, select <b>Upload Through Client</b>.</p>
	Software package	<ol style="list-style-type: none"> <li>1. Select <b>CodeArts Release Repo</b> or <b>OBS</b> where the software packages are located. <ul style="list-style-type: none"> <li>- If you select <b>CodeArts Release Repo</b>, upload the software package to the software release repository in advance. For details, see <a href="#">Uploading a Software Package</a>.</li> <li>- If you select <b>OBS</b>, upload the software package to the OBS bucket in advance. For details, see <a href="#">Uploading an Object</a>.</li> </ul> </li> <li>2. <b>Build Type</b>: Select <b>System default</b> or <b>Custom Dockerfile</b>. <ul style="list-style-type: none"> <li>- <b>System default</b>: Use the default Dockerfile based on the selected language or runtime system.</li> <li>- <b>Custom Dockerfile</b>: Customize the Dockerfile based on the selected language.</li> </ul> </li> </ol>

**Figure 5-6** Upgrading a component

**Upgrade Component**

Component: source-test

Specifications: 0.5 Core | 1 GiB

Version: 1.0.5

Code Source:

- Source code repository: CodeArts
- Username/Organization: [Redacted]
- Repository: cae-backend
- Branch: master

Language/Runtime System: Java8

Build Type: Default | **Custom** ?

**⚠ Exercise caution when inputting sensitive information in the echo, cat, or debug command, or encrypt sensitive information to avoid leakage.**

```
1 cd test02
```

Dockerfile: Custom | Default

Dockerfile Address ? : /

The Docker program reads the Dockerfile file to generate a custom image. Enter 1 to 255 characters. Only letters, digits, hyphens (-), underscores (\_), and slashes (/) are allowed. If the file name is Dockerfile, you can only enter a directory address and this address must end with a slash (/).

**Step 5** Click **Upgrade Now**.

----End

### 5.3.7 Rolling Back a Component

You can roll back to a historical version and configuration. (A version number is generated for each component configuration. The number is the same as the current one, but the time is different.)

#### Procedure

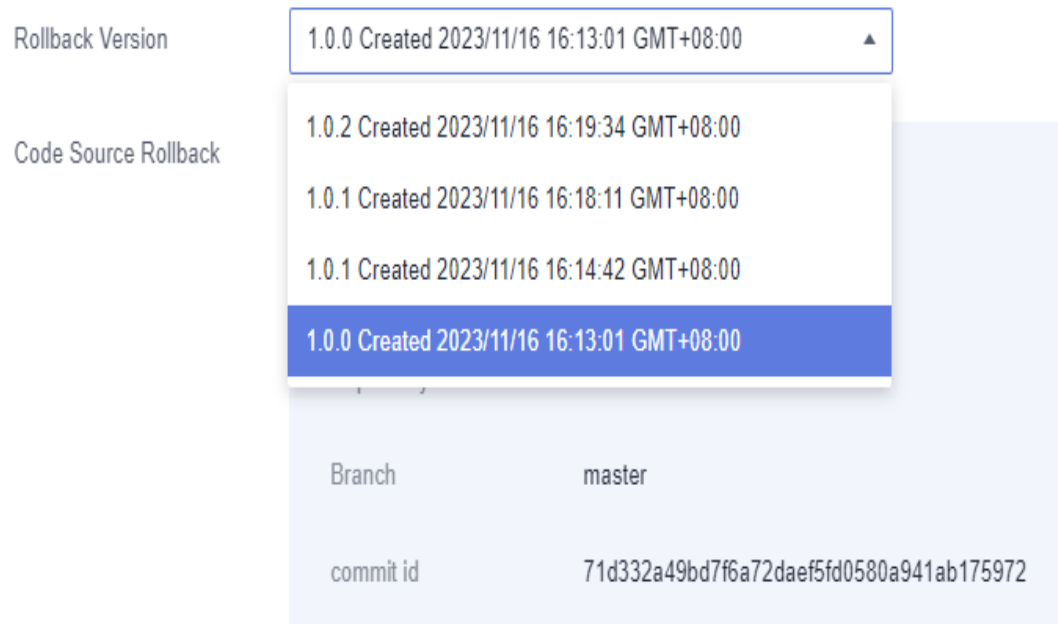
**Step 1** [Log in to CAE](#).

**Step 2** Choose **Components**.

**Step 3** Select the target component and click **More > Roll back** in the **Operation** column.

**Step 4** Select a rollbak version.

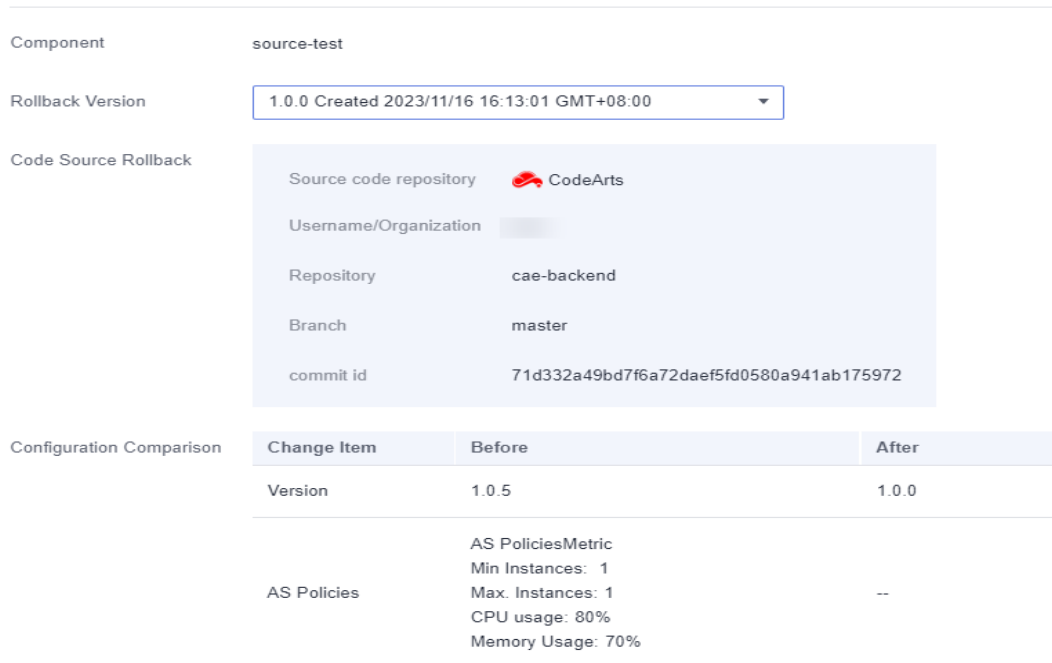
**Figure 5-7** Selecting a rollback version



**Step 5** Confirm the component configuration and code source of the rollback version, and click **Roll Back Now**.

**Figure 5-8** Confirming information

**Rolling Back Components**



----End


### 5.3.8 Manually Scaling Component Instances

The number of instances will be increased or decreased immediately after the configuration is complete.

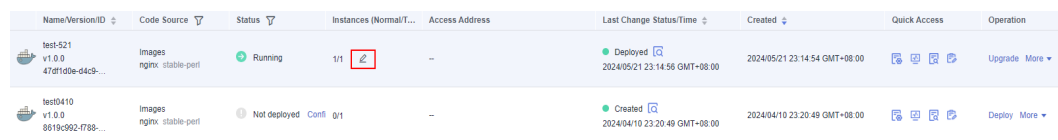
**NOTE**

Ensure that no AS policy is enabled. Disable the AS policy before configuring manual scaling. For details, see [Disabling an AS Policy](#).

**Procedure**

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Components**.
- Step 3** Mouse over the target component instance and click the displayed .

**Figure 5-9** Configuring manual scaling



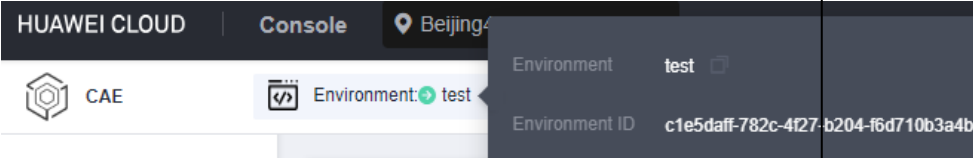
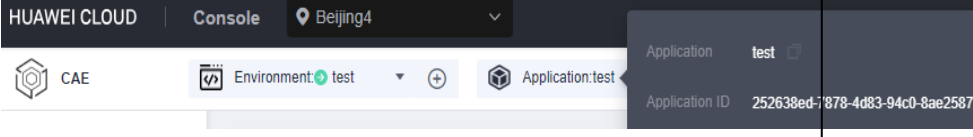
- Step 4** Enter the target number of instances, which ranges from 1 to 99.
  - Step 5** Click **OK**.
- End














**5.3.9 Related Operations**

After the component is created or deployed, you can view the environment ID, application ID, component ID, component name, code source, status, number of instances, and creation time on the **Components** page.

On the **Components** page, you can perform the following operations on created or deployed components:

**Table 5-3** Related operations

Operation	Description
View an environment ID	<p>Mouse over <b>Environment</b> to view the environment name and ID.</p> 
View an application ID	<p>Mouse over <b>Application</b> to view the application name and ID.</p> 

Operation	Description
View a component ID	<p>Mouse over a component to view its name, version, and ID.</p> 
Search for a component	Enter a component name in the search box above the component list to search for the component in fuzzy mode.
Refresh the component list	Click  in the upper right corner of the component list.
Customize columns	Click  in the upper right corner of the component list to show or hide a column.
Filter components	Click  in the <b>Code Source</b> or <b>Status</b> column to filter components.
Switch the component sorting	Click  in the <b>Name/Version/ID</b> , <b>Last Change Status/Time</b> , or <b>Created</b> column to switch the component sorting.  indicates the default sorting order,  indicates the ascending order, and  indicates the descending order.
Configure a component	Click  on the right of a component to go to the component configuration page. For details, see <a href="#">Component Configurations</a> .
View component monitoring	Click  on the right of a component to go to the component monitoring page. For details, see <a href="#">Viewing Component Monitoring</a> .
View component logs	Click  on the right of a component to go to the component log page. For details, see <a href="#">Viewing Component Logs</a> .
View component events	Click  on the right of a component to go to the component event page. For details, see <a href="#">Viewing Component Events</a> .
View change details	Click  in the <b>Last Change Status/Time</b> column of a component to view its change history.

# 6 Instance Management

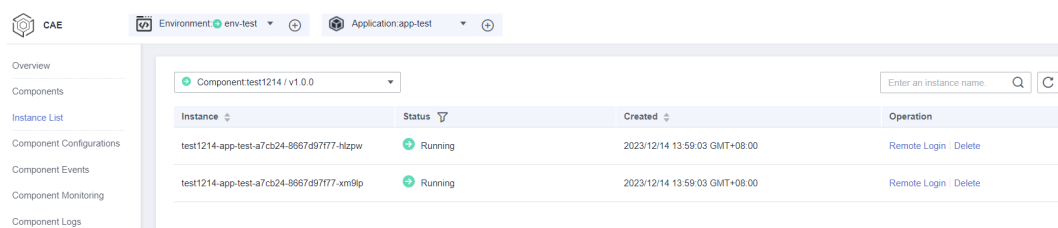
## 6.1 Viewing an Instance

After a component is created, you can view the instance details on the **Instance List** page, including the instance name, running status, and creation time.

### Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Instance List**.
- Step 3** Select the target environment and application from the drop-down lists in the upper part of the page, and click the target component.
- Step 4** View the instance name and running status.

**Figure 6-1** Instance list



----End

## 6.2 Deleting an Instance

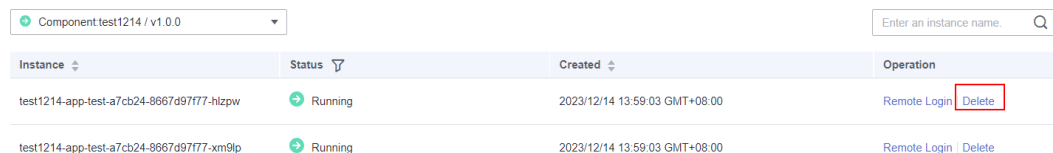
If an instance is abnormal, you can perform the following operations to delete it. You are advised to delete only the abnormal instances.

**NOTICE**

This operation will forcibly delete the instance. Ensure that data has been backed up or data loss risk assessment has been completed. Deleted instances cannot be recovered. Exercise caution when performing this operation.

**Procedure**

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Instance List**.
- Step 3** Select the target environment and application from the drop-down lists in the upper part of the page, and click the target component.
- Step 4** Select the target instance and click **Delete** in the **Operation** column.
- Step 5** In the displayed dialog box, click **OK**.

**Figure 6-2** Deleting an instance

Instance	Status	Created	Operation
test1214-app-test-a7cb24-8867d97f77-hlzp	Running	2023/12/14 13:59:03 GMT+08:00	Remote Login <b>Delete</b>
test1214-app-test-a7cb24-8867d97f77-xm9lp	Running	2023/12/14 13:59:03 GMT+08:00	Remote Login   Delete

----End

## 6.3 Logging In to a Container Using CloudShell

If unexpected problems occur when you use a container, you can use CloudShell to log in to the container for debugging.

**NOTE**

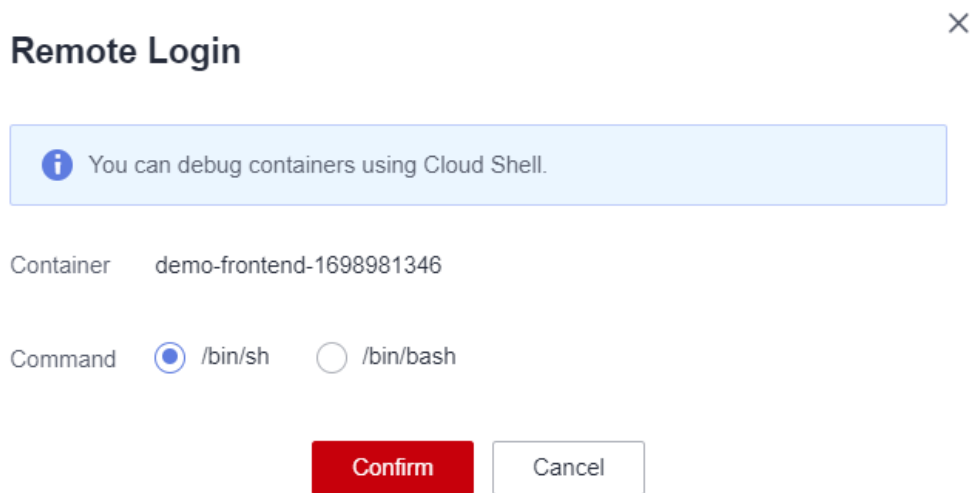
Only instances in the **Running** state support remote login.

**Procedure**

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Instance List**.
- Step 3** Select the target environment and application from the drop-down lists in the upper part of the page, and click the target component.
- Step 4** Select the target instance and click **Remote Login** in the **Operation** column.
- Step 5** In the displayed dialog box, select the command to be executed.
  - /bin/sh
  - /bin/bash



**Figure 6-3** Login command



**Step 6** Click **Confirm**.

**Step 7** Switch to CloudShell, initialize kubectl, and run the **kubectl exec** command to log in to the container.

**NOTE**

Wait until the **kubectl exec** command is automatically executed.

**Figure 6-4** Running the kubectl exec command to log in to the container



**Step 8** Run commands in CloudShell as required to view and debug your container.

----End

# 7 Component Configurations

---

## 7.1 Overview

You can configure RDS for data interaction and CSE for microservice management and governance, and configure environment variables, access modes, AS policies, cloud storage mounting, health check, lifecycle, log collection, performance management, and custom metrics for components.

### Prerequisites

1. You have created an environment. For details, see [Creating an Environment](#).
2. You have created an application. For details, see [Creating an Application](#).
3. You have created a component. For details, see [Creating a Component](#).

## 7.2 Configuring RDS

To store application data permanently, you need to use Relational Database Service (RDS). Based on the cloud computing platform, CAE provides RDS for MySQL which is reliable, scalable, easy to manage, and ready for use. [RDS for MySQL](#) enables you to easily set and scale relational databases on the cloud. Using the RDS service, you can perform nearly all necessary tasks without programming. This service simplifies operation procedures and reduces routine O&M workloads, so that you can focus on application and service development.

You can bind a cloud database in component configuration. Then, you can read environment variables to obtain MySQL information during application running to access MySQL.

### NOTE

The cloud database to be bound must be in the same VPC as the environment.

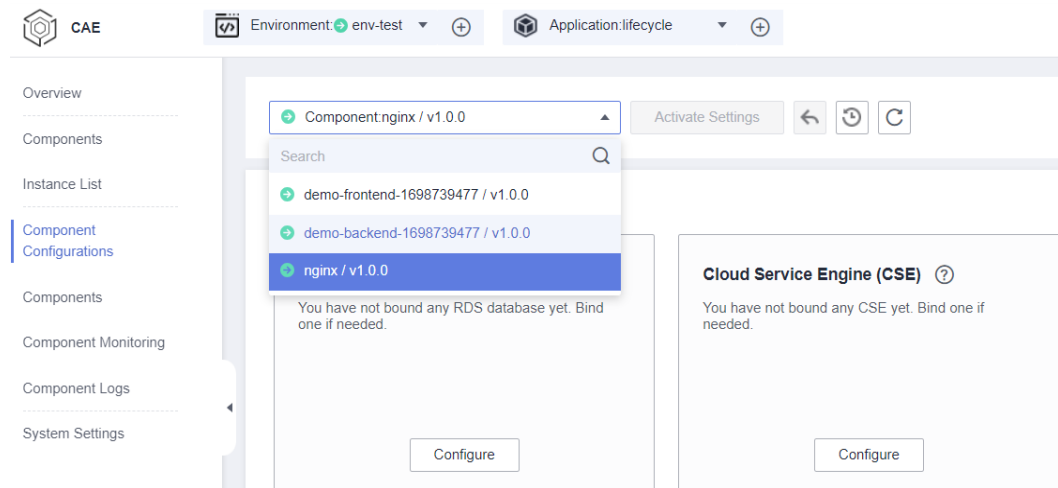
### Prerequisites

You have created an RDS MySQL DB instance. For details, see [Buy a DB Instance](#).

## Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-1** Selecting a component



- Step 4** Click **Configure** in the **Relational Database Service (RDS)** module.
- Step 5** You need to set RDS environment variables in your code when configuring an RDS instance for the first time. Available variables:

Variable	Description
RDS_ADDRESS	Private IP address of the RDS database instance
RDS_DB_NAME	Database name
RDS_USER_NAME	Database username
RDS_PASSWORD	Database password
RDS_PORT	Database port

After the configurations take effect, user code can obtain RDS database parameters through environment variables and use these parameters to connect to the databases for adding, deleting, modifying, and querying data.

For example, use GORM to connect to postgres:

```
func initDB() (*gorm.DB, error) {
// Obtain parameters from environment variables.
dbAddress := os.Getenv("RDS_ADDRESS")
dbName := os.Getenv("RDS_DB_NAME")
dbUserName := os.Getenv("RDS_USER_NAME")
dbPassword := os.Getenv("RDS_PASSWORD")
dbPort := os.Getenv("RDS_PORT")

// Use the obtained parameters to build DSN.
```

```
dbDSN := fmt.Sprintf("host=%s port=%s user=%s dbname=%s sslmode=disable password=%s",dbAddress,
5432, dbUserName, dbName, dbPassword)

// Connect to a database.
instance, err := gorm.Open("postgres", dbDSN)
if err != nil {
log.Println("connect db failed : " + err.Error())
return nil, err
}

return instance, nil
}
```

**Step 6** In the right pane, select an RDS instance.

If the existing RDS instances do not meet service requirements:

1. Click **Go to RDS Console** to create an RDS instance.
2. Click **Next** to configure and **buy** the instance.

**Step 7** Set the parameters by referring to [Table 7-1](#).

**Table 7-1** Configuring RDS

Parameter	Description
RDS Instance	You can select an RDS database instance in the same VPC as CAE.
Database	Select the target database.
Database Username	Select a user under the database.
Database Password	Enter a database password. The password is mandatory.
Confirm Password	Enter the password again.
Database Port	Enter a database port.

**Step 8** Click **Save**.

**Step 9** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## 7.3 Configuring CSE

CAE provides Cloud Service Engine (CSE) with service registry, service governance, and configuration management. It allows you to quickly develop microservice applications and implement high-availability O&M.

## Prerequisites

You have created a microservice engine instance. For details, see [Creating a ServiceComb Engine](#).

## Binding a Microservice Engine

### NOTE

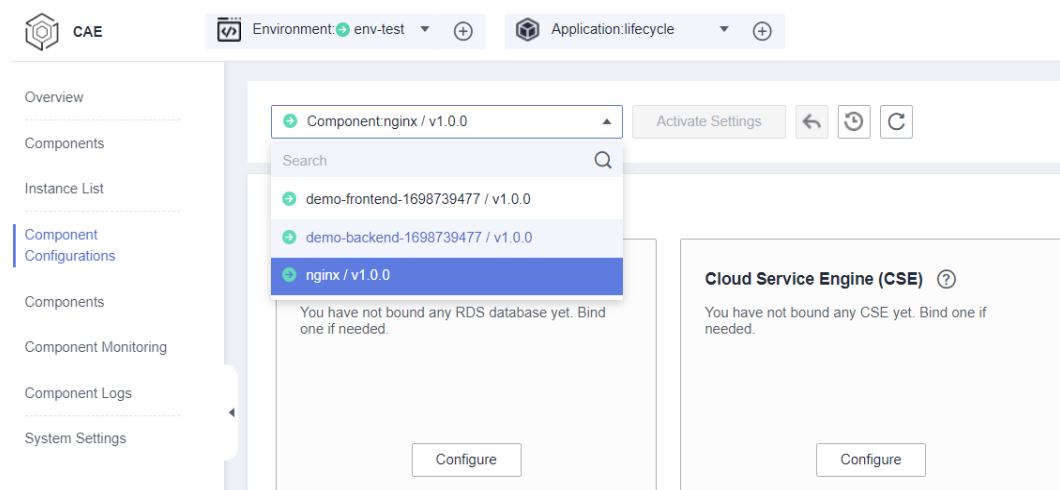
- Only microservice engines in the **Available** state can be bound.
- Multiple microservice engines cannot be bound at the same time.
- The microservice engine to be bound must be in the same VPC as the environment.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-2** Selecting a component

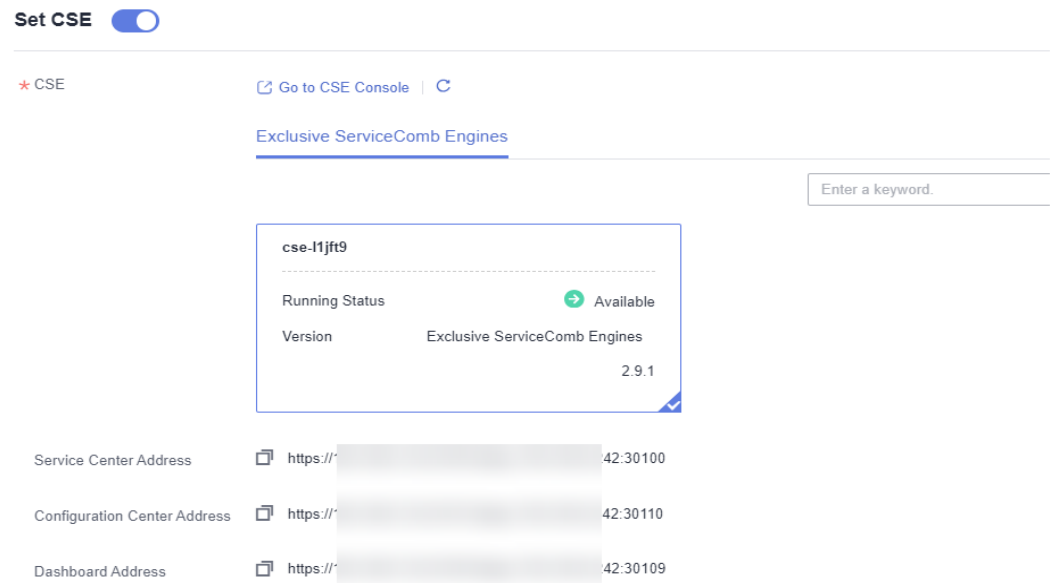


**Step 4** Click **Configure** in the **Cloud Service Engine (CSE)** module.

**Step 5** Select a microservice engine.

- Click **Exclusive ServiceComb Engines** and select a ServiceComb engine.

**Figure 7-3** Exclusive ServiceComb engines



- If the existing microservice engines do not meet service requirements:
  - a. Click **Go to CSE Console** to create a microservice engine. For details, see [Creating a ServiceComb Engine](#).
  - b. Select the created microservice engine.

**Step 6** Click **Save**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**NOTE**

- After the ServiceComb engine is bound, you can view microservice running metrics and govern microservices based on real-time dashboard data. For details, see [Using ServiceComb Engines](#).
- After the Nacos engine is bound, you can manage the services registered with the Nacos engine. For details, see [Using Nacos Engines](#).

----End

## Viewing Microservice Engine Configurations

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

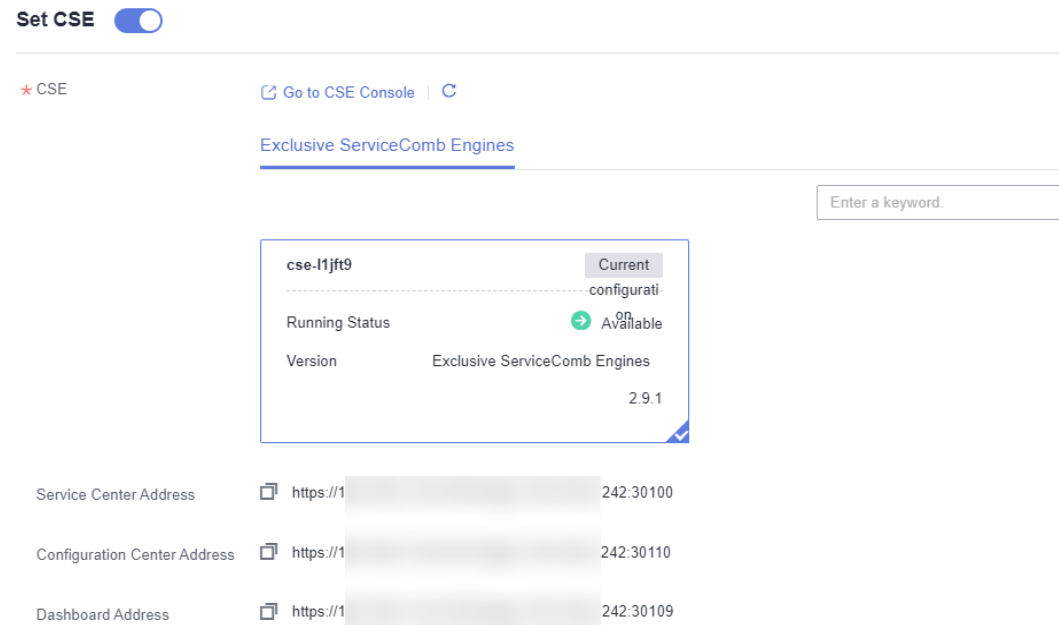
**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Configure** in the **Cloud Service Engine (CSE)** module.

**Step 5** View the microservice engine configurations, such as the name, status, version, private IP address, and binding status.

The bound microservice engine is labeled with **Current Configuration**.

**Figure 7-4** Microservice engine configurations



----End

## Modifying Microservice Engine Configurations

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Configure** in the **Cloud Service Engine (CSE)** module.

**Step 5** Select the target microservice engine and click **Save**.

**Step 6** Click **Activate Settings** in the upper part of the **Component Configurations** page.

**Step 7** In the displayed dialog box, confirm the configurations and click **OK** for the configurations to take effect.


----End

## Unbinding a Microservice Engine

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

- Step 4** Click **Configure** in the **Cloud Service Engine (CSE)** module.
- Step 5** Click  to disable CSE settings.
- Step 6** Click **Save**.
- Step 7** In the displayed dialog box, enter **SWITCHOFF** and click **OK**.
- Step 8** Click **Activate Settings** in the upper part of the **Component Configurations** page.
- Step 9** In the displayed dialog box, confirm the configurations and click **OK** for the configurations to take effect.

----End

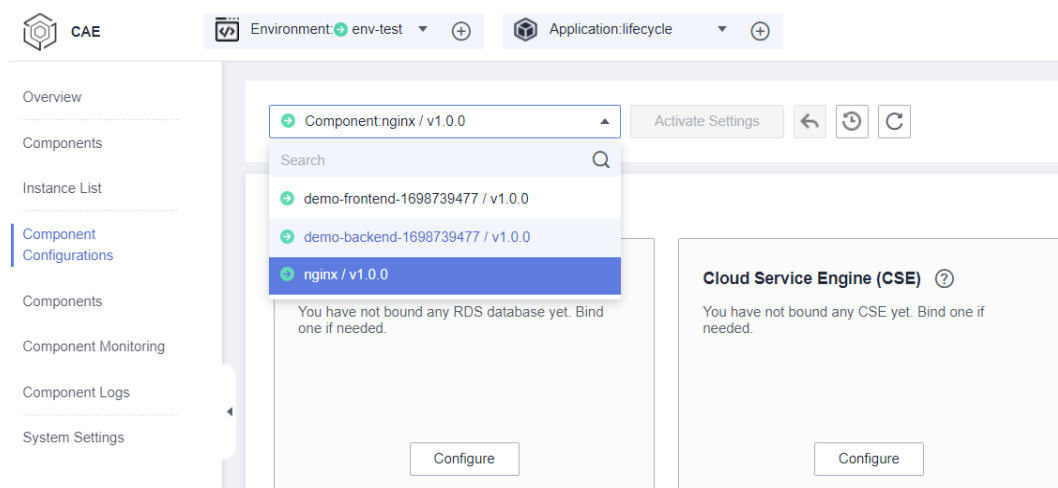
## 7.4 Configuring Environment Variables

Environment variables are parameters set in the system or user applications. You can obtain the values of environment variables by calling APIs. During deployment, parameters are specified through environment variables instead of in the code, which makes the deployment flexible.

### Adding an Environment Variable

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-5** Selecting a component



- Step 4** Click **Edit** in the **Environment Variables** module. On the right, click **Add Environment Variable**.
- Step 5** Set the parameters by referring to [Table 7-2](#).



**Table 7-2** Configuring an environment variable

Parameter	Description
Type	Select <b>Add manually</b> or <b>Import secret</b> .
Name	Name of an environment variable, which must be unique.
Variable/Variable Reference	Value of a variable. If <b>Type</b> is set to <b>Import secret</b> , select a created credential configuration from the drop-down list. For details, see <a href="#">Adding a Secret</a> .

For example, if you set **Name** to **TZ** and **Variable/Variable reference** to **Asia/Shanghai**, when the program code reads the **TZ** environment variable, **Asia/Shanghai** is obtained. You can view the time zone of Shanghai and the time difference between local and Shanghai time. The actual execution effect depends on the code.

**Figure 7-6** Configuring an environment variable

**Set Environment Variable**

Exercise caution when inputting sensitive information in configuring environment variables, or encrypt sensitive information to avoid information leakage. Examples: user privacy and database password

+ Add Environment Variable
Import
Bulk Delete

<input type="checkbox"/>	Type	Name	Variable/Variable Reference	Operation
<input type="checkbox"/>	Add manually ▾	<input type="text" value="TZ"/>	<input type="text" value="Asia/Shanghai"/>	<a href="#">Save</a>   <a href="#">Cancel</a>
<input type="checkbox"/>	Import secret	admin	test1	<a href="#">Edit</a>   <a href="#">Delete</a>
<input type="checkbox"/>	Add manually	test	123456	<a href="#">Edit</a>   <a href="#">Delete</a>

**Step 6** (Optional) Click **Import** to import the custom environment variable file.

**NOTE**

The file to import must be a key-value pair in character string format. Upload up to 200 environment variables at a time (JSON and YAML formats only). Example: {"key1": "value1", "key2": "value2"...}.

**Step 7** Click **Save** in the **Operation** column. On the **Set Environment Variable** page, click **OK**.

**Step 8** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

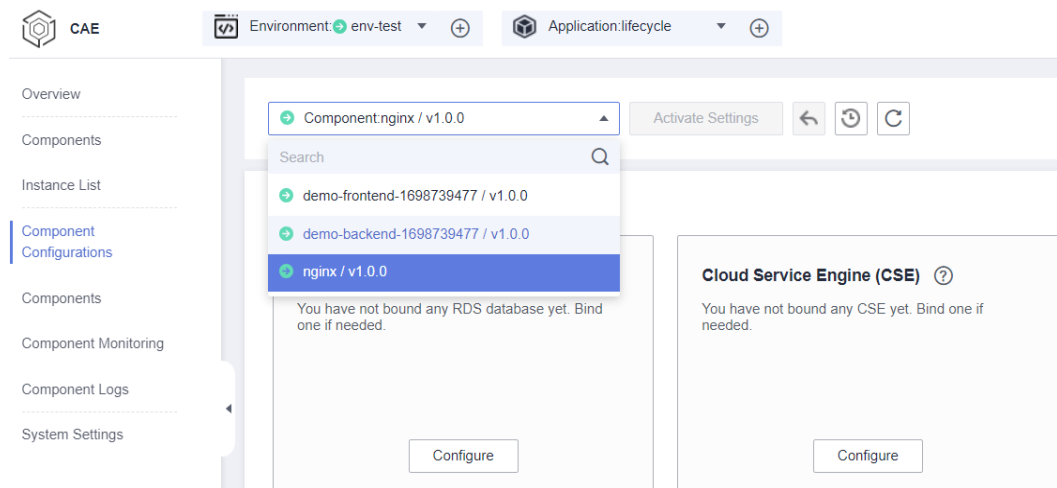
## Updating an Environment Variable

**Step 1** Log in to CAE.

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-7** Selecting a component



**Step 4** Click **Edit** in the **Environment Variables** module.

**Step 5** Select the target configuration and click **Edit** in the **Operation** column. Update the environment variable by referring to [Table 7-3](#).

**Table 7-3** Configuring an environment variable

Parameter	Description
Type	Select <b>Add manually</b> or <b>Import secret</b> .
Name	Name of an environment variable, which must be unique.
Variable/Variable Reference	Value of a variable. If <b>Type</b> is set to <b>Import secret</b> , select a created credential configuration from the drop-down list. For details, see <a href="#">Adding a Secret</a> .

**Step 6** Click **Save** in the **Operation** column. On the **Set Environment Variable** page, click **OK**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

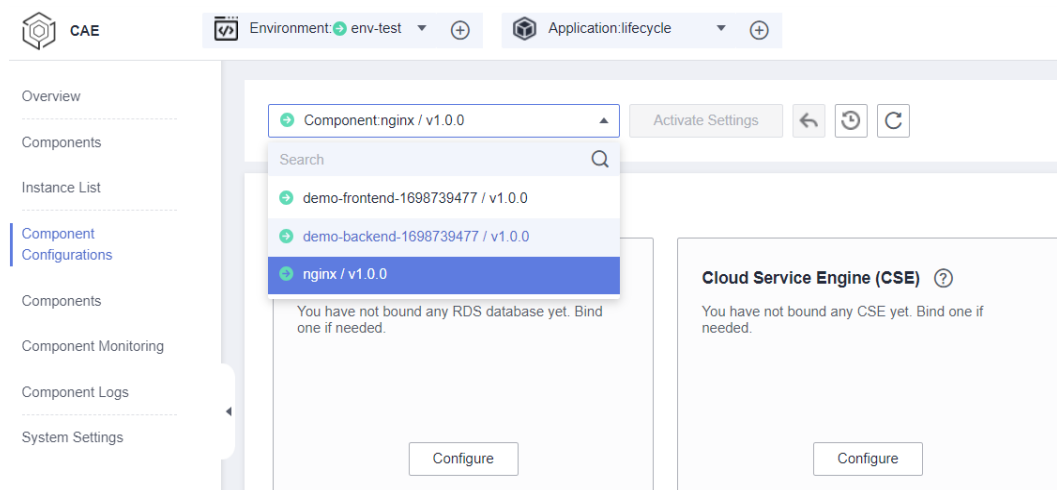
## Deleting an Environment Variable

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

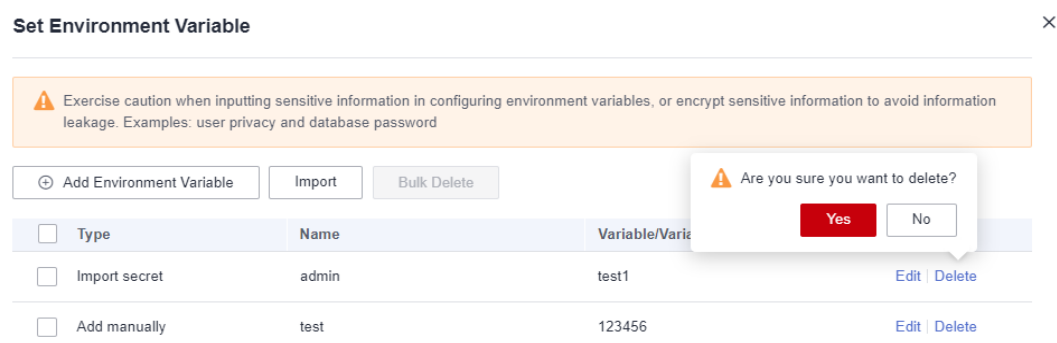
**Figure 7-8** Selecting a component



**Step 4** Click **Edit** in the **Environment Variables** module.

**Step 5** Select the target configuration and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

**Figure 7-9** Deleting an environment variable



**Step 6** On the **Set Environment Variable** page, click **OK**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## 7.5 Configuring the Access Mode

### 7.5.1 Configuring Access Ports in the Environment

This section describes how to configure the ports for other components in the environment to access the component. After configuration, log in to the cluster node and run the `curl` command to access the component.

#### Prerequisites

You have [created an application](#) and [component](#).

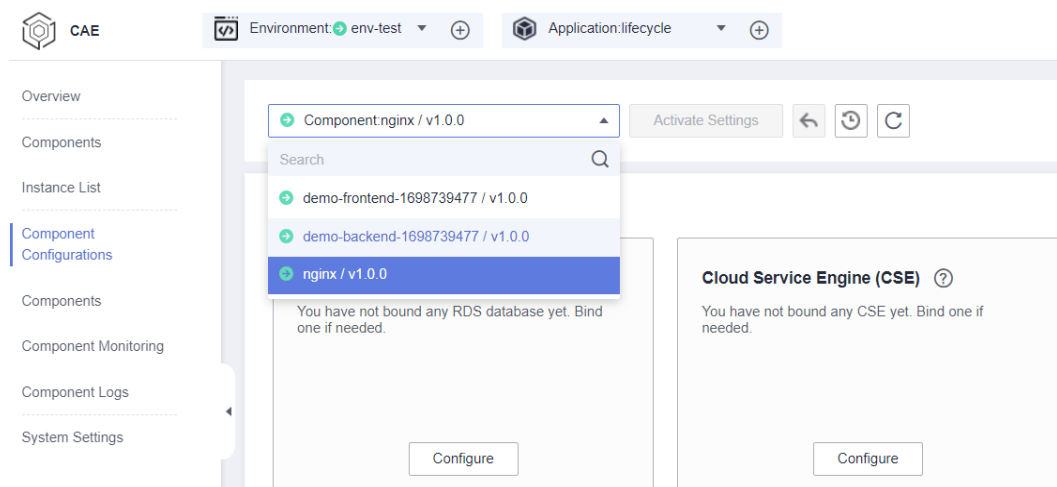
#### Adding a Port Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-10** Selecting a component



**Step 4** Click **Edit** in the **Access Mode** module.

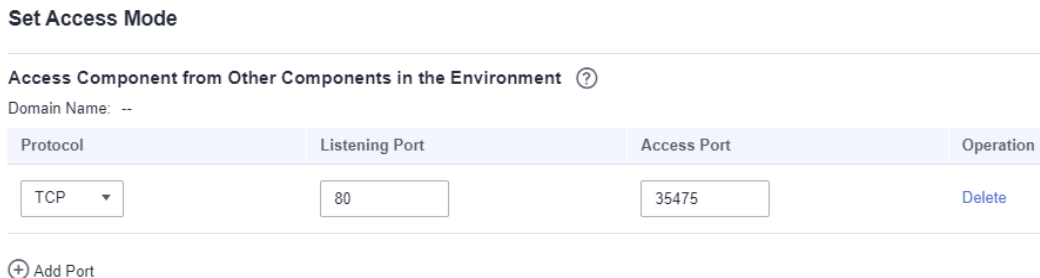
**Step 5** In the **Access Component from Other Components in the Environment** area, click **Add Configuration** and set parameters by referring to [Table 7-4](#).

**Table 7-4** Configuring private network access

Parameter	Description
Protocol	TCP and UDP are supported.
Listening Port	Listening port of program in a component, which is obtained from the user program code. Value range: 1 to 65535.
Access Port	Port provided by a component for external access, which is set by user and must be unique. Value range: 1 to 65535.

If TCP is used, the listening port is 80 and the access port is 35475. After the configurations take effect, log in to the cluster node and run the **curl** command to access the component.

**Figure 7-11** Configuring private network access



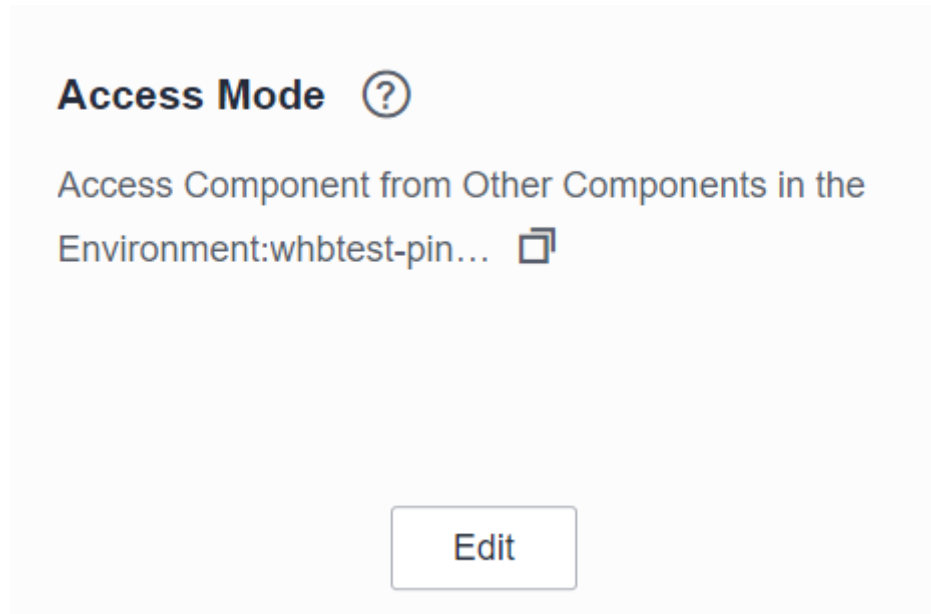
**Step 6** (Optional) To add more port configurations, click **Add Port** and set parameters by referring to [Table 7-4](#).

**Step 7** Click **OK**.

**Step 8** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

Figure 7-12 Private network access

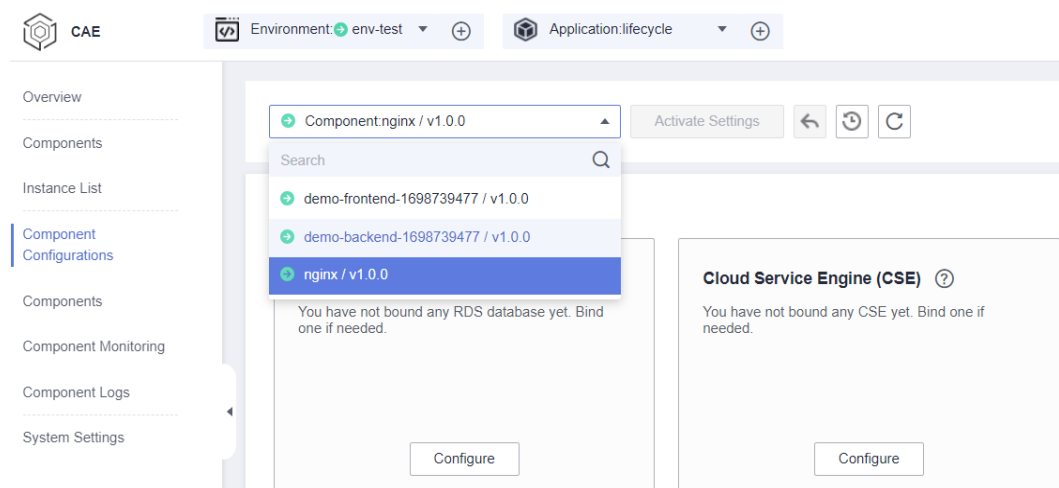


----End

## Modifying a Port Configuration

- Step 1** Log in to CAE.
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

Figure 7-13 Selecting a component



- Step 4** Click **Edit** in the **Access Mode** module.
- Step 5** In the **Access Component from Other Components in the Environment** area, modify parameters by referring to **Table 7-5**.

**Table 7-5** Configuring private network access

Parameter	Description
Protocol	TCP and UDP are supported.
Listening Port	Listening port of program in a component, which is obtained from the user program code. Value range: 1 to 65535.
Access Port	Port provided by a component for external access, which is set by user and must be unique. Value range: 1 to 65535.

**Step 6** Click **OK**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## Deleting a Port Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

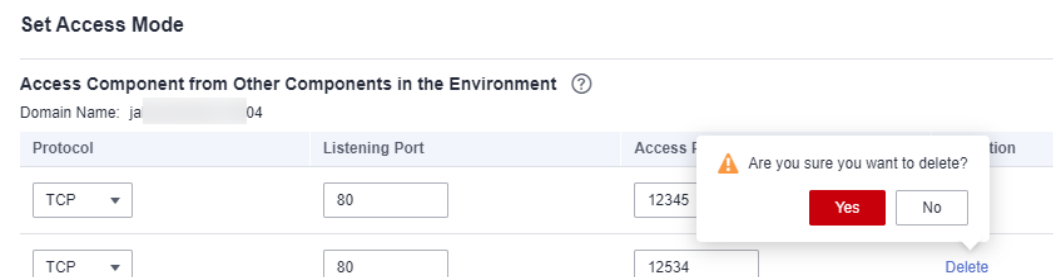
**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Access Mode** module.

**Step 5** In the **Access Component from Other Components in the Environment** area, select the target port configuration and click **Delete** in the **Operation** column.

**Step 6** In the displayed dialog box, click **Yes**.

**Figure 7-14** Deleting a port configuration



**Step 7** Click **OK**.

**Step 8** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## 7.5.2 Configuring Load Balancing

This section describes how to configure the endpoint for component access from outside the environment. Access it from your VPC or Internet.

CAE allows you to configure multiple load balancers at the same time to implement multiple access modes for a component.

### NOTE

Up to 10 load balancers can be configured for a component at the same time.

### Prerequisites

You have [created an application](#) and [component](#).

### Adding a Load Balancing Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Access Mode** module.

**Step 5** In the **Access Component from Another Environment** area, click **Load Balancing > Add Load Balancer**.

**Step 6** On the **Create Load Balancer** page, set parameters by referring to [Table 7-6](#).



**Table 7-6** Configuring load balancing for public network access

Parameter	Description
Load Balancer	<p>You can select <b>Dedicated</b> or <b>Built-in load balancer</b>.</p> <ul style="list-style-type: none"> <li>• If you select <b>Built-in load balancer</b>, only EIP-based public network access is supported.</li> <li>• If you select <b>Dedicated</b>, select the corresponding load balancer from the drop-down list.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- To use a <b>Dedicated</b> load balancer, <a href="#">add the configuration for VPC to access the CAE environment</a> first.</li> <li>- Only load balancers in the environment's VPC are supported.</li> <li>- You can configure an EIP for the load balancer to access CAE components from public network.</li> </ul> <p>If no load balancer is available, click <b>Create Load Balancer</b> to create a load balancer. For details, see <a href="#">Creating a Dedicated Load Balancer</a>.</p>

Parameter	Description
Health Check	<p>The health check is for the load balancer.</p> <ul style="list-style-type: none"> <li>● <b>Disable</b></li> <li>● <b>Enable:</b> default. <ul style="list-style-type: none"> <li>- Protocol Protocol type of a health check request. Value: <b>TCP</b> or <b>HTTP</b>. Default value: <b>TCP</b>.</li> </ul> </li> </ul> <p><b>NOTE</b> The protocol cannot be directly switched. To switch the protocol, disable it before selecting another one.</p> <ul style="list-style-type: none"> <li>- Check Path This parameter is mandatory when <b>Protocol</b> is set to <b>HTTP</b>. Health check URL. The path must start with a slash (/) and contain 1 to 80 characters. It can contain letters, digits, and the following characters: <code>-.%?&amp;_</code>.</li> <li>- Check Interval (s) Interval for sending health check requests, in seconds. Value range: 1 to 50. Default value: <b>5</b>.</li> <li>- Timeout (s) Maximum time required for waiting for a response from the health check, in seconds. Value range: 1 to 50. Default value: <b>10</b>.</li> <li>- Max. Retries Maximum number of health check retries. Value range: 1 to 10. Default value: <b>3</b>.</li> </ul>
Access Control	<p>You can create an access control policy to allow or forbid an IP address to access a component. The value can be an IP address or an IP network segment.</p> <ul style="list-style-type: none"> <li>● Allow all IP addresses</li> <li>● Whitelist Only IP addresses in the whitelist are allowed to access the component.</li> <li>● Blocklist IP addresses in the blocklist are forbidden to access the component.</li> </ul>

Parameter	Description
Port Settings	<ul style="list-style-type: none"> <li>• <b>Protocol:</b> TCP and UDP are supported.</li> <li>• <b>Listening Port:</b> listening port of the program in a component, which is obtained from the user program code. Value range: 1 to 65535.</li> <li>• <b>Access Port:</b> port provided by a component for external access, which is set by user and must be unique. Value range: 1 to 65535.</li> </ul>

**Figure 7-15** Configuring load balancing

**Load Balancing** Load Balancing and Route Configuration

Load Balancer: Built-in load ba... ▾

Health Check: Disable Enable

Protocol: TCP | Check Interval (s): 5 | Timeout (s): 10 | Max. Retries: 3 [✎](#)

Access Control: Whitelist ▾

Whitelist [?](#)

100  
192  
172

Port Settings

Protocol	Listening Port	Access Port	Operation
TCP ▾	80	8090	Delete

[+ Add Port](#)

**Figure 7-16** Configuring health check

**Health Check Settings** ✕

Protocol: TCP HTTP

Check Path:

Check Interval (s):

Timeout (s):

Max. Retries:

Confirm
Cancel

**Step 7** Click **OK**.

**Step 8** (Optional) To add more load balancing configurations, repeat **Step 5** to **Step 7**.

**Step 9** Click **OK**.

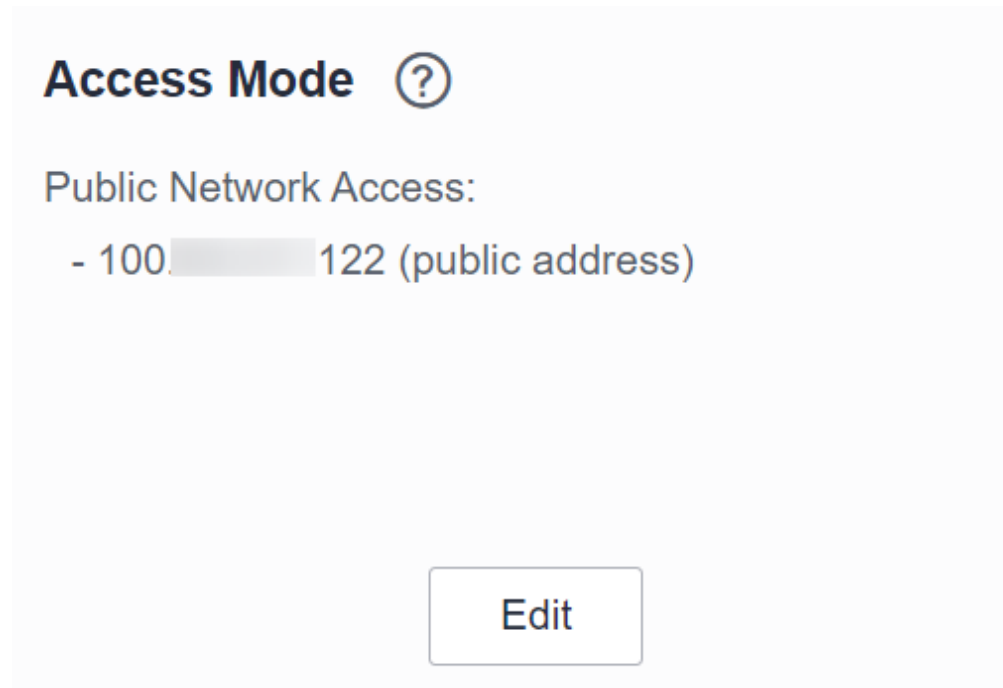
**Step 10** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

If a Nginx component is used, the protocol is TCP, listening port is 80, and access port is 8089. After deployment, choose **Components**, click the public network address in the **Access Address** column of the Nginx component to view its static web page.

If you have configured an access control whitelist or blacklist, only IP addresses in the whitelist or not in the blacklist can access the component.

**Figure 7-17** Public network access

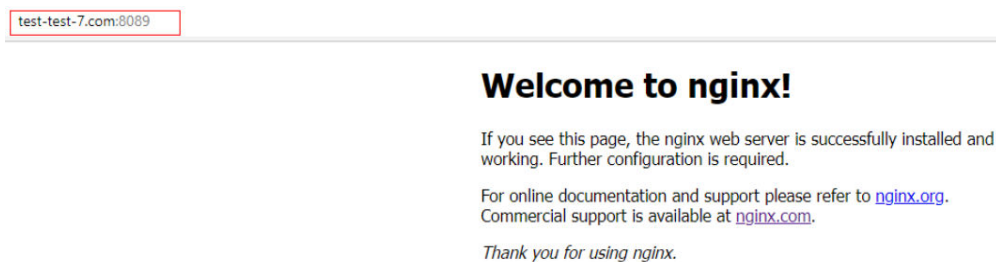


You can also use a domain name for access, for example, `http://test-test-7.com:8089`, if you have **added a domain name** and bound it.

**Figure 7-18** Configuring a domain name



**Figure 7-19** Access using a domain name



----End

## Modifying a Load Balancing Configuration

- Step 1** [Log in to CAE.](#)
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.
- Step 4** Click **Edit** in the **Access Mode** module.
- Step 5** In the **Access Component from Another Environment** area, click **Load Balancing**.
- Step 6** Find the target configuration item and click **Edit** in the **Operation** column.

**Figure 7-20** Modifying a load balancing configuration



**Step 7** Modify parameter settings by referring to [Table 7-6](#).

**Step 8** Click **OK**.

**Step 9** Click **OK**.

**Step 10** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## Deleting a Load Balancing Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

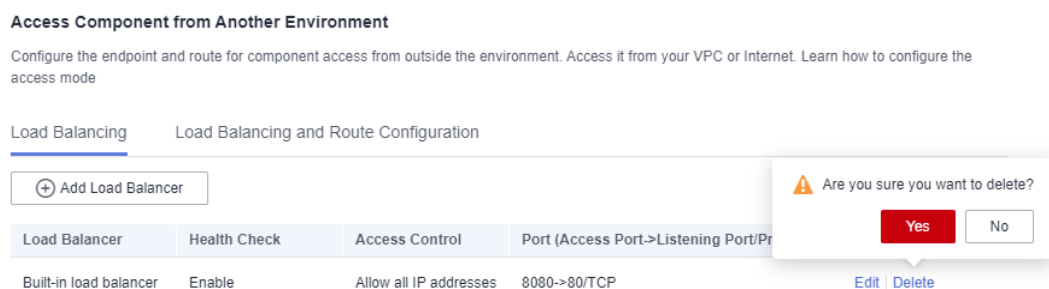
**Step 4** Click **Edit** in the **Access Mode** module.

**Step 5** In the **Access Component from Another Environment** area, click **Load Balancing**.

**Step 6** Find the target configuration item and click **Delete** in the **Operation** column.

**Step 7** In the displayed dialog box, click **Yes**.

**Figure 7-21** Deleting a Load Balancing Configuration



**Step 8** Click **OK**.

**Step 9** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

### 7.5.3 Configuring Load Balancing and Route

This section describes how to configure the endpoint and route for component access from outside the environment. Access it from your VPC or Internet.

CAE allows you to configure multiple load balancers at the same time to implement multiple access modes for a component.

#### NOTE

Up to 10 load balancers can be configured for a component at the same time.

#### Prerequisites

You have [created an application](#) and [component](#).

#### Configuring Load Balancing and Route

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.
- Step 4** Click **Edit** in the **Access Mode** module.
- Step 5** In the **Access Component from Another Environment** area, click **Load Balancing and Route Configuration > Add Load Balancing and Route Configuration**.
- Step 6** On the **Create Load Balancing and Route Configuration** page, select a load balancer and configure a load balancing policy by referring to [Table 7-8](#).

**Table 7-7** Selecting a load balancer

Parameter	Description
Load Balancer	<p>You can select <b>Dedicated</b> or <b>Built-in load balancer</b>.</p> <ul style="list-style-type: none"> <li>• If you select <b>Built-in load balancer</b>, only EIP-based public network access is supported.</li> <li>• If you select <b>Dedicated</b>, select the corresponding load balancer from the drop-down list.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- To use a <b>Dedicated</b> load balancer, <a href="#">add the configuration for VPC to access the CAE environment</a> first.</li> <li>- Only load balancers in the environment's VPC are supported.</li> </ul> <p>If no load balancer is available, click <b>Create Load Balancer</b> to create a load balancer. For details, see <a href="#">Creating a Dedicated Load Balancer</a>.</p>



**Table 7-8** Configuring a load balancing policy

Parameter	Description
Policy	<p>You can select <b>Weighted round robin</b>, <b>Weighted least connections</b>, or <b>Source IP hash</b>.</p> <ul style="list-style-type: none"> <li>• <b>Weighted round robin:</b> Requests are forwarded to different servers based on their weights, which indicate server processing performance. Backend servers with higher weights receive proportionately more requests, whereas equal-weighted servers receive the same number of requests. This algorithm is often used for short connections, such as HTTP services.</li> <li>• <b>Weighted least connections:</b> In addition to the weight assigned to each server, the number of connections processed by each backend server is also considered. Requests are forwarded to the server with the lowest connections-to-weight ratio. Building on least connections, the weighted least connections algorithm assigns a weight to each server based on their processing performance. This algorithm is often used for persistent connections, such as database connections.</li> <li>• <b>Source IP hash:</b> The source IP address of each request is calculated using the hash algorithm to obtain a unique hash key, and all backend servers are numbered. The generated key allocates the client to a particular server. This allows requests from different clients to be routed based on source IP addresses and ensures that a client is directed to the same server as always. This algorithm applies to TCP connections without cookies.</li> </ul>

Parameter	Description
Sticky Session	<p>This parameter is available when <b>Policy</b> is set to <b>Weighted round robin</b> or <b>Weighted least connections</b>.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: default.</li> <li>• <b>Application cookie</b>: A cookie will be generated after receiving a request from the client. All subsequent requests with the cookie are routed to the same backend server.</li> </ul>
Health Check	<p>The health check is for the load balancer.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: default.</li> <li>• <b>HTTP</b>: initiates an HTTP request.</li> <li>• <b>TCP</b>: specifies a port for TCP connections.</li> </ul>

**Step 7** Set the parameters by referring to [Table 7-9](#) and [Table 7-10](#).

**Table 7-9** Configuring a listener

Parameter	Description
*External Protocol	<p><b>HTTP</b> and <b>HTTPS</b> are supported. Default value: <b>HTTPS</b>.</p>
*Access Port	<p>The default value is <b>443</b> for <b>HTTPS</b> and <b>80</b> for <b>HTTP</b>. Value range: 1 to 65535. The port number must be unique.</p>

Parameter	Description
Access Control	<p>This parameter is available when you select <b>Built-in load balancer</b> for <b>Load Balancer</b>.</p> <p>You can create an access control policy to allow or forbid an IP address to access a component. The value can be an IP address or an IP network segment.</p> <ul style="list-style-type: none"> <li>• Allow all IP addresses</li> <li>• Whitelist Only IP addresses in the whitelist are allowed to access the component.</li> <li>• Blocklist IP addresses in the blocklist are forbidden to access the component.</li> </ul> <p><b>NOTE</b></p> <p>In the access mode configuration, the same access port of the same load balancer can have only one access control configuration. Therefore, pay attention to the following:</p> <ul style="list-style-type: none"> <li>- If you select <b>Built-in load balancer</b> for <b>Load Balancer</b> and configure multiple routing rules for the same port, the access control configurations of these routing rules must be the same.</li> <li>- If you select <b>Dedicated</b> for <b>Load Balancer</b>, access control cannot be configured on CAE. Each time you configure a port, a listener is created on the selected load balancer. You can configure access control for the listener corresponding to the port by referring to <a href="#">What Is Access Control?</a></li> </ul>

Parameter	Description
Security Policy	<p>The value cannot be changed after being set.</p> <ul style="list-style-type: none"> <li>• <b>TLS-1-2</b> supports TLS 1.2 and corresponding cipher suites (moderate compatibility and high security).</li> <li>• <b>TLS-1-0</b> supports TLS 1.0, 1.1, and 1.2 and corresponding cipher suites (ultra-high compatibility and low security).</li> <li>• <b>TLS-1-1</b> supports TLS 1.1 and 1.2 and corresponding cipher suites (moderate compatibility and high security).</li> <li>• <b>TLS-1-2-STRICT</b> supports TLS 1.2 and corresponding cipher suites (fair compatibility and high security).</li> </ul> <p><b>NOTE</b> The security policies in an environment must be the same.</p>
*Default Server Certificate	<p>Select a certificate from the drop-down list.</p> <p>This parameter is available when <b>External Protocol</b> is set to <b>HTTPS</b>.</p> <p>To add a certificate, click <b>Add Certificate</b>. For details, see <a href="#">Adding a Certificate</a>.</p>
SNI	<p>Select a domain name and the corresponding certificate from the drop-down list.</p> <p>This parameter is available when <b>External Protocol</b> is set to <b>HTTPS</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• If many domain names are bound and the corresponding certificates need to be configured, configure <b>SNI</b>.</li> <li>• If it is not configured, all domain names are resolved using <b>Default Server Certificate</b>.</li> </ul>

**Table 7-10** Forwarding policy

Parameter	Description
Domain Name	Select a domain name from the drop-down list.  <b>NOTE</b> To add a domain name, select <b>Configure new domain name</b> . For details, see <a href="#">Adding a Domain Name</a> .
Match URL By	You can select <b>Prefix</b> , <b>Regular expression</b> , or <b>Exact</b> . <ul style="list-style-type: none"> <li>• <b>Prefix:</b> URLs whose prefix is the same as the specified one can be accessed, for example, <b>/healthz/v1</b> and <b>/healthz/v2</b>.</li> <li>• <b>Regular expression:</b> The URL rule can be set, for example, <b>/[A-Za-z0-9_.-]+/test</b>. All URLs that comply with this rule can be accessed, for example, <b>/abcA9/test</b> and <b>/v1-Ab/test</b>. Two regular expression standards are supported: POSIX and Perl.</li> <li>• <b>Exact:</b> Only the URL that is the same as the specified one can be accessed. For example, if the URL is set to <b>/healthz</b>, only <b>/healthz</b> can be accessed.</li> </ul>
URL	Start with a slash (/) and use letters, digits, and special characters <code>_~'!@^-%#&amp;\$.*+?,=!: /()[]{};</code> , for example: <b>/healthz</b> .
Listening Port	Value range: 1 to 65535.

**Figure 7-22** Load balancing and route configuration

**Access Component from Another Environment**

Configure the endpoint and route for component access from outside the environment. Access it from your VPC or Internet. Learn how to configure the access mode

Load Balancing [Load Balancing and Route Configuration](#)

Load Balancer

Load Balancing Policy Weighted round robin [Customize](#)

Listener

External Protocol	<input type="text" value="HTTP"/>
Access Port	<input type="text" value="13456"/>
Access Control	<input type="text" value="Blocklist"/>
Blocklist <span>?</span>	<input type="text" value="100"/>

Forwarding Policy

Domain Name	Match URL By	URL	Component	Listening ...	Opera...
<input type="text" value="test-tes..."/>	<input type="text" value="Prefix"/>	<input type="text" value="/"/>	pingtest	<input type="text" value="80"/>	<a href="#">Delete</a>
<input type="text" value="ssss.com"/>	<input type="text" value="Prefix"/>	<input type="text" value="/tmp"/>	pingtest	<input type="text" value="80"/>	<a href="#">Delete</a>

The access address consists of a domain name and access port. For example, if the domain name is test-test-16.com and the access port is 13456, the access address is http://test-test-16.com:13456/.

**Step 8** Click **OK**.

**Step 9** (Optional) To add more load balancing and route configurations, repeat **Step 5** to **Step 8**.

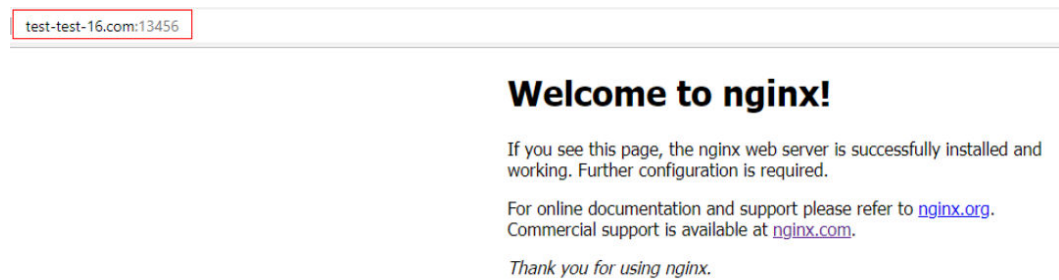
**Step 10** Click **OK**.

**Step 11** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**Step 12** Choose **Components**, click the IP address (example: **http://test-test-16.com:13456/**) in the **Access Address** column of the component to view its static web page. If you have configured an access control whitelist or blocklist, only IP addresses in the whitelist or not in the blocklist can access the component.

**Figure 7-23** Accessing a static page

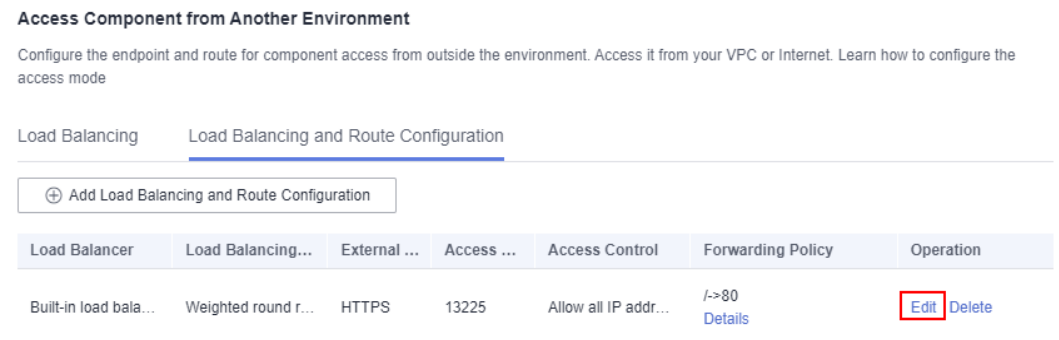


----End

## Modifying a Load Balancing and Route Configuration

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.
- Step 4** Click **Edit** in the **Access Mode** module.
- Step 5** In the **Access Component from Another Environment** area, click **Load Balancing and Route Configuration**.
- Step 6** Find the target configuration item and click **Edit** in the **Operation** column.

**Figure 7-24** Modifying a load balancing and route configuration



- Step 7** Modify parameter by referring to [Table 7-8](#), [Table 3 Configuring a listener](#), and [Table 7-10](#).
- Step 8** Click **OK**.
- Step 9** Click **OK**.
- Step 10** Make the configurations take effect.
  - If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## Deleting a load balancing and route configuration

**Step 1** Log in to CAE.

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

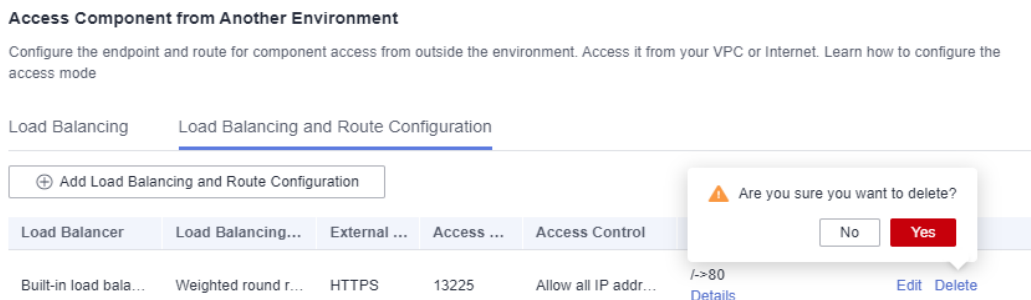
**Step 4** Click **Edit** in the **Access Mode** module.

**Step 5** In the **Access Component from Another Environment** area, click **Load Balancing and Route Configuration**.

**Step 6** Find the target configuration item and click **Delete** in the **Operation** column.

**Step 7** In the displayed dialog box, click **Yes**.

**Figure 7-25** Deleting a load balancing and route configuration



**Step 8** Click **OK**.

**Step 9** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## 7.6 Configuring an AS Policy

### 7.6.1 Configuring a Metric AS Policy

This section describes how to configure a metric AS policy. Currently, instances can be automatically added or deleted based on CPU, memory thresholds, and custom



metrics. This frees you from repeatedly adjusting resources to keep up with service changes and peak pressures, helping you reduce resources and labor costs.

**NOTE**

CAE instance scaling is calculated by current and expected metrics.

Expected instances = ceil [Current instances \* (Current metrics/Expected metrics)] (ceil is rounded up.)

There is an error tolerance of 10% to prevent frequent fluctuation of instance quantity, so there is no scaling when Current metrics/Expected metric ranges from 0.9 to 1.1.

## Application Scenario

This policy is useful for burst traffic and typical periodic traffic, mainly in industries such as the Internet, games, and social platforms.

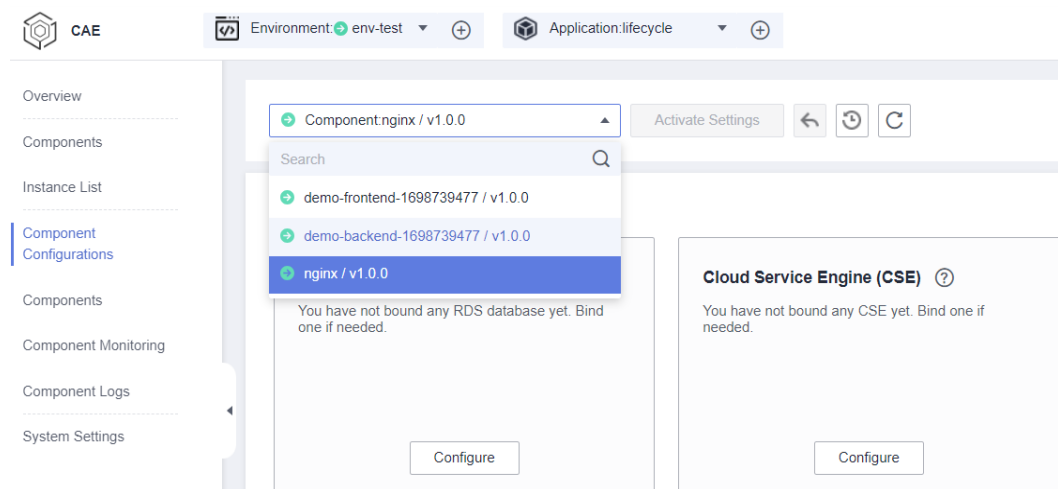
## Procedure

**Step 1** Log in to CAE.

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-26** Selecting a component



**Step 4** Click **Edit** in the **AS Policies** module.

**Step 5** Select **Metric** and configure the policy by referring to [Table 7-11](#).

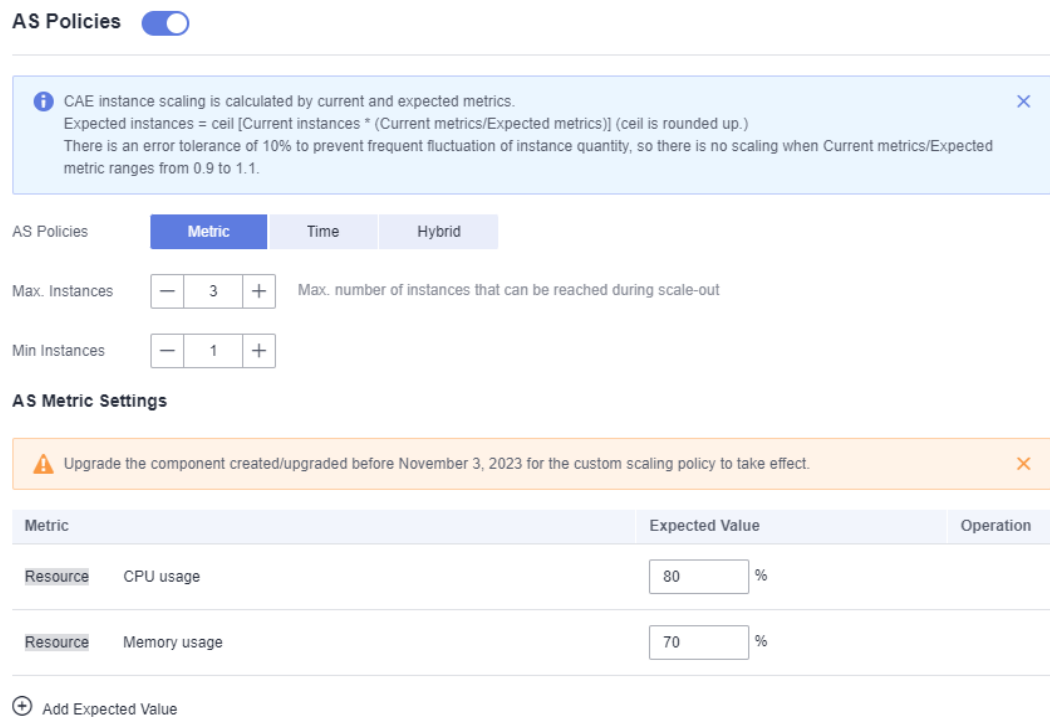
**Table 7-11** Configuring a metric policy

Parameter	Description
Max. Instances	Max. number of instances that can be reached during scale-out. Value range: 1 to 99. <b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b> .
Min Instances	Min number of instances that can be reached during scale-in. Value range: 1 to 99.
Metric	<ul style="list-style-type: none"> <li>• CPU usage, a preset metric in the system</li> <li>• Memory usage, a preset metric in the system</li> <li>• Custom metrics. Click <b>Add Expected Value</b> and select a custom metric from the drop-down list to add a custom metric. For details about how to create a custom metric, see <a href="#">Configuring Custom Metrics</a>. You can add multiple custom metrics.</li> </ul> <b>NOTE</b> <ul style="list-style-type: none"> <li>- You must enter a PromQL statement. PromQL is a built-in data query language from Prometheus, and is used to select, aggregate, and perform logical calculation on time series data. For details, see <a href="#">Prometheus</a>.</li> <li>- The query result of the PromQL statement must be a single value of the vector or scalar type.</li> <li>- Upgrade the component created/ upgraded before November 3, 2023 for the custom scaling policy to take effect.</li> </ul>

You can scale instances based on the CPU and memory thresholds.

For example, set the maximum expected CPU usage to 80 and memory usage to 70. When the CPU usage of a component is greater than 80% or the memory usage is greater than 70%, the system automatically increases the number of component instances. When the CPU usage of a component is less than 80% and the memory usage is less than 70%, the system automatically reduces the number of component instances.

**Figure 7-27** Configuring a metric policy



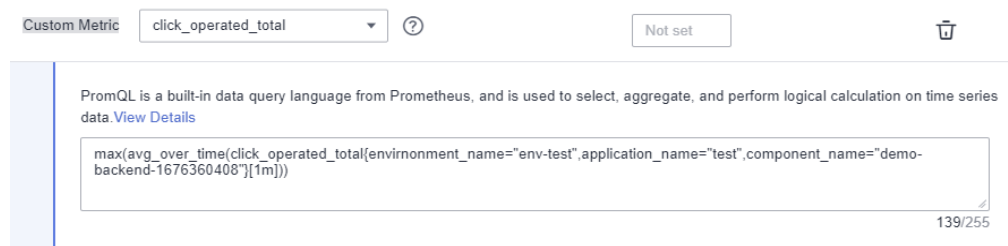
You can scale instances based on the custom metrics.

For example, select **click\_operated\_total** from the drop-down list, enter the PromQL statement

**max(avg\_over\_time(click\_operated\_total{environment\_name="env-test",application\_name="test",component\_name="demo-backend-1676360408"}[1m]))**, and set the expected value to **10**.


- The PromQL statement indicates the maximum average value of **click\_operated\_total** per minute of all the **demo-backend-1676360408** component instances.
- If the value of the PromQL statement is greater than the expected value, the system automatically increases the number of component instances.
- If the value of the PromQL statement is less than the expected value, the system automatically reduces the number of component instances.

**Figure 7-28** Configuring a custom metric policy

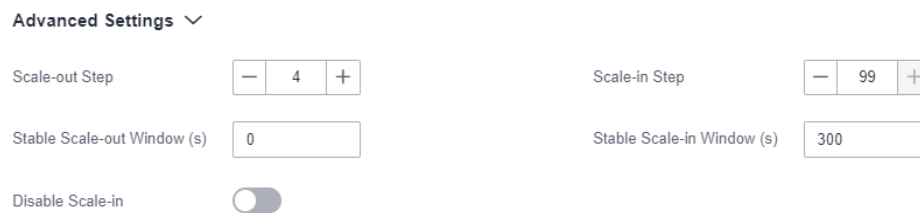


**Step 6** (Optional) Expand **Advanced Settings** and configure advanced settings by referring to [Table 7-12](#).

**Table 7-12** Configuring advanced settings

Parameter	Description
Scale-out Step	Number of pods to be added per minute. Value range: 1 to 99. Default value: <b>4</b> .
Stable Scale-out Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>0</b> .
Scale-in Step	Number of pods to be reduced per minute. Value range: 1 to 99. Default value: <b>99</b> .
Stable Scale-in Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>300</b> .
Disable Scale-in	Click  to disable scale-in.

**Figure 7-29** Advanced settings



**Step 7** Click **OK**.

**Step 8** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.6.2 Configuring a Time AS Policy

This section describes how to configure a time AS policy. You can configure a time policy to periodically scale instances. This frees you from repeatedly adjusting resources to keep up with service changes and peak pressures, helping you reduce resources and labor costs.

### NOTE

CAE instance scaling is calculated by current and expected metrics.

Expected instances = ceil [Current instances \* (Current metrics/Expected metrics)] (ceil is rounded up.)

There is an error tolerance of 10% to prevent frequent fluctuation of instance quantity, so there is no scaling when Current metrics/Expected metric ranges from 0.9 to 1.1.

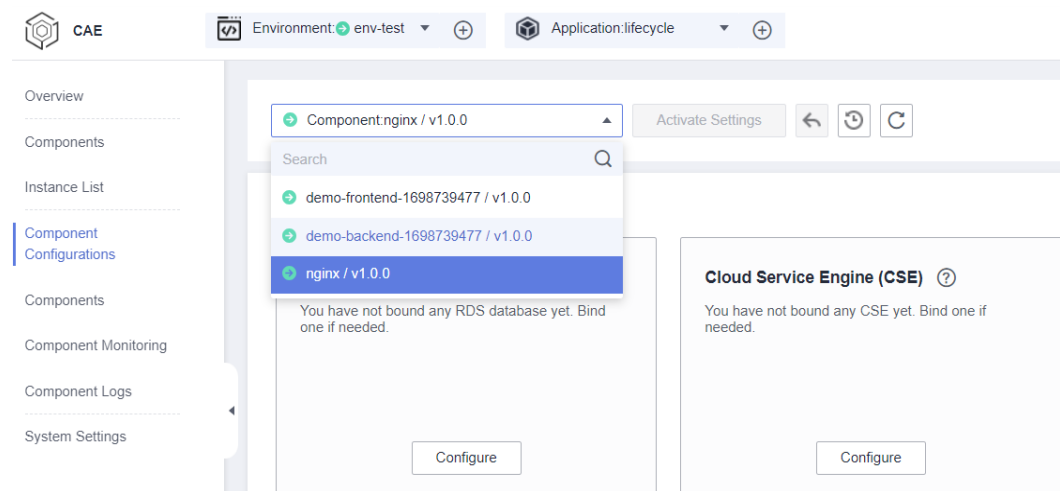
## Application Scenario

This policy is useful for periodic resource usage, mainly in industries such as securities, healthcare, and education.

## Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-30** Selecting a component



- Step 4** Click **Edit** in the **AS Policies** module.
- Step 5** Select **Time** and configure the policy by referring to [Table 7-13](#).

**Table 7-13** Configuring a time policy

Parameter	Description
Max. Instances	Max. number of instances that can be reached during scale-out. Value range: 1 to 99. <b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b> .
Min Instances	Min number of instances that can be reached during scale-in. Value range: 1 to 99.
Trigger Cycle	The policy is expected to be executed at a specified interval. Value: <b>Every day</b> , <b>Every day</b> , or <b>Monthly</b> .

Parameter	Description
Trigger Time in a Day	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every day</b>. Configure the policy triggered every day. For example, the number of instances remains 3 after 18:00 every day. Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Week	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every week</b>. Configure the policy triggered every week. For example, the number of instances remains 4 after 08:00 on every Monday. Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Month	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Monthly</b>. Configure the policy triggered every month. For example, the number of instances remains 4 after 06:00 on the fifth day of each month. Click <b>Add Trigger Time</b> to add more time policies.</p>

You can configure time segments to control instance scaling.

For example, set **Trigger Cycle** to **Every day**, and set **From 18:00** and **Instances 3**, and **From 00:00** and **Instances 1**. The system keeps 1 instance from 00:00 to 18:00, and 3 instances from 18:00 to 00:00 every day.

**Figure 7-31** Configuring a time policy

AS Policies

**i** CAE instance scaling is calculated by current and expected metrics.  
 Expected instances = ceil [Current instances \* (Current metrics/Expected metrics)] (ceil is rounded up.)  
 There is an error tolerance of 10% to prevent frequent fluctuation of instance quantity, so there is no scaling when Current metrics/Expected metric ranges from 0.9 to 1.1.

AS Policies Metric Time Hybrid

Max. Instances - 4 + Max. number of instances that can be reached during scale-out

Min Instances - 1 +

**AS Time**

Trigger Cycle Every day ▾

Trigger Time in a Day

From	<span style="border: 1px solid #ccc; padding: 2px 5px;">18:00</span> <span style="font-size: 1em;">🕒</span>	Instances	<span style="border: 1px solid #ccc; padding: 2px 5px;">3</span>	<span style="font-size: 1em;">🗑️</span>
From	<span style="border: 1px solid #ccc; padding: 2px 5px;">00:00</span> <span style="font-size: 1em;">🕒</span>	Instances	<span style="border: 1px solid #ccc; padding: 2px 5px;">1</span>	<span style="font-size: 1em;">🗑️</span>

⊕ Add Trigger Time

**Step 6** Click **OK**.

**Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

### 7.6.3 Configuring a Hybrid AS Policy

This section describes how to configure a hybrid AS policy. You can configure metrics and time segments at the same time to control instance scaling.

**NOTE**

CAE instance scaling is calculated by current and expected metrics.

Expected instances = ceil [Current instances \* (Current metrics/Expected metrics)] (ceil is rounded up.)

There is an error tolerance of 10% to prevent frequent fluctuation of instance quantity, so there is no scaling when Current metrics/Expected metric ranges from 0.9 to 1.1.

### Application Scenario

This policy is useful for periodic resource usage, burst traffic, and typical periodic traffic, mainly used in industries such as the Internet, education, and catering.

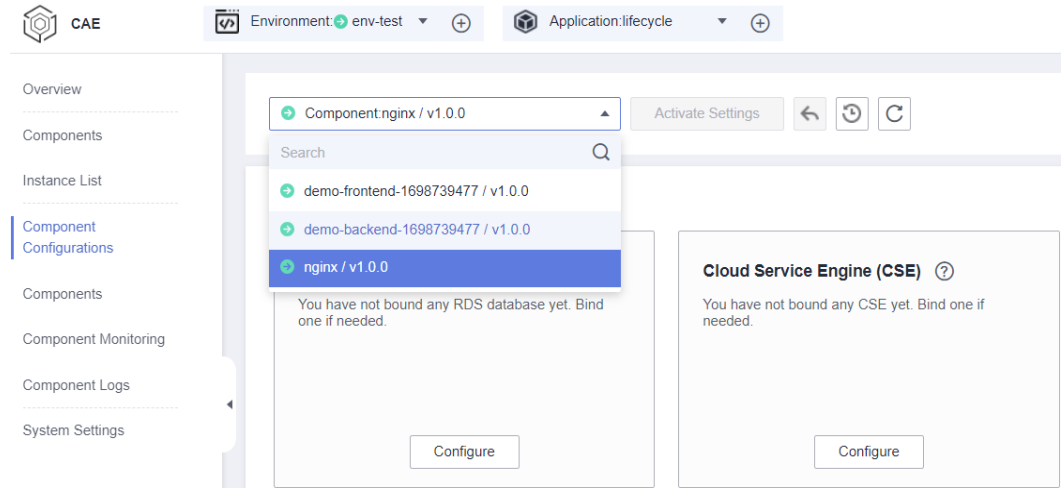
### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-32** Selecting a component



**Step 4** Click **Edit** in the **AS Policies** module.

**Step 5** Select **Hybrid** and configure the policy by referring to [Table 7-14](#).

**Table 7-14** Configuring a hybrid policy

Parameter	Description
Max. Instances	Max. number of instances that can be reached during scale-out. Value range: 1 to 99. <b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b> .
Min Instances	Min number of instances that can be reached during scale-in. Value range: 1 to 99.



Parameter	Description
Metric	<ul style="list-style-type: none"> <li>● CPU usage, a preset metric in the system</li> <li>● Memory usage, a preset metric in the system</li> <li>● Custom metrics. Click <b>Add Expected Value</b> and select a custom metric from the drop-down list to add a custom metric. For details about how to create a custom metric, see <a href="#">Configuring Custom Metrics</a>. You can add multiple custom metrics.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- You must enter a PromQL statement. PromQL is a built-in data query language from Prometheus, and is used to select, aggregate, and perform logical calculation on time series data. For details, see <a href="#">Prometheus</a>.</li> <li>- The query result of the PromQL statement must be a single value of the vector or scalar type.</li> <li>- Upgrade the component created/ upgraded before November 3, 2023 for the custom scaling policy to take effect.</li> </ul>
Trigger Cycle	<p>The policy is expected to be executed at a specified interval. Value: <b>Every day, Every day, or Monthly</b>.</p>
Trigger Time in a Day	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every day</b>. Configure the policy triggered every day.</p> <p>For example, the number of instances remains 3 after 18:00 every day.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>

Parameter	Description
Trigger Time in a Week	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every week</b>. Configure the policy triggered every week.</p> <p>For example, the number of instances remains 4 after 08:00 on every Monday.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Month	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Monthly</b>. Configure the policy triggered every month.</p> <p>For example, the number of instances remains 4 after 06:00 on the fifth day of each month.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>

 **NOTE**

The rules of a hybrid policy are OR related. When either the time or metric policy meets the condition, scaling is triggered.

For example, set the maximum expected CPU usage to 80 and memory usage to 70, set **Trigger Cycle** to **Every day**, and set **From 18:00** and **Instances 3**, and **From 00:00** and **Instances 1**. The system keeps 1 instance from 00:00 to 18:00. However, if the CPU usage of a component is greater than 80% or the memory usage is greater than 70% during this period, the system automatically increases the number of component instances.

**Figure 7-33** Configuring a hybrid policy

**AS Policies**

**i** CAE instance scaling is calculated by current and expected metrics. ×

Expected instances = ceil [Current instances \* (Current metrics/Expected metrics)] (ceil is rounded up.)

There is an error tolerance of 10% to prevent frequent fluctuation of instance quantity, so there is no scaling when Current metrics/Expected metric ranges from 0.9 to 1.1.

AS Policies: Metric Time Hybrid

Max. Instances:  Max. number of instances that can be reached during scale-out

Min Instances:

**AS Metric Settings**

**⚠** Upgrade the component created/upgraded before November 3, 2023 for the custom scaling policy to take effect. ×

Metric	Expected Value	Operation
Resource CPU usage	<input type="text" value="80"/> %	
Resource Memory usage	<input type="text" value="70"/> %	

+ Add Expected Value

**AS Time**

Trigger Cycle: Every day

Trigger Time in a Day:


From <input type="text" value="00:00"/>	<input type="text" value="1"/> Instances	<input type="text"/>	<input type="text"/>
From <input type="text" value="18:00"/>	<input type="text" value="3"/> Instances	<input type="text"/>	<input type="text"/>

+ Add Trigger Time

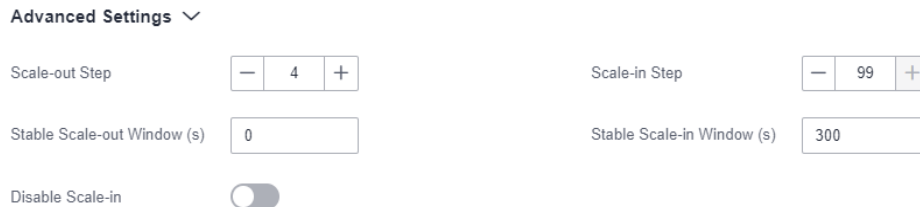
**Step 6** (Optional) Expand **Advanced Settings** and configure advanced settings by referring to [Table 7-15](#).

**Table 7-15** Configuring advanced settings

Parameter	Description
Scale-out Step	Number of pods to be added per minute. Value range: 1 to 99. Default value: <b>4</b> .
Stable Scale-out Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>0</b> .
Scale-in Step	Number of pods to be reduced per minute. Value range: 1 to 99. Default value: <b>99</b> .
Stable Scale-in Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>300</b> .

Parameter	Description
Disable Scale-in	Click  to disable scale-in.

**Figure 7-34** Advanced settings



**Step 7** Click **OK**.

**Step 8** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.6.4 Editing an AS Policy

This section describes how to edit an AS policy.

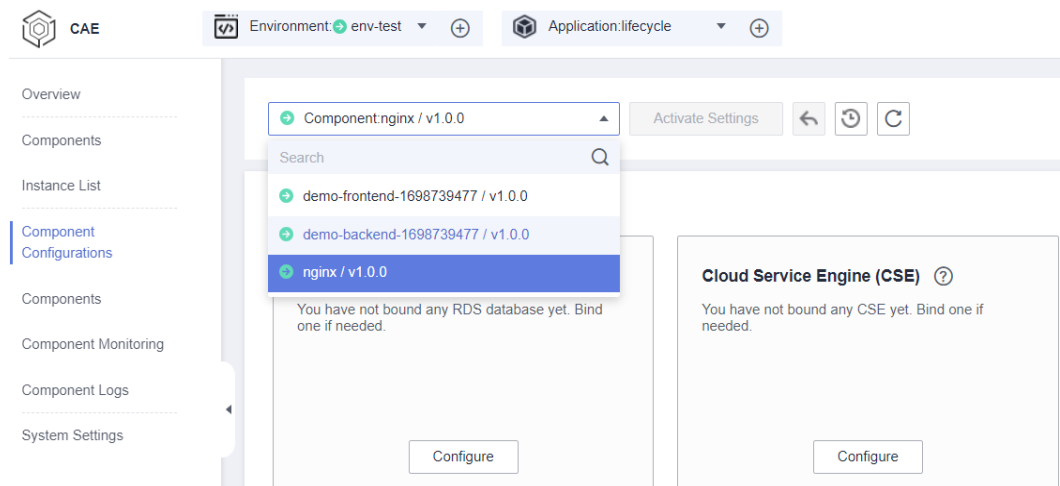
### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-35** Selecting a component



**Step 4** Click **Edit** in the **AS Policies** module.

**Step 5** Update configuration parameters.

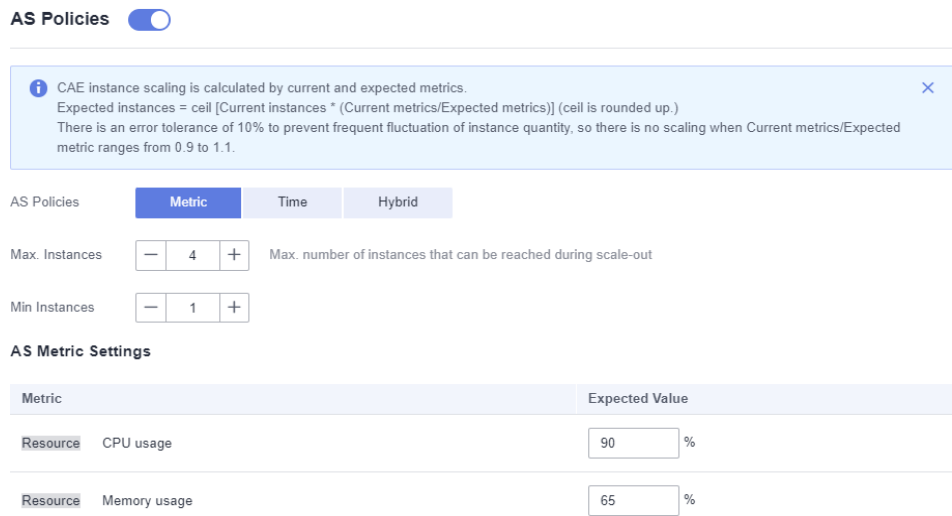
- Configure a metric AS policy
  - a. Select **Metric**.
  - b. Reconfigure the metric AS policy by referring to the following table.

**Table 7-16** Parameters

Parameter	Description
Max. Instances	Max. number of instances that can be reached during scale-out. Value range: 1 to 99. <b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b> .
Min Instances	Min number of instances that can be reached during scale-in. Value range: 1 to 99.

Parameter	Description
Metric	<ul style="list-style-type: none"> <li>▪ CPU usage, a preset metric in the system</li> <li>▪ Memory usage, a preset metric in the system</li> <li>▪ Custom metrics. Click <b>Add Expected Value</b> and select a custom metric from the drop-down list to add a custom metric. For details about how to create a custom metric, see <a href="#">Configuring Custom Metrics</a>.</li> </ul> <p>You can add multiple custom metrics.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>○ You must enter a PromQL statement. PromQL is a built-in data query language from Prometheus, and is used to select, aggregate, and perform logical calculation on time series data. For details, see <a href="#">Prometheus</a>.</li> <li>○ The query result of the PromQL statement must be a single value of the vector or scalar type.</li> <li>○ Upgrade the component created/upgraded before November 3, 2023 for the custom scaling policy to take effect.</li> </ul>

**Figure 7-36** Configure a metric AS policy



- c. (Optional) Expand **Advanced Settings** and configure advanced settings by referring to [Table 7-17](#).

**Table 7-17** Configuring advanced settings

Parameter	Description
Scale-out Step	Number of pods to be added per minute. Value range: 1 to 99. Default value: <b>4</b> .
Stable Scale-out Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>0</b> .
Scale-in Step	Number of pods to be reduced per minute. Value range: 1 to 99. Default value: <b>99</b> .
Stable Scale-in Window (s)	Value range: 1 to 3600, in seconds. Default value: <b>300</b> .
Disable Scale-in	Click <input type="checkbox"/> to disable scale-in.

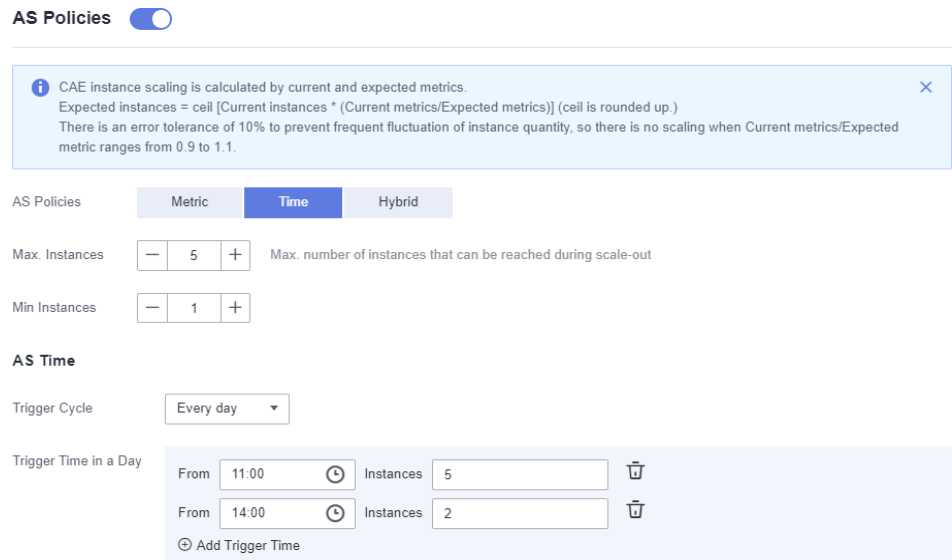
- Configure a time AS policy
  - a. Select **Time**.
  - b. Reconfigure the time AS policy by referring to the following table.

**Table 7-18** Parameters

Parameter	Description
Max. Instances	<p>Max. number of instances that can be reached during scale-out.</p> <p>Value range: 1 to 99.</p> <p><b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b>.</p>
Min Instances	<p>Min number of instances that can be reached during scale-in.</p> <p>Value range: 1 to 99.</p>
Trigger Cycle	<p>The policy is expected to be executed at a specified interval.</p> <p>Value: <b>Every day</b>, <b>Every day</b>, or <b>Monthly</b>.</p>
Trigger Time in a Day	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every day</b>.</p> <p>Configure the policy triggered every day.</p> <p>For example, the number of instances remains 5 after 11:00 every day.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Week	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every week</b>.</p> <p>Configure the policy triggered every week.</p> <p>For example, the number of instances remains 2 after 08:00 on every Monday.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Month	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Monthly</b>.</p> <p>Configure the policy triggered every month.</p> <p>For example, the number of instances remains 3 after 06:00 on the fifth day of each month.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>



**Figure 7-37** Configuring a time policy



- Configure a hybrid AS policy
  - i. Select **Hybrid**.
  - ii. Reconfigure the hybrid AS policy by referring to the following table.

**Table 7-19** Configuring a hybrid policy


Parameter	Description
Max. Instances	Max. number of instances that can be reached during scale-out. Value range: 1 to 99. <b>NOTE</b> <b>Max. Instances</b> must be greater than <b>Min Instances</b> .
Min Instances	Min number of instances that can be reached during scale-in. Value range: 1 to 99.

Parameter	Description
Metric	<ul style="list-style-type: none"> <li>○ CPU usage, a preset metric in the system</li> <li>○ Memory usage, a preset metric in the system</li> <li>○ Custom metrics. Click <b>Add Expected Value</b> and select a custom metric from the drop-down list to add a custom metric. For details about how to create a custom metric, see <a href="#">Configuring Custom Metrics</a>. You can add multiple custom metrics.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>○ You must enter a PromQL statement. PromQL is a built-in data query language from Prometheus, and is used to select, aggregate, and perform logical calculation on time series data. For details, see <a href="#">Prometheus</a>.</li> <li>○ The query result of the PromQL statement must be a single value of the vector or scalar type.</li> <li>○ Upgrade the component created/upgraded before November 3, 2023 for the custom scaling policy to take effect.</li> </ul>
Trigger Cycle	<p>The policy is expected to be executed at a specified interval. Value: <b>Every day</b>, <b>Every day</b>, or <b>Monthly</b>.</p>
Trigger Time in a Day	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every day</b>. Configure the policy triggered every day. For example, the number of instances remains 3 after 18:00 every day. Click <b>Add Trigger Time</b> to add more time policies.</p>

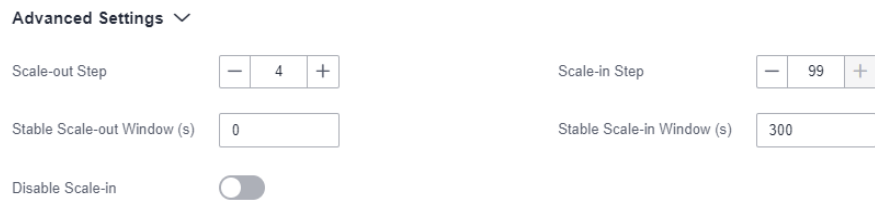
Parameter	Description
Trigger Time in a Week	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Every week</b>.</p> <p>Configure the policy triggered every week.</p> <p>For example, the number of instances remains 4 after 08:00 on every Monday.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>
Trigger Time in a Month	<p>This parameter is mandatory when <b>Trigger Cycle</b> is set to <b>Monthly</b>.</p> <p>Configure the policy triggered every month.</p> <p>For example, the number of instances remains 4 after 06:00 on the fifth day of each month.</p> <p>Click <b>Add Trigger Time</b> to add more time policies.</p>

- iii. (Optional) Expand **Advanced Settings** and configure advanced settings by referring to [Table 7-20](#).

**Table 7-20** Configuring advanced settings

Parameter	Description
Scale-out Step	<p>Number of pods to be added per minute.</p> <p>Value range: 1 to 99. Default value: <b>4</b>.</p>
Stable Scale-out Window (s)	<p>Value range: 1 to 3600, in seconds. Default value: <b>0</b>.</p>
Scale-in Step	<p>Number of pods to be reduced per minute.</p> <p>Value range: 1 to 99. Default value: <b>99</b>.</p>
Stable Scale-in Window (s)	<p>Value range: 1 to 3600, in seconds. Default value: <b>300</b>.</p>
Disable Scale-in	<p>Click  to disable scale-in.</p>

**Figure 7-38** Advanced settings



**Step 6** Click **OK**.

**Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.6.5 Disabling an AS Policy

Disable an AS policy that is no longer needed. After the AS policy is disabled, instances will not be automatically scaled.

 **NOTE**

Disable the AS policy before stopping a component or configuring manual scaling.

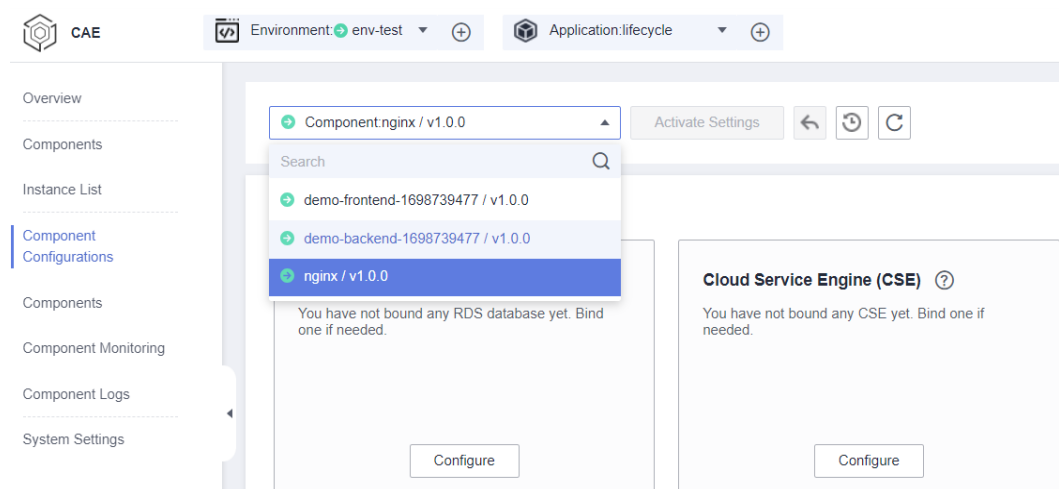
### Procedure

**Step 1** [Log in to CAE](#).


**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-39** Selecting a component



**Step 4** Click **Edit** in the **AS Policies** module.

**Step 5** Click . A message is displayed indicating that the AS policy is disabled.

**Step 6** Click **OK**.

**Step 7** In the displayed dialog box, enter **SWITCHOFF** and click **OK**.

**Step 8** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.7 Configuring Cloud Storage

### 7.7.1 Cloud Storage Description

CAE supports parallel file system and bucket. [Table 7-21](#) describes the features and application scenarios of them.

**Table 7-21** Cloud storage comparison

Dimension	OBS Parallel File System	OBS Bucket
Definition	Parallel File System (PFS) is a high-performance system with access latency in milliseconds. Provided by OBS, PFS supports bandwidth up to the TB/s level and millions of IOPS for processing high-performance computing (HPC) workloads.	A bucket is a container for storing objects in OBS. It provides massive, secure, reliable, and cost-effective data storage.
Data storage logic	Stores files but supports object APIs. That is, you can process files the same way you process objects, implementing the interworking between objects and files.	Stores objects. Files directly stored automatically generate the system metadata, which can also be customized by users.
Features	Shared storage and user-mode file system. High-performance storage services are provided.	Shared storage and user-mode file system. You can configure the object storage class as required.
Application scenario	High-performance computing and media asset archiving, such as video surveillance, online video on demand (VoD), HPC, and big data	Big data analytics, static website hosting, VoD, gene sequencing, intelligent video surveillance, backup and archiving, and enterprise cloud boxes (web disks)

## 7.7.2 Configuring a Parallel File System

Parallel File System (PFS) is a high-performance system with access latency in milliseconds. Provided by OBS, PFS supports bandwidth up to the TB/s level and millions of IOPS for processing high-performance computing (HPC) workloads.

This section uses the parallel file system of the Nginx component as an example to describe how to configure cloud storage.

### NOTICE

- The cloud storage configuration path must be different from the [log collection path](#).
- Only parallel file systems with Standard storage type are supported.

### Prerequisites

You have uploaded all files in the application path to be mounted to the OBS parallel file system.

For details, see [Uploading an Object](#).

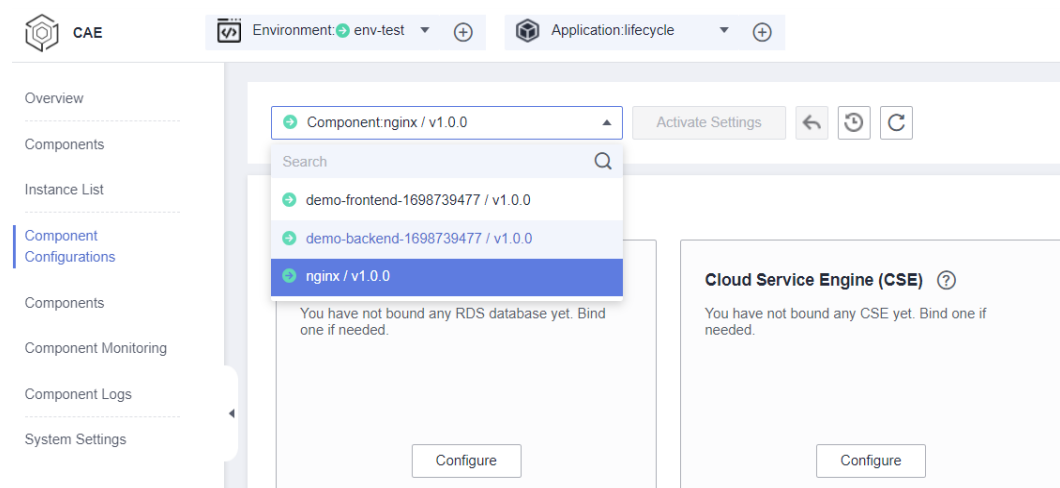
### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-40** Selecting a component



**Step 4** Click **Edit** in the **Cloud Storage** module.

**Step 5** Click **Set Parallel File System**.

**Step 6** Select an authorized parallel file system from the drop-down list.

To add an authorization, click **Authorize Parallel File System**. For details, see [Authorizing a Parallel File System](#).

**Step 7** Configure the path to which the container is mounted and the permissions on the path. For details, see [Table 7-22](#).

**Table 7-22** Parameters

Parameter	Description
File Mask (umask)	<p>File mask (umask) of the file to mount. Enter four digits (0 to 7). Default value: <b>0027</b>.</p> <p><b>NOTE</b> A user file-creation mask (umask) is used to set permissions for newly created files. You can set a umask in the CAE cloud storage configuration to set permissions for the directories and files to mount. For example, 0027 indicates that the permission on the directory is 750 and that on the file is 640.</p>
Mount Path	<p>Component path to which the data storage is mounted. In this example, use the default path <b>/usr/share/nginx/html</b> of <b>nginx</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Do not mount the data storage to a system directory, such as <b>/</b> or <b>/var/run</b>. Otherwise, an exception occurs.</li> <li>The mount path of the cloud storage must be unique.</li> </ul>
Sub-path	<p>Sub-path in the cloud storage referenced by data. For example, if the <b>index.html</b> file is stored in the <b>test</b> folder of the OBS parallel file system <b>test-nginx</b>, enter <b>test/index.html</b> to reference the file.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>A sub-path is used to mount a local volume so that the same data volume is used in a single pod.</li> <li>If this parameter is left blank, the root path is used.</li> <li>If a parallel file system is mounted to a sub-path that does not exist, an exception occurs. You need to create the corresponding file or folder in the mounted bucket first.</li> </ul>
Required Permissions	<p>Permissions on the mount path and files in the mount path. The value can be <b>Read/Write</b> or <b>Read only</b>. In this example, select <b>Read/Write</b>.</p>

**Figure 7-41** Configuring a parallel file system

**Set Parallel File System**

---

Parallel File System  [C Authorize Parallel File System](#)  
Only parallel file systems with Standard storage type are supported.

File Mask (umask)   
Set default permissions for new files and directories.

Mount Path ?	Sub-path ?	Required Permissions	Operation
<input type="text" value="/usr/share/nginx/html"/>	<input type="text" value="Please enter the subPath, for example, tmp"/>	<input type="text" value="Read/Write"/>	<a href="#">Delete</a>

[+ Add Mount Path](#)

**Step 8** (Optional) Click **Add Mount Path** to configure more mount paths.

**Step 9** Click **OK**.

You can view the configured parallel file systems on the **Cloud Storage** page.

**Step 10** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**NOTE**

You can update the Nginx access page in real time by updating static files in the parallel file system.

----End

### 7.7.3 Configuring a Bucket

A bucket is a container for storing objects in OBS. It provides massive, secure, reliable, and cost-effective data storage.

**NOTICE**

- The cloud storage configuration path must be different from the **log collection path**.
- Currently, only Standard buckets are supported.

#### Prerequisites

You have uploaded all files in the application path to be mounted to the OBS bucket.

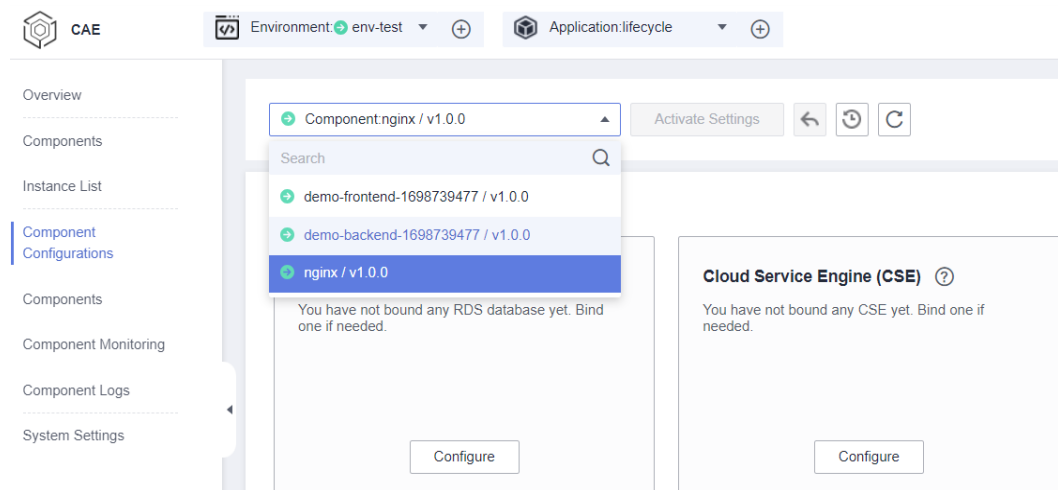
For details, see **Uploading an Object**.



## Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-42** Selecting a component



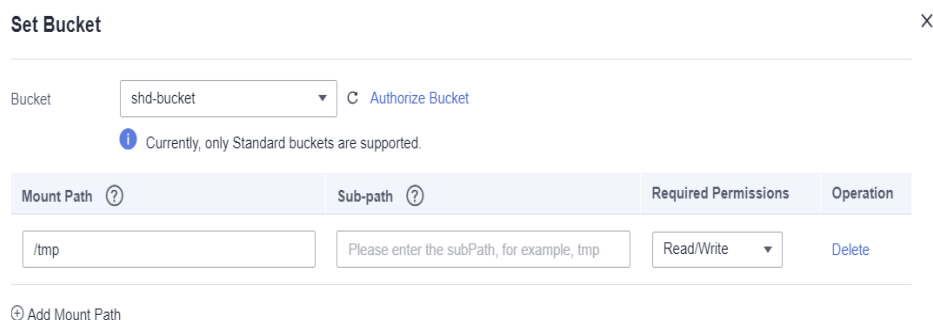
- Step 4** Click **Edit** in the **Cloud Storage** module.
- Step 5** Click **Set Bucket**.
- Step 6** Select an authorized bucket from the drop-down list.  
To add an authorization, click **Authorize Bucket**. For details, see [Authorizing a Bucket](#).
- Step 7** Configure the path to which the container is mounted and the permissions on the path. For details, see [Table 7-23](#).

**Table 7-23** Parameters

Parameter	Description
File Mask (umask)	<p>File mask (umask) of the file to mount. Enter four digits (0 to 7). Default value: <b>0027</b>.</p> <p><b>NOTE</b> A user file-creation mask (umask) is used to set permissions for newly created files. You can set a umask in the CAE cloud storage configuration to set permissions for the directories and files to mount. For example, 0027 indicates that the permission on the directory is 750 and that on the file is 640.</p>

Parameter	Description
Mount Path	<p>Component path to which the data storage is mounted.</p> <p>For example, if the <b>index.html</b> file is stored in the OBS bucket <b>test-nginx</b>, enter <b>index.html</b> to reference the file.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Do not mount the data storage to a system directory, such as <b>/</b> or <b>/var/run</b>. Otherwise, an exception occurs.</li> <li>The mount path of the cloud storage must be unique.</li> </ul>
Sub-path	<p>Sub-path in the cloud storage referenced by data.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>A sub-path is used to mount a local volume so that the same data volume is used in a single pod.</li> <li>If this parameter is left blank, the root path is used.</li> </ul>
Required Permissions	<p>Permissions on the mount path and files in the mount path. The value can be <b>Read/Write</b> or <b>Read only</b>.</p>

**Figure 7-43** Configuring a bucket



**Step 8** (Optional) Click **Add Mount Path** to configure more mount paths.

**Step 9** Click **OK**.

You can view the configured buckets on the **Cloud Storage** page.

**Step 10** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## 7.7.4 Editing a Cloud Storage Mounting Configuration

After cloud storage mounting is configured, you can perform the following steps to modify the mounting path, read and write permissions, and file mask.

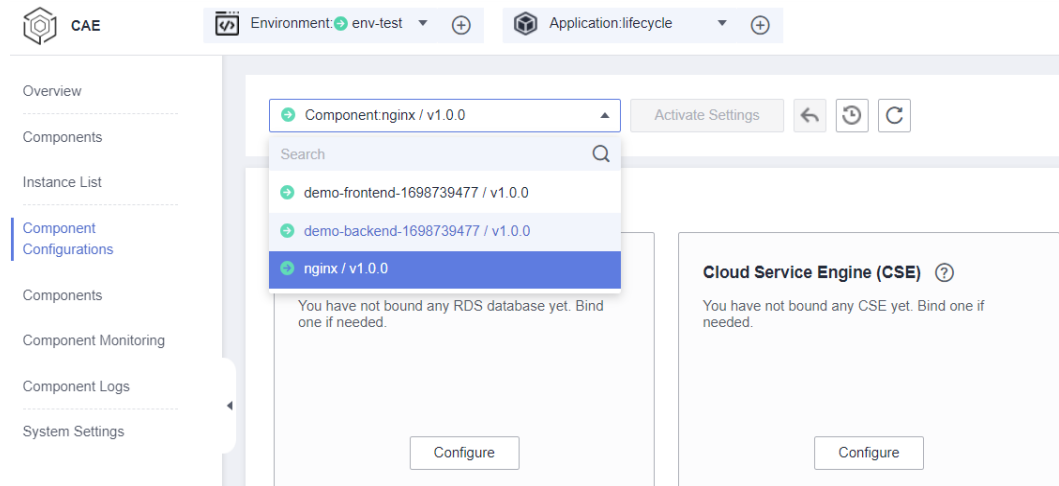
## Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-44** Selecting a component



**Step 4** Click **Edit** in the **Cloud Storage** module.

**Step 5** Select the target configuration and click **Modify** in the **Operation** column.

**Figure 7-45** Modifying a cloud storage configuration

### Cloud Storage

Name	Type	Storage Capa...	Mount Path	Sub-path	Created	Operation
cae-demo	Parallel File Sy...	0.00MB	Read/Write /...	--	2023/12/19 15:16:54 G...	<a href="#">Modify</a> <a href="#">Delete</a>

**Step 6** Modify parameters by referring to [Table 7-24](#) and click **OK**.

**Table 7-24** Parameters

Parameter	Description
File Mask (umask)	File mask (umask) of the file to mount. Enter four digits (0 to 7). Default value: <b>0027</b> . <b>NOTE</b> A user file-creation mask (umask) is used to set permissions for newly created files. You can set a umask in the CAE cloud storage configuration to set permissions for the directories and files to mount. For example, 0027 indicates that the permission on the directory is 750 and that on the file is 640.
Mount Path	Component path to which the data storage is mounted. <b>NOTE</b> <ul style="list-style-type: none"> <li>Do not mount the data storage to a system directory, such as / or <b>/var/run</b>. Otherwise, an exception occurs.</li> <li>The mount path of the cloud storage must be unique.</li> </ul>
Sub-path	Component sub-path to which the data storage is mounted. <b>NOTE</b> <ul style="list-style-type: none"> <li>A sub-path is used to mount a local volume so that the same data volume is used in a single pod.</li> <li>If this parameter is left blank, the root path is used.</li> </ul>
Required Permissions	Permissions on the mount path and files in the mount path. The value can be <b>Read/Write</b> or <b>Read only</b> .

**Step 7** Click **OK**.

**Step 8** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.7.5 Deleting a Cloud Storage Mounting Configuration

You can delete a cloud storage mounting configuration that is no longer needed.

After a cloud storage mounting configuration is deleted, data stored in the file system will not be deleted. To mount the cloud storage again, configure the cloud storage mounting path.

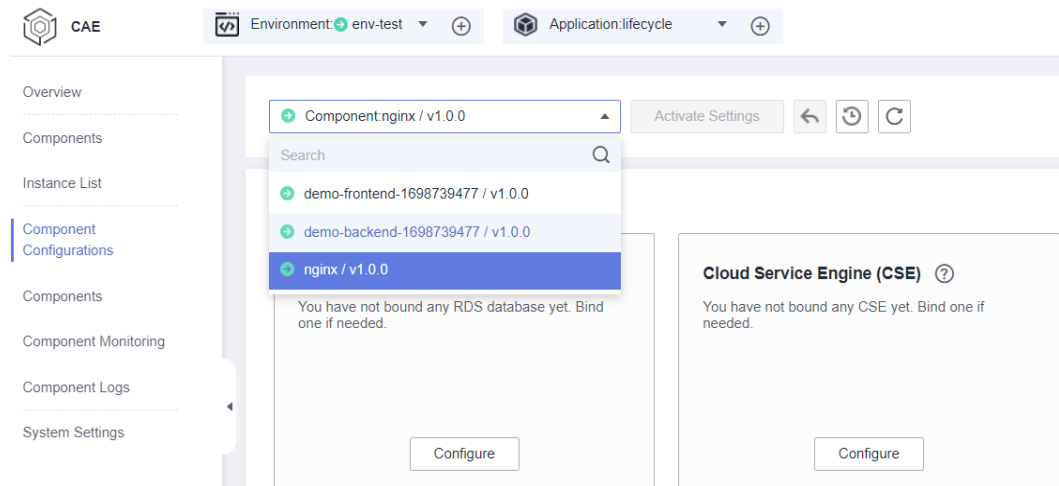
### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-46** Selecting a component

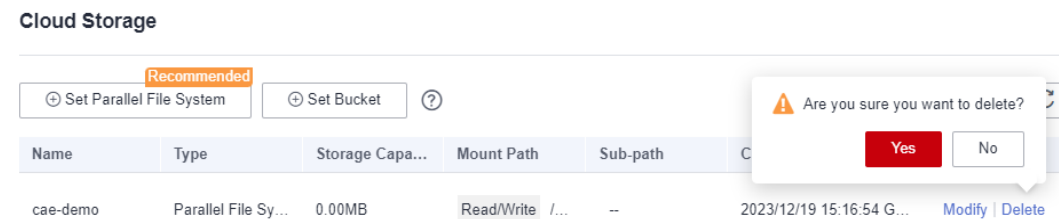


**Step 4** Click **Edit** in the **Cloud Storage** module.

**Step 5** Select the target configuration and click **Delete** in the **Operation** column.

**Step 6** In the displayed dialog box, click **Yes**.

**Figure 7-47** Deleting a cloud storage configuration



**Step 7** Click **OK**.

**Step 8** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End

## 7.8 Configuring Health Check

Health check helps you check whether application instances and services are running.

This section describes health check by checking whether an application is interrupted during upgrade.

### Precautions

- When only the liveliness probe is used, if the network fluctuates or the program starts slowly, the instance will keep restarting and remains in the **Not ready** state.

The following solutions are available:

- Use startup probe together.
- Increase **Failure Threshold** to increase the fault tolerance rate and increase **Latency** to ensure that the program accepts the liveness probe detection after startup.
- If status code 200 is returned, the check is successful.
- If a status code other than 200 is returned and the number of consecutive failures reaches **Failure Threshold**, the check fails.

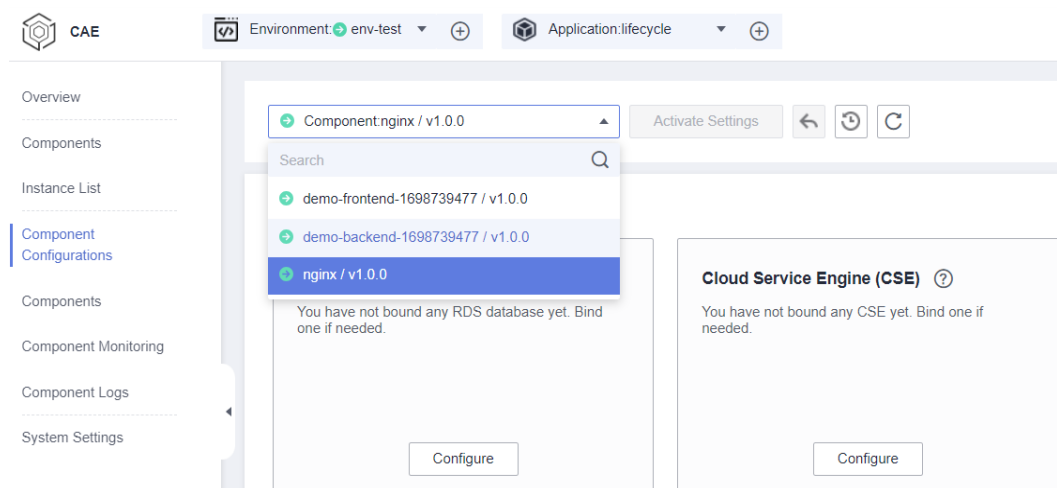
## Procedure

**Step 1** Log in to CAE.

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-48** Selecting a component



**Step 4** Click **Edit** in the **Health Check** module.

**Step 5** You can select liveness probe, readiness probe, or startup probe. Different probes can be enabled at the same time.

- Liveness probe checks the startup health of application instances. The application instances are being started. Click  next to **Liveness Probe** to configure the check method.
- Readiness probe checks the startup health of application instances. The application instances are available to provide services. Click  next to **Readiness Probe** to configure the check method. In this example, the readiness probe must be enabled.
- Startup probe checks the running health of application instances. If application instances are unhealthy, CAE restarts them. Click  next to **Startup Probe** to configure the check method.

**Figure 7-49** Readiness probe

**Health Check**

Liveness Probe

**Readiness Probe**

Startup Probe

**Readiness Probe**

Check Method: HTTP TCP Command ?

Port:

Check Interval:

Latency(s):

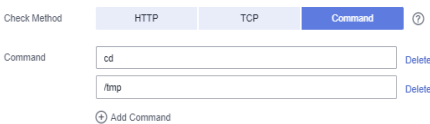
Timeout Interval(s):

Success Threshold:

Failure Threshold:

**Step 6** Select a check method and set parameters. For details, see [Table 7-25](#) and [Table 7-26](#).

**Table 7-25** Check method parameters

Check Method	Parameter	Description
HTTP	Port	Port used to establish an HTTP GET connection.
	Path	Path used to establish an HTTP GET connection.
	Protocol	Select <b>HTTP</b> or <b>HTTPS</b> .
	Header	HTTP header in the request.
TCP	Port	Port for TCP connections. In this example, select <b>TCP</b> .
Command	Command	<p>Add a command. Click <b>Add Command</b> to add more commands.</p> <p><b>NOTE</b> No space is allowed after the command line.</p> 

**Table 7-26** Common parameters of the three check methods

Parameter	Description
Check Interval	Detection interval, in seconds. Default value: <b>10</b> . Minimum value: <b>1</b> . In this example, use the default value.
Latency	Maximum latency, in seconds. Default value: <b>0</b> . Minimum value: <b>0</b> . In this example, use the default value. <b>NOTE</b> If you configure health check before starting the container, set <b>Latency</b> to 3 minutes.
Timeout Interval	Detection timeout interval, in seconds. Default value: <b>1</b> . Minimum value: <b>1</b> . In this example, use the default value.
Success Threshold	Health check is passed after a specified number of consecutive successful detections. Default value: <b>1</b> . Minimum value: <b>1</b> . For liveness and startup probes, set it to <b>1</b> . In this example, use the default value.
Failure Threshold	Health check fails after a specified number of consecutive failed detections. Default value: <b>3</b> . Minimum value: <b>1</b> . In this example, use the default value.

**Step 7** Click **OK**.

**Step 8** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**Step 9** After **upgrading the component**, choose **Component Events**. If the **Component instance healthy** event is **Normal**, the component is successfully upgraded.



**Figure 7-50** Component health check

Event	Severity	Type	Occurrences	Description
Component instance healthy	Normal	Instances	1	container docker://f9dbf4793908202c3...
Component instance unhea...	Abnormal	Instances	1	Readiness probe failed: dial tcp 10.0.1....
Volume mounted	Normal	Instances	2	Successfully mounted volumes for pod ...
Component startup	Normal	Instances	1	Started container demo-frontend-1697...
Component instance created.	Normal	Instances	1	Created container demo-frontend-1697...

----End

## References

- [Cooperation Between Startup and Liveliness Probes](#)
- [Using Readiness Probe to Ensure Normal Traffic During Upgrade](#)

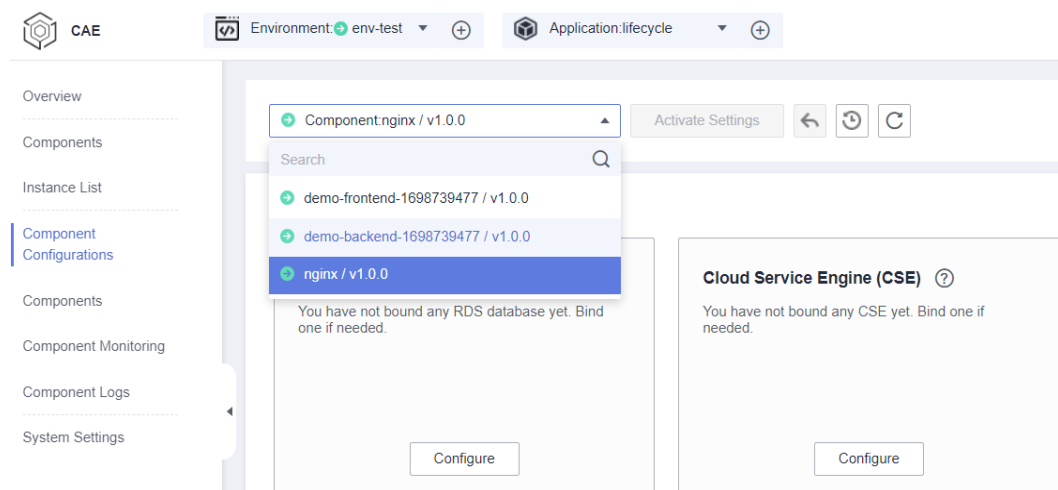
## 7.9 Configuring Lifecycle

CAE provides callback functions for the lifecycle management of containerized applications. For example, if you want a container to perform a certain operation before stopping, you can register a hook function.

### Procedure

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-51** Selecting a component



**Step 4** Click **Edit** in the **Lifecycle Management** module.

**Step 5** Configure **PostStart** or **PreStop**. They can be enabled at the same time.

- **PostStart**: triggered after a container is started. For details, see [Table 7-27](#).
- **PreStop**: triggered before a container is stopped. This ensures that necessary tasks can be executed in advance of upgrades or instance deletions. For details, see [Table 7-28](#).

 **NOTE**

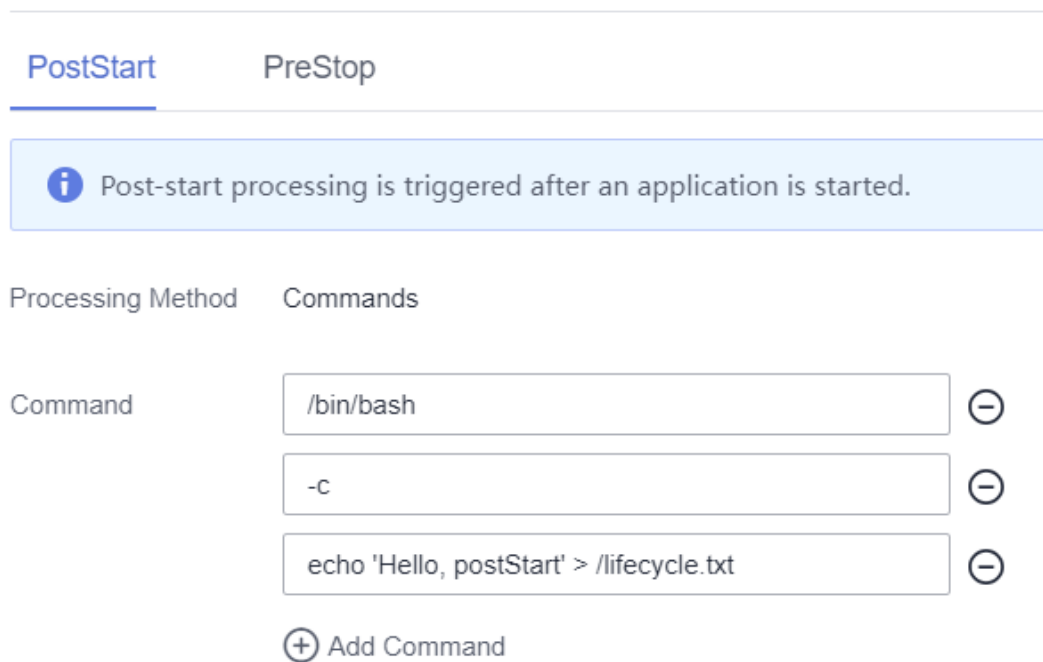
If a while infinite loop is configured for **PostStart** and health check is also configured, the container health check may fail. As a result, component deployment or upgrade fails.

**Table 7-27** PostStart parameters

Parameter	Description
Command	<p>Command to be executed in the container. The command format is <b>Command</b> <i>Args[1]</i> <i>Args[2]</i>...</p> <p><b>Command</b> is a system command or a user-defined executable program. If no path is specified, an executable program in the default path will be selected. If multiple commands need to be executed, write the commands into a script for execution.</p> <p><b>Commands that are executed in the background or asynchronously are not supported.</b></p> <p>For example, to write files using post-start processing, run the following commands:</p> <pre data-bbox="715 1171 1433 1261">/bin/bash -c echo 'Hello, postStart' &gt; /lifecycle.txt</pre>

**Figure 7-52** Configuring PostStart commands

### Lifecycle Management



**Table 7-28** PreStop parameters

Parameter	Description
Command	<p>Command to be executed in the container. The command format is <b>Command</b> <i>Args[1]</i> <i>Args[2]</i>.... <b>Command</b> is a system command or a user-defined executable program. If no path is specified, an executable program in the default path will be selected. If multiple commands need to be executed, write the commands into a script for execution.</p> <p>For example, to gracefully stop Nginx using pre-stop processing, run the following commands:</p> <pre>/bin/bash -c nginx -s quit;while killall -0 nginx;do sleep 1;done</pre>

**Figure 7-53** Configuring PreStop commands

## Lifecycle Management

PostStart
PreStop

**i** The pre-stop hook is called immediately before an application is stopped and exits (Completed).

Processing Method	Commands
Command	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="/bin/bash"/> <span style="float: right;">⊖</span>
	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="-c"/> <span style="float: right;">⊖</span>
	<input style="width: 90%; border: 1px solid #ccc;" type="text" value="nginx -s quit;while killall -0 nginx;do sleep 1;done"/> <span style="float: right;">⊖</span>
	<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">+</span> Add Command

**Step 6** Click **OK**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

----End

## References

- [Writing Files Using Post-start Processing](#)
- [Gracefully Stopping Nginx Using Pre-stop Processing](#)

## 7.10 Configuring Log Collection

CAE provides log collection. Currently, logs can be collected only to LTS. You can configure the log collection path. In advanced settings, you can configure the log format (single-line (default) or multi-line).

This section uses Kafka as an example to describe how to customize log paths.

**NOTICE**

- If log files are mounted to system directories such as / and **/var/run**, components may not work. An empty directory is recommended. If the directory is not empty, ensure that the directory does not contain any file that affects component startup. Otherwise, the files will be replaced, causing component startup exceptions. As a result, the component fails to be created.
- The log path must contain the log file name, for example, **/var/log/test/error.log**. To use a wildcard, you must also specify the extension, for example, **/var/log/test/\*.log**, not **/var/log/test/\*** or **/var/log/test/\*.\***.
- The log files must be text files.
- By default, standard logs are collected for all components and are stored in the **stdout** file.
- The log path must be different from the **cloud storage configuration path**.
- An application in CAE maps to a log group in LTS. Creating a CAE application creates a log group.

## Adding Log Collection

 **NOTE**

You can configure up to 20 log collection paths.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Log Collection** module.

**Step 5** Click **Add Log Path**.

**Step 6** Enter the path of the logs to be collected in **Log Collection Path**. For example: **/var/log/springboot.log**

**Figure 7-54** Configuring a log path

Collection Path ?

Collection Path

Log Collection Path	Operation
<input type="text" value="/var/log/springboot.log"/>	<a href="#">Save</a>   <a href="#">Cancel</a>

**Step 7** Click **Save**.

**Step 8** Configure advanced settings

By default, the system collects and displays the logs printed by the program by line. If a complete log occupies multiple lines and you want to collect and display the entire log, you can set **Log Format** to enable multi-line logs.

- **Single-line:** The system collects logs by line.
- **Multi-line:** Multiple lines are merged into one line. The system collects logs by configured matching rules. The log lines that do not meet the matching rules will be merged with the lines that last met the matching rules.

- If you select **Log time**, the time matching mode is used. If you select **Regular expression**, the regular expression matching mode is used.

**Time Wildcard:** Enter the time wildcard when **Log Segmentation** is set to **Log time**.

For example, if the time format of each log is YYYY-MM-DD hh:mm:ss, set the time wildcard to YYYY-MM-DD hh:mm:ss.

Example time wildcard:

```
YY - year (19)
YYYY - year (2019)
M - month (1)
MM - month (01)
D - day (1)
DD - day (01)
hh - hours (23)
mm - minutes (59)
ss - seconds (59)
SSS - millisecond (999)
hpm - hours (03PM)
h:mmpm - hours:minutes (03:04PM)
h:mm:sspm - hours:minutes:seconds (03:04:05PM)
hh:mm:ss ZZZZ (16:05:06 +0100)
hh:mm:ss ZZZ (16:05:06 CET)
hh:mm:ss ZZ (16:05:06 +01:00)
```

- **Regular expression:** If **Log Segmentation** is set to **Regular expression**, enter the regular expression based on the format of the beginning of each log.

Example regular expression:

Example 1:

```
19:41:33.217 [http-nio-8000-exec-1] ERROR o.a.c.c.c.[.[localhost].[/].[dispatcherServlet] -
Servlet.service() for servlet [dispatcherServlet] in context with path [] threw exception [Request
processing failed; nested exception is java.lang.NullPointerException: Cannot invoke
"com.example.springboothello.controller.HelloController.write()" because "helloController" is
null] with root cause
java.lang.NullPointerException: Cannot invoke
"com.example.springboothello.controller.HelloController.write()" because "helloController" is null
at
com.example.springboothello.controller.HelloController.nullPointerException(HelloController.java:23
4)
    at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at java.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:77)
    at java.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:4
3)
    at java.base/java.lang.reflect.Method.invoke(Method.java:568)
```

Regular expression for merging the preceding logs into one line:  $\wedge \{d\}:\{d\}:\{d\}$ .

All lines that do not start with time are merged to the previous line.

Example 2:

```
Exception in thread "main" java.lang.IllegalStateException: A book has a null property
    at com.example.myproject.Author.getBookIds(Author.java:38)
    at com.example.myproject.Bootstrap.main(Bootstrap.java:14)
Caused by: java.lang.NullPointerException
    at com.example.myproject.Book.getId(Book.java:22)
```

```
at com.example.myproject.Author.getBookIds(Author.java:35)
... 1 more
```

Regular expression for merging the preceding logs into one line:  
**^Exception.**

All lines that do not start with **Exception** are merged to the previous line. The page provides regular expression verification. You can copy the logs to **Log Example**, enter a regular expression, and click **Verify** to check whether the regular expression matches.

**Step 9** Click **OK**.

**Step 10** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

After the configurations take effect, you can [view component logs in a specified path](#) on the **Component Logs** page

----End

## Modifying a Log Path

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Log Collection** module.

**Step 5** Select the target path and click **Edit** in the **Operation** column.

**Step 6** Reconfigure the log collection path, for example, `/var/log/CAE/logs/*.out`.

**Figure 7-55** Modifying a log path



**Step 7** (Optional) Reconfigure the log collection format as required.

**Step 8** Click **Save** and **OK**.

**Step 9** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

**Step 10** View the logs in the new path.

----End

## Deleting a Log Path

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.
- Step 4** Click **Edit** in the **Log Collection** module.
- Step 5** Select the target path and click **Delete** in the **Operation** column.
- Step 6** In the displayed dialog box, click **Yes**. After deleting the path, click **OK**.

**Figure 7-56** Deleting a log path



- Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

### NOTE

Deleted path files no longer collect logs. But you can still view the historical logs of the corresponding log file.

----End

## 7.11 Configuring Performance Management

Performance management helps you quickly locate problems and identify performance bottlenecks to improve your experience. [Enabling performance management](#) will start the Application Performance Management (APM) service and install probes on the nodes, which consumes a small amount of resources. Java probes use the bytecode enhancement technology to trace Java application calls and generate topology and call chain data.

CAE allows you to configure performance management during component deployment.

### Prerequisites

You have [configured the monitoring system](#).

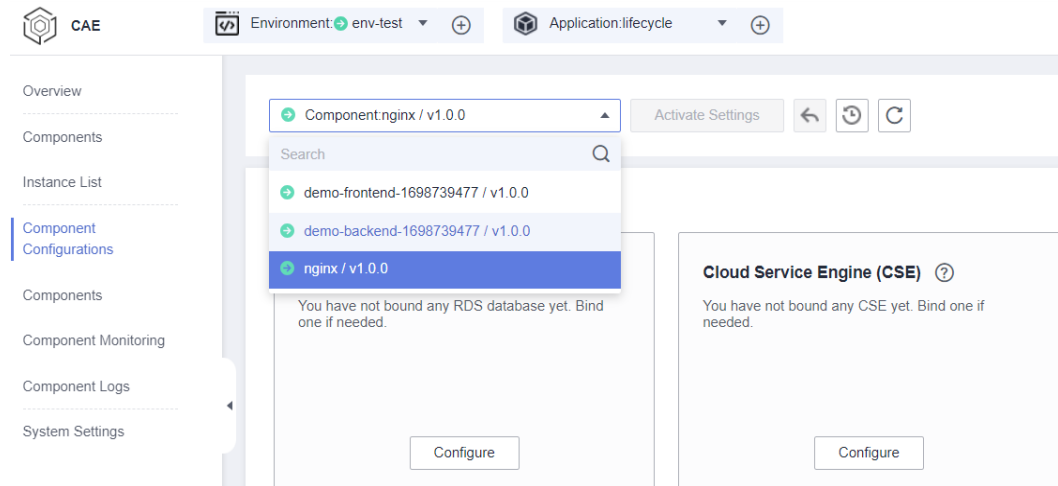
### Enabling Performance Management

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.



**Step 3** Select the target component from the drop-down list in the upper part of the page.

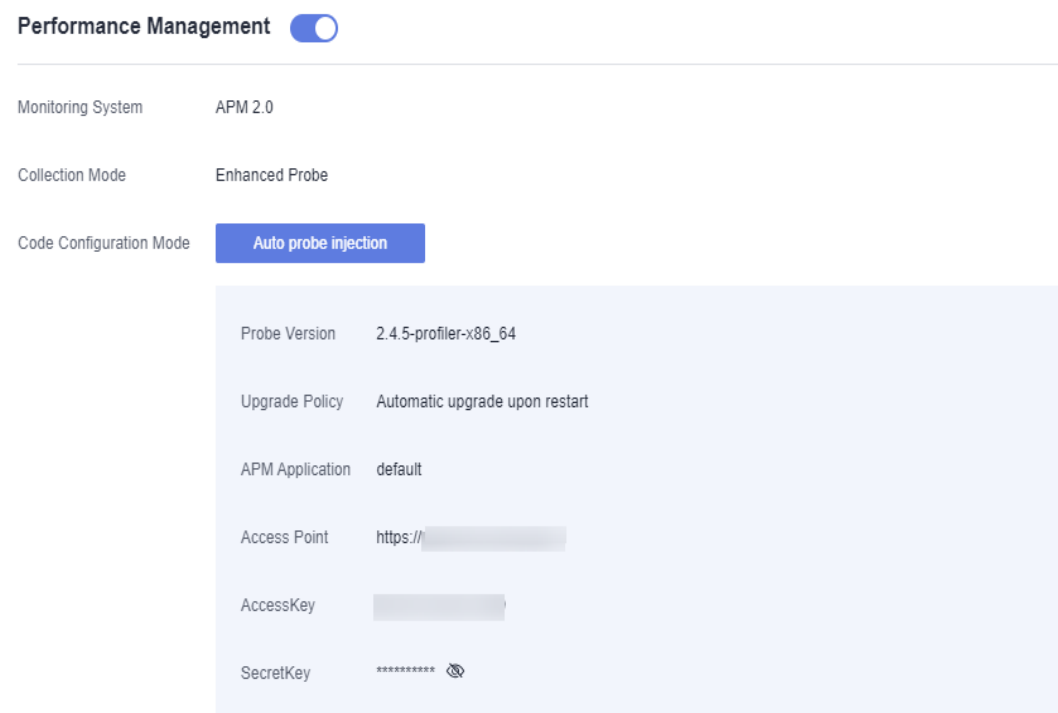
**Figure 7-57** Selecting a component



**Step 4** Click **Edit** in the **Performance Management** module.

**Step 5** Click  to enable performance management.

**Figure 7-58** Configuring performance management



**Step 6** Click **OK**.

**Step 7** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

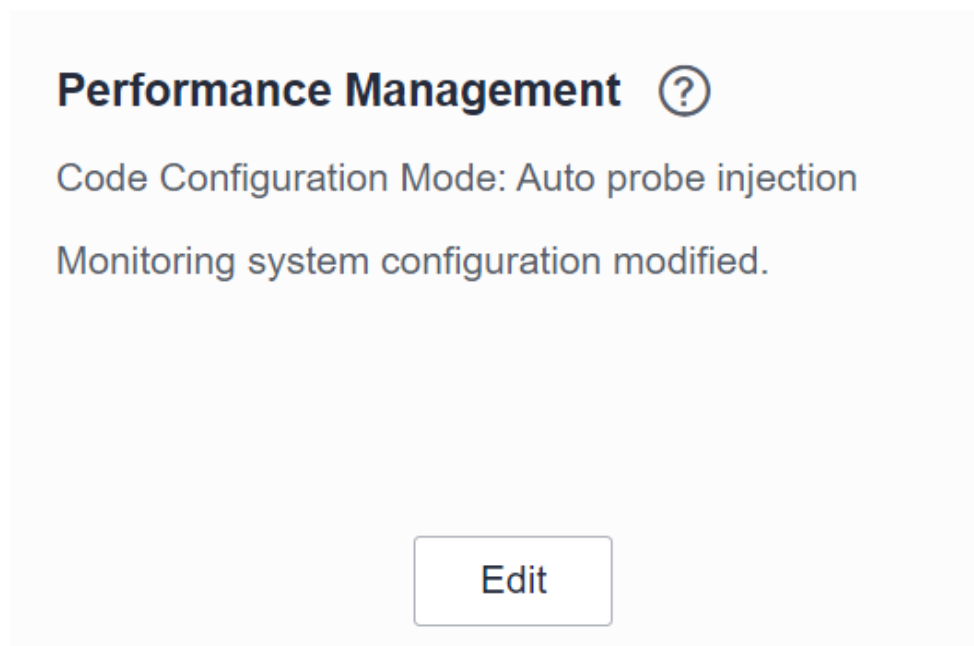
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**Step 8** After performance management is enabled, the APM agent periodically collects some performance metric data. You can log in to the APM console to view [Application Metric Monitoring, Tracing](#), and [Application Topology](#). For details, see [Application Performance Management 2.0 User Guide](#).

 **NOTE**


After the component performance management configuration takes effect, if you **modify the monitoring system configuration**, reconfigure performance management and make the configuration take effect.

**Figure 7-59** Viewing performance management status



----End

## Disabling Performance Management

- Step 1** [Log in to CAE](#).
- Step 2** Choose **Component Configurations**.
- Step 3** Select the target component from the drop-down list in the upper part of the page.
- Step 4** Click **Edit** in the **Performance Management** module.
- Step 5** Click  to disable performance management. Click **OK**.
- Step 6** In the displayed dialog box, enter **SWITCHOFF** and click **OK**.
- Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

**Figure 7-60** Confirming information**Set Changes**

 Ensure that your configuration has been changed as follows:

Change Item	Before	After
Performance Management	Code Configuration Mode: Auto probe injection	--

----End

## 7.12 Configuring Custom Metrics

The [Prometheus](#) component is deployed on CAE internal nodes. Data is collected every 15 seconds. You can use this method to report custom component monitoring metrics.

### Precautions

- Currently, only the [four types](#) supported by Prometheus can be obtained.
- Before configuring custom monitoring for application components, you need to understand [Prometheus](#) and provide the GET API for obtaining custom metric data in your application components so that CAE can obtain the data through this API. Prometheus provides clients in various languages, including Go, Java, Python, Ruby, and Net. For details about the clients, see [Client Libraries](#). For details about how to develop exporter, see [Writing Exporters](#). The Prometheus community provides various third-party exporters that can be directly used. For details, see [Exporters and Integrations](#).

### Configuring Custom Metrics

 NOTE

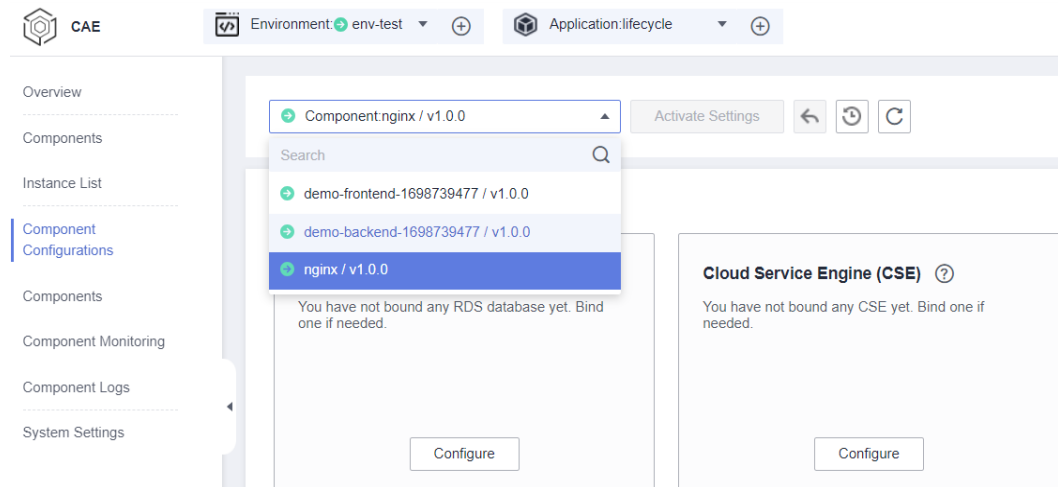
Custom metrics are charged separately. For details, see [Pricing Details](#).

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Figure 7-61** Selecting a component



**Step 4** Click **Edit** in the **Custom Metric** module.

**Step 5** Click  to enable custom metrics. Configure the custom metric by referring to [Table 7-29](#).

**Table 7-29** Custom metric parameters

Parameter	Description	Mandatory
Collection Path	Path exposed by the component using the GET method for CAE to obtain custom metric data. For example, <b>/actuator/prometheus</b> .	Yes
Collection Port	Port exposed by the component using the GET method for CAE to obtain custom metric data. Value range: 1 to 65535. For example: <b>9090</b> .	Yes
Metric	Name of the custom metric exposed by the component using the GET method. For easy understanding, ensure that the name can reflect the actual meaning. For details, see <a href="#">Metric and Label Naming</a> . For example, to define the number of clicks of a button, name it <b>click_operated_total</b> . If the metric exposed by the component is inconsistent with the entered metric name, the metric does not take effect. The metric name contains 5 to 100 characters, including only letters, digits, and underscores (_).	Yes

**Step 6** (Optional) Click **Add Monitoring Metric** to add more custom metrics.

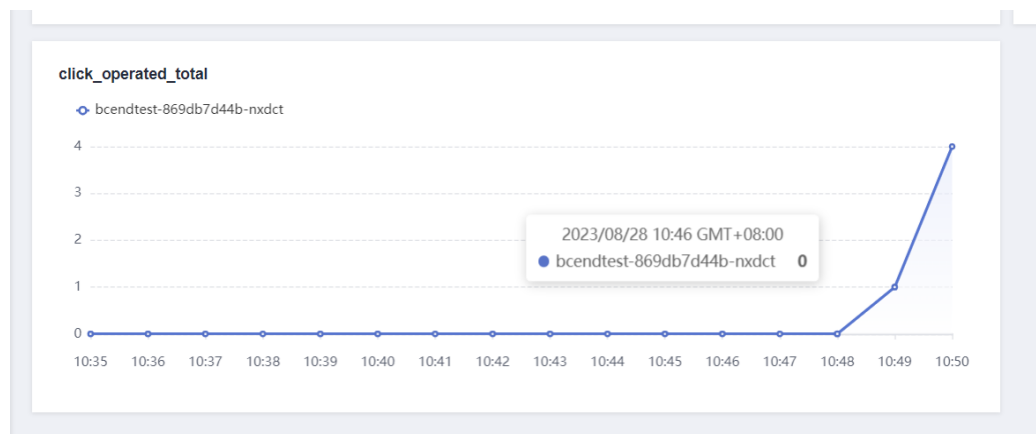
**Step 7** Click **OK**.

**Step 8** Make the configurations take effect.

- If the component has been deployed, click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.
- If the component has not been deployed, click **Set and Deploy Component** in the upper part of the page. In the dialog box displayed on the right, click **OK**. After the deployment is complete, the configurations take effect.

**Step 9** After the configuration and deployment are complete, you can [view monitoring metrics](#) on the **Component Monitoring** page.

**Figure 7-62** Viewing custom metrics



----End

## Editing Custom Metrics


**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Custom Metric** module.

**Step 5** Edit or delete a monitoring metric.

- Reconfigure the parameters by referring to [Table 7-29](#).
- Click  next to a metric to delete it.

**Step 6** Click **OK**.

**Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

----End


## Disabling Custom Metrics

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Configurations**.

**Step 3** Select the target component from the drop-down list in the upper part of the page.

**Step 4** Click **Edit** in the **Custom Metric** module.

**Step 5** Click  to disable custom metrics. Click **OK**.

**Step 6** In the displayed dialog box, enter **SWITCHOFF** and click **OK**.

**Step 7** Click **Activate Settings** in the upper part of the page. In the dialog box displayed on the right, confirm the configurations and click **OK** for the configurations to take effect.

**Step 8** After the configurations take effect, the custom metric data of the corresponding instance is not displayed on the **Component Monitoring** page.

----End

# 8 Component O&M

## 8.1 Viewing Component Events

Component events are generated when you use components, including component deployment and scaling events. Visualized component events help you view component activities. If a fault occurs, you can view component events to locate the fault.

### Prerequisites

1. You have created an application. For details, see [Creating an Application](#).
2. You have created a component. For details, see [Creating a Component](#).

### Procedure

**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Events**.

**Step 3** By default, the **Component Events** page displays data generated within one hour. For details, see [Table 8-1](#).

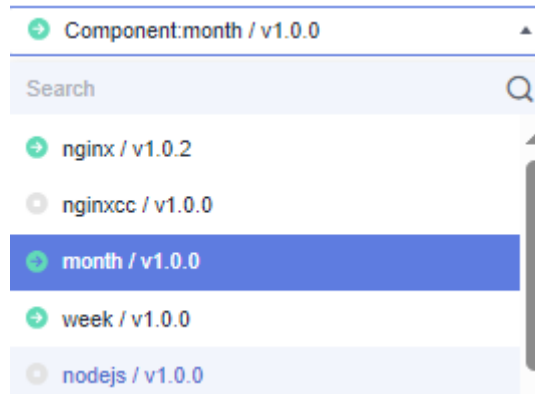
**Table 8-1** Component event information

Parameter	Description
Event	Name of an event.
Severity	Severity of an event. The value can be <b>Normal</b> or <b>Abnormal</b> .
Occurrences	Number of times an event occurred.
Description	Event details.
First Occurred	Time when an event occurred for the first time.
Last Occurred	Time when an event occurred for the last time.

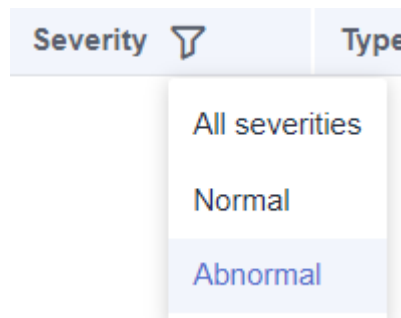
**Step 4** View component events. You can set filter criteria to view events.

The search criteria are as follows:

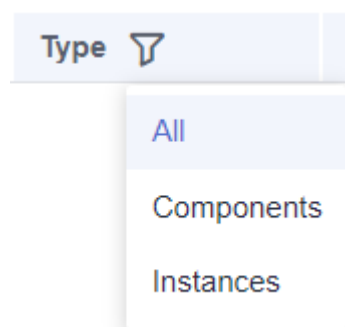
- Filter by component name: Select a component to filter and display the data generated within one hour for the component. You can also search for and select a component from the drop-down list of the filter criteria.



- Filter by event severity: You can select **All severities**, **Normal**, or **Abnormal**. Abnormal events require special attention.



- Filter by event type: You can select **All**, **Components**, or **Instances**.



- Search by event name: Enter an event name and click  .

 **NOTE**

Events help you view component activities. If a fault occurs, you can view component events to locate the fault.





----End

## 8.2 Viewing Component Monitoring

Component monitoring displays some component metrics. You can determine the health status of your services based on these metrics. You can customize monitoring metrics. For details, see [Configuring Custom Metric](#).

### NOTE

- [Configure performance management](#) probes to collect more service metrics.
- If you have [configured performance management](#), click **go to Application Performance Management (APM)** to view more service metrics.

### Prerequisites

1. You have created an application. For details, see [Creating an Application](#).
2. You have created a component. For details, see [Creating a Component](#).

### Procedure

**Step 1** [Log in to CAE](#).

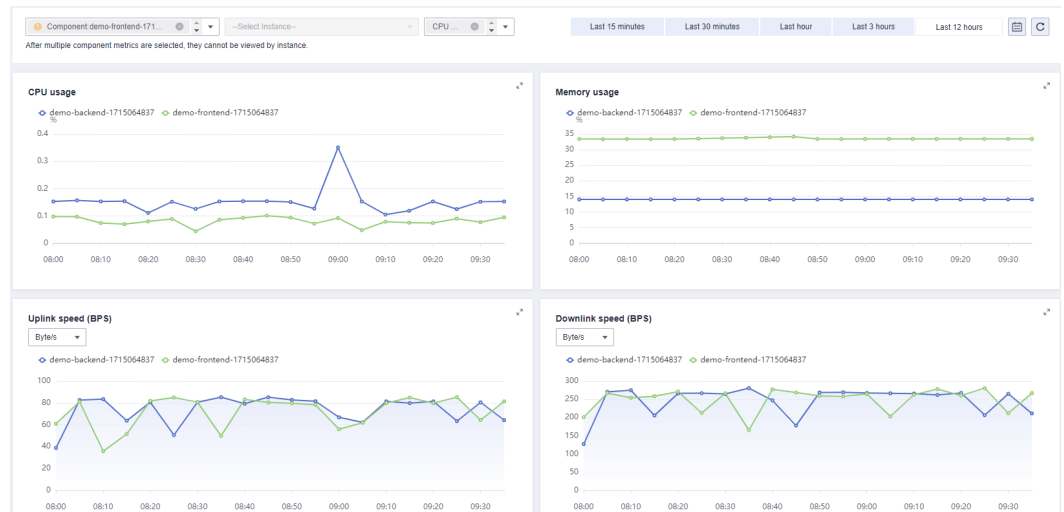
**Step 2** Choose **Component Monitoring**.

**Step 3** Use the three drop-down lists to select components, instances, and monitoring metrics to view component monitoring information.

**NOTE**

You can select multiple components from the drop-down list to view their statuses at the same time. If multiple components are selected, you cannot view the statuses by instance or custom metric.

**Figure 8-1** Multi-component monitoring



**Step 4** You can view uplink and downlink speeds, uplink and downlink rates, CPU and memory usage, and custom metrics. For details, see [Table 8-2](#).

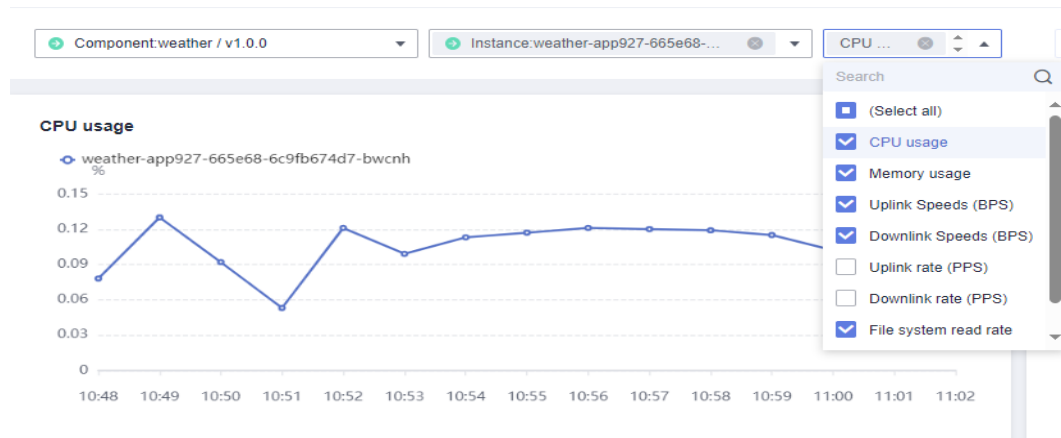
**Table 8-2** Component monitoring information

Parameter	Description
Uplink Speeds (BPS)	Outbound traffic speed of a measured object
Downlink Speeds (BPS)	Inbound traffic speed of a measured object
Uplink rate (PPS)	Number of data packets sent by a NIC per second
Downlink rate (PPS)	Number of data packets received by a NIC per second
CPU usage	CPU usage of an instance
Memory usage	Memory usage of an instance
File system read rate	Number of bytes read from the file system per unit time
File system write rate	Number of bytes written to the file system per unit time
Custom metric	Monitoring dimension configured in <a href="#">Configuring Custom Metric</a>

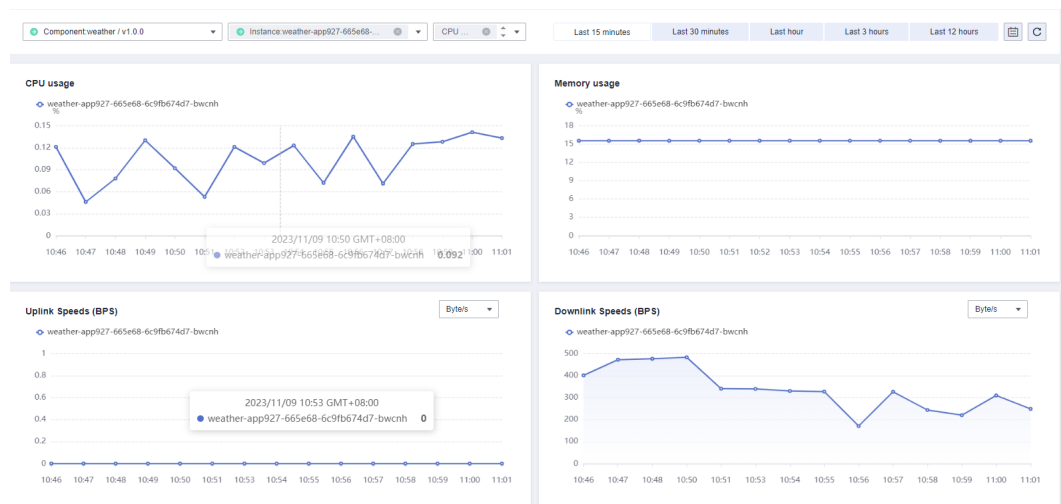
**NOTE**

By default, **Uplink Speeds (BPS)**, **Downlink Speeds (BPS)**, **CPU usage**, and **Memory usage** are displayed. Select or deselect metrics from the drop-down list as required.

**Figure 8-2** Selecting monitoring metrics to be displayed



**Figure 8-3** Viewing component monitoring



----End

## 8.3 Viewing Component Logs

**NOTE**

- The page displays up to 500 logs. To view more, go to Log Tank Service (LTS) to view real-time standard output logs.
- The system continues to collect logs beyond the free quota (500 MB). You will be billed for extra logs on a pay-per-use basis. For details, see [Pricing Details](#).
- By default, log data is stored for 30 days. Retained logs are deleted at the end of the duration. For long-term storage, transfer logs to OBS buckets. For details, see [Log Transfer](#).

## Prerequisites

1. You have created an application. For details, see [Creating an Application](#).
2. You have created a component. For details, see [Creating a Component](#).

## Procedure

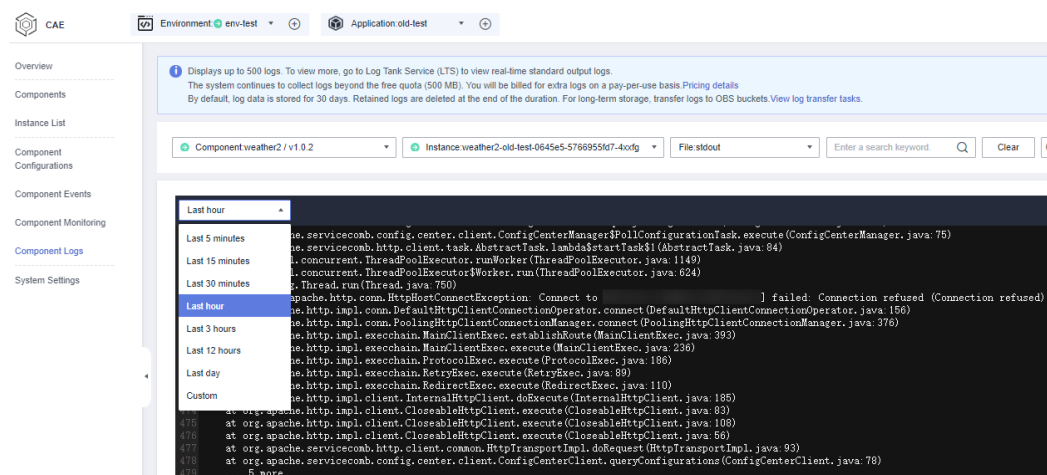
**Step 1** [Log in to CAE](#).

**Step 2** Choose **Component Logs** to view and locate component faults.

**Step 3** Use the drop-down lists to select environments, applications, components, and component instances, and view component logs.

**Step 4** The page displays component instance logs in different time dimensions. You can select a time dimension from the drop-down list. CAE also allows you to view component instance logs in a specified time period.

**Figure 8-4** Viewing logs



----End

# 9 System Settings

This section describes cloud storage authorizations, source code repository authorizations, domain names, certificates, and start/stop policy configuration.

## 9.1 Authorizing Cloud Storage

Cloud storage is a service that provides storage for applications. CAE supports multiple types of cloud storage mounting. Cloud storage can be mounted to containers to ensure application reliability.

After authorization, the cloud storage will be used by each component, but must be **configured** in the corresponding component configuration.

### Authorizing a Parallel File System

 **NOTE**

- This service supports only authorization and creation of parallel file systems with multi-AZ data redundancy storage and Standard storage.
- Before authorizing a parallel file system, ensure its object data is backed up or out of use, and not occupied by other services (such as CTS and Cloud Eye).
- Parallel file systems are charged separately. For details, see [Product Pricing Details](#).

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Cloud Storage Authorizations** module.

**Step 4** Click **Authorize Parallel File System**.

**Step 5** (Optional) To create a parallel file system, click **Create Parallel File System**, enter a name, and click **OK**.

**Step 6** Select the created parallel file system. You can also enter a keyword in the search box above the list to filter data.

**Step 7** Click **Authorize**.

**Step 8** In the displayed dialog box, enter the AK/SK and click **OK**.

You can click **Obtain Access Key** to obtain the AK/SK. For details, see [Access Keys](#).

 NOTE

If your environment was created before April 20, 2024, skip this step.

**Step 9** If "Authorization successful" is displayed, the parallel file system has been authorized.

----End

## Authorizing a Bucket

 NOTE

- This service supports only authorization and creation of Standard buckets.
- Before authorizing object storage, ensure its data is backed up or out of use, and not occupied by other services (such as CTS and Cloud Eye).
- Buckets are charged separately. For details, see [Pricing Details](#).

**Step 1** [Log in to CAE](#).

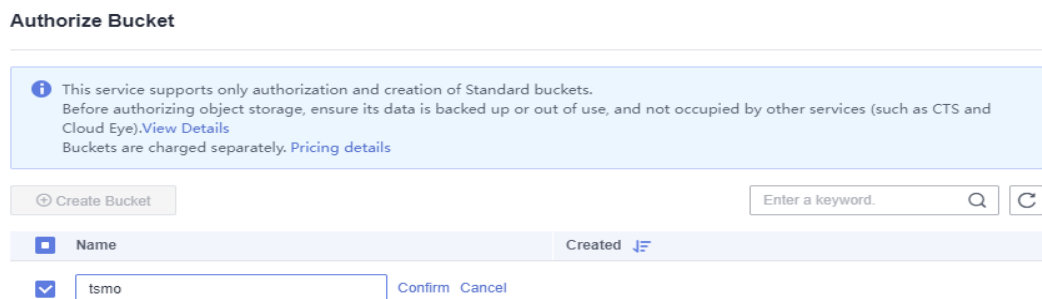
**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Cloud Storage Authorizations** module.

**Step 4** Click **Authorize Bucket**.

**Step 5** (Optional) To create a bucket, click **Create Bucket**, enter a name, and click **OK**.

**Figure 9-1** Authorizing a bucket



**Step 6** Select the created bucket. You can also enter a keyword in the search box above the list to filter data.

**Step 7** Click **Authorize**.

**Step 8** In the displayed dialog box, enter the AK/SK and click **OK**.

You can click **Obtain Access Key** to obtain the AK/SK. For details, see [Access Keys](#).

 NOTE

If your environment was created before April 20, 2024, skip this step.

**Step 9** If "Authorization successful" is displayed, the bucket has been authorized.

----End

## Unbinding Cloud Storage

 NOTE

If the authorized cloud storage has been bound to a component, choose **Component Configurations > Cloud Storage** to delete the mounted data of the component before unbinding the cloud storage. For details, see [Deleting a Cloud Storage Mounting Configuration](#).

- Step 1** [Log in to CAE](#).
  - Step 2** Choose **System Settings**.
  - Step 3** Click **Edit** in the **Cloud Storage Authorizations** module.
  - Step 4** Select the target cloud storage and click **Unbind** in the **Operation** column.
- End

## 9.2 Authorizing a Source Code Repository

### Creating an Authorization

- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Source Code Repository Authorizations** module.
- Step 4** Click **Create Authorization**, select the required source code repository by referring to [Table 9-1](#), and set parameters.

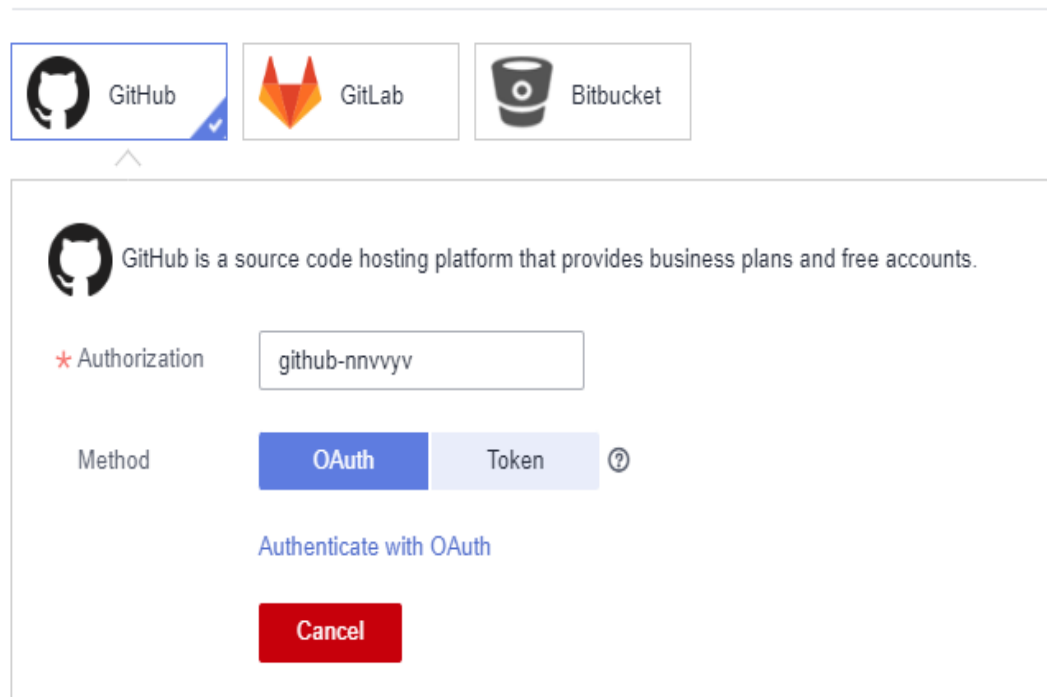
**Table 9-1** Authorization parameters

Parameter	Description
*Authoriza tion	Authorization name, which cannot be changed after being created.
*Repositor y Type	The following official repositories are supported: <ul style="list-style-type: none"> <li>● GitHub (<a href="https://github.com">https://github.com</a>) Authorization mode: OAuth or private token.</li> <li>● Bitbucket (<a href="https://bitbucket.org">https://bitbucket.org</a>) Authorization mode: OAuth or private Bitbucket.</li> <li>● GitLab (<a href="https://gitlab.com">https://gitlab.com</a>) Authorization mode: OAuth or private token.</li> </ul>

- Step 5** Click **OK**.

**Figure 9-2** Creating a source code repository authorization

### Authorized Source Code Repository



**Step 6** In the **Service Statement** dialog box, select **I understand that the source code building function of the ServiceStage service collects the information above and agree to authorize the collection and use of the information**. Click **OK**.

**Step 7** On the **Authorized Source Code Repository** page, you can view the authorization information about the authorized source code repositories, including the authorization name, status, type, repository username, authorization mode, creation time, and update time.

----End

### Re-authorizing a Source Code Repository

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Source Code Repository Authorizations** module.

**Step 4** Select the target authorization and click **Re-authorize** in the **Operation** column.

#### NOTE

During re-authorization, the code source repository cannot be changed. You can only select another authorization mode.

**Step 5** Click **OK**.

----End



## Deleting an Authorization

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

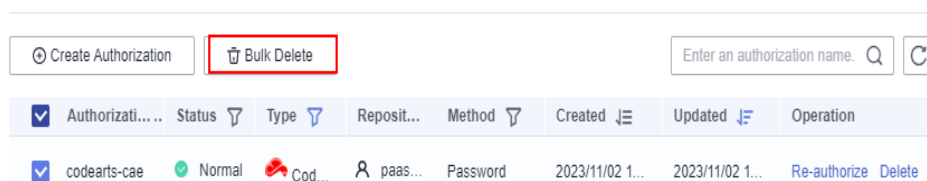
**Step 3** Click **Edit** in the **Source Code Repository Authorizations** module.

**Step 4** Use either of the following methods to delete an authorization:

- Batch deletion
  - a. Select the target authorized source code repositories and click to delete **Bulk Delete**.

**Figure 9-3** Batch deletion

Authorized Source Code Repository



- b. In the displayed dialog box, enter **DELETE** and click **OK**.
- Individual deletion
    - a. Select the target authorized source code repository and click **Delete** in the **Operation** column.
    - b. In the displayed dialog box, enter **DELETE** and click **OK**.

----End

## 9.3 Configuring a Domain Name

### NOTE

- Before configuring a domain name in CAE, ensure that you have purchased a domain name and the domain name has been licensed by the Ministry of Industry and Information Technology (MIIT).
- You can bind up to 100 domain names.
- For details about how to configure the domain name, see [How Do I Bind a User-Defined Domain Name to CAE?](#)

### Adding a Domain Name

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Domain Names** module.

**Step 4** Click **Add Domain Name** and enter the licensed domain name.

**Step 5** Click **OK**.

----End

## Unbinding a Domain Name

- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Domain Names** module.
- Step 4** Select the target domain name and click **Unbind** in the **Operation** column.
- Step 5** In the displayed dialog box, click **OK**.

### NOTE

If "The domain name is still used in the following components. Go to Component Configurations > Public Network Access > Forwarding Policy to check whether the forwarding policy has been deleted." is displayed during unbinding, choose **Component Configurations > Access Mode > Forwarding Policy** to check whether the domain name is in use.

----End

For more operations, see:

- [How Do I Bind a User-Defined Domain Name to CAE?](#)
- [How Do I Test the Domain Name Resolution?](#)
- [How Do I Migrate a Domain Name to Huawei Cloud?](#)
- [How Does a Domain Name Configured on a Third-Party Cloud Support Huawei Cloud Services?](#)

## 9.4 Configuring Certificates

### NOTE

You can bind up to 10 certificates.

### Adding a Certificate

- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Certificates** module.
- Step 4** Click **Add Certificate**.
- Step 5** Enter a certificate name For example, **test-1**.
- Step 6** Upload **Server Certificate Content** and **Server Private Key Content**.
- Step 7** Click **OK**.

----End

### Editing a Certificate

- Step 1** [Log in to CAE](#).

- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Certificates** module.
- Step 4** Select the target certificate and click **Edit** in the **Operation** column.
- Step 5** Edit **Server Certificate Content** and **Server Private Key Content**.

**Figure 9-4** Editing a certificate

**Edit Certificates**

---

\* Certificate Name

---

\* Server Certificate Content ?

```
cAAYE7FsZ9LNerOyjJpyi256oypdBvGs9JAUBN5WaFk81UQx29wAyNixX+bKa0DB
WpUDqr84V1f9vdQc75v9WoujcnIKszpV6qePPC7igJJpu4QOI362BrWzJCYQbg4
Uzo1KYBhLFx0TovAgMBAAGjc8wgcwHQPVDVR0OBBYEFM6TvDyvE2KsRy9zPq/J
WOjovG+WMIGcBgNVHSMEEgZQwGZGAFMBTvDyvE2KsRy9zPq/JWOjovG+WoW6kbDBq
MQswCQYDVQQGEwJ4eDELMAkGA1UECBMCEHgxGzAJBgNVBACeTAnh4MQswCQYDVQQK
EwJ4eDELMAkGA1UECjMCEHgxGzAJBgNVBAMTAnh4MR0wGAYJKoZIhvcNAQkBFg4
eHhAMTYzLmNvbYUJALV96mEIVF4EMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
BQADgYEAASkC/iwiALa2RU3YCxqZFEEsZzVQxikrDkDbFeoa6Tk49Fnb1f7FCW6
PTIY3HPWl5ygsMsSy0Fi3xp3jmulwzJhcQ3tcK5gC99HWp6Kw37RL8WoB8GWFU0Q
4tHLOjBkxZROPRhH+zMirQuexv6fsb3NWKhnlfh1Mj5wQE4Ldo=
-----END CERTIFICATE-----
```

---

\* Server Private Key Content ?

```
AoGBAJvLzJCyIsCjCKHwL6onbSUIDtyFwPVID1QrVatQYabF14g8CGUGZ/9fgheu
TXPtDcvu7cZdUArvgYw3I9F9IBb2Imf3a44xfiAKdDhzr4DK/vQhvhPuuTeZA41
r2zp8Cu+Bp40pSxmoAOK3B0/peZAka01Ju7c7ZChDWrxdeHZAKEA/6dcaWHofGS
eW5YLBsms3f0m0GH38nRI7oxyCW6yMIDkFHURVMBKW1OhrCuGo80nTMI5IH9gRg
5bH8XcuJQJBAMWBQgzCHyoSeryD3TFieXIFzgdBw6VeShyMjUjvqVdKoxRPvpO
kclc39QHP6Dm2wrXHEej+9RILx6ZCvQNbMCQQC42i+Uf0nHvPuXNUkZzomDHde
h1ySsOAO4H+8Y6OSI87I3HUrByCQ7stX1z3L0HofjHqV9Koy9emGTFLEzSdAkB7
Ei6cUKKmtkYe3rr+RcATEmwAw3IEJOHmrW5ErApVZK2TzLMQZ7WZpIPzQRCYnY
2ZZLDuZWFFG3vW+wKKktAkAaQ5GNzwbwRlpXF1FZFuNF7erxypzstbUmU/31b7IS
i5LmXTGKLxRYtZEHjya4kkkg140q1MrUsglybFYMF2
-----END RSA PRIVATE KEY-----
```

- Step 6** Click **OK**.
- End

## Deleting a Certificate

- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Certificates** module.
- Step 4** Select the target certificate and click **Delete** in the **Operation** column.
- Step 5** If **Deleted** is displayed, the certificate is deleted.

 **NOTE**

If **Failed to unbind xx** is displayed when you delete a certificate, choose **Component Configurations > Access Mode > Forwarding Policy** to check whether the certificate is in use.

----End

## 9.5 Configuring Start/Stop Policies

### NOTE

- You can configure up to 20 start/stop policies.
- Do not start or stop a component when it is being scaled. [Disable the AS policy](#) before the operation.
- When a component is being started, restarted, or stopped, AS policies cannot be added or enabled for the component.

### Adding a Start/Stop Policy

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Start/Stop Policy Configuration** module.

**Step 4** Click **Add Policy**. Configure the start/stop policy by referring to the following table.

Parameter	Description
Policy Name	Enter a policy name. The policy name must be unique.
Effectuated Components	<ul style="list-style-type: none"> <li>• <b>All in the environment:</b> The start/stop policy takes effect for all components in the environment.</li> <li>• <b>All in the application:</b> The start/stop policy takes effect for all components in the selected application.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Start/stop policies do not take effect for components in the <b>Not deployed</b> state.</li> <li>- For components in the <b>Deploying</b> state, start/stop policies will fail to be executed. For details about the failure cause, see <a href="#">Viewing a Start/Stop Policy</a>.</li> <li>- <b>All in the environment</b> and <b>All in the application</b> policies also take effect for newly added components.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Some:</b> The start/stop policy takes effect for the selected components.</li> </ul> <p><b>NOTE</b></p> <p>Components in the <b>Not deployed</b> state cannot be selected.</p>
Status	<ul style="list-style-type: none"> <li>• <b>Enable:</b> The start/stop policy is enabled and will be triggered at the specified time.</li> <li>• <b>Disabled:</b> The start/stop policy is disabled.</li> </ul>

Parameter	Description
Policy	<ul style="list-style-type: none"> <li>• <b>Start:</b> After the policy is configured, components will be started in batches. Components that have been started are not affected.</li> <li>• <b>Stop:</b> After the policy is configured, components will be stopped in batches. Components that have been stopped are not affected.</li> </ul>
Trigger	<ul style="list-style-type: none"> <li>• <b>Once:</b> The policy is triggered only once. After the policy is triggered, <b>Status</b> will be disabled.</li> <li>• <b>Periodically:</b> The policy is executed periodically. Currently, the policy can be executed by week or day.</li> </ul>
Triggered	<ul style="list-style-type: none"> <li>• Select a time when <b>Trigger</b> is set to <b>Once</b>.</li> <li>• When <b>Trigger</b> is set to <b>Periodically</b>: <ul style="list-style-type: none"> <li><b>Every week:</b> Select a date and time for triggering the policy every week. For example, 17:30 on every Monday.</li> <li><b>Every day:</b> Select a time for triggering the policy every day. For example, 01:00 every day.</li> </ul> </li> </ul> <p><b>NOTE</b> Triggered time must be at least two minutes after the current time.</p>

**Step 5** Click **OK**.

----End

## Editing a Start/Stop Policy

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Start/Stop Policy Configuration** module.

**Step 4** Select the target policy and click **Edit** in the **Operation** column. Reconfigure the policy by referring the following table.

Parameter	Description
Effectuated Components	<ul style="list-style-type: none"> <li>• <b>All in the environment:</b> The start/stop policy takes effect for all components in the environment.</li> <li>• <b>All in the application:</b> The start/stop policy takes effect for all components in the selected application.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Start/stop policies do not take effect for components in the <b>Not deployed</b> state.</li> <li>- For components in the <b>Deploying</b> state, start/stop policies will fail to be executed. For details about the failure cause, see <a href="#">Viewing a Start/Stop Policy</a>.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Some:</b> The start/stop policy takes effect for the selected components.</li> </ul> <p><b>NOTE</b></p> <p>Components in the <b>Not deployed</b> state cannot be selected.</p>
Status	<ul style="list-style-type: none"> <li>• <b>Enable:</b> The start/stop policy is enabled and will be triggered at the specified time.</li> <li>• <b>Disabled:</b> The start/stop policy is disabled.</li> </ul>
Policy	<ul style="list-style-type: none"> <li>• <b>Start:</b> After the policy is configured, components will be started in batches.</li> <li>• <b>Stop:</b> After the policy is configured, components will be stopped in batches.</li> </ul>
Trigger	<ul style="list-style-type: none"> <li>• <b>Once:</b> The policy is triggered only once. After the policy is triggered, <b>Status</b> will be disabled.</li> <li>• <b>Periodically:</b> The policy is executed periodically. Currently, the policy can be executed by week or day.</li> </ul>
Triggered	<ul style="list-style-type: none"> <li>• Select a time when <b>Trigger</b> is set to <b>Once</b>.</li> <li>• When <b>Trigger</b> is set to <b>Periodically</b>: <ul style="list-style-type: none"> <li><b>Every week:</b> Select a date and time for triggering the policy every week. For example, 17:30 on every Monday.</li> <li><b>Every day:</b> Select a time for triggering the policy every day. For example, 01:00 every day.</li> </ul> </li> </ul> <p><b>NOTE</b></p> <p>Triggered time must be at least two minutes after the current time.</p>

**Step 5** Click **OK**.

----End

## Deleting a Start/Stop Policy

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Start/Stop Policy Configuration** module.

**Step 4** Select the target policy and click **Delete** in the **Operation** column.

**Step 5** If **Deleted** is displayed, the policy is deleted.

----End

## Searching for a Start/Stop Policy

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Start/Stop Policy Configuration** module.

**Step 4** In the search box in the upper right corner, enter a policy name (fuzzy search is supported).

**Step 5** Click  to filter the start/stop policy.

----End

## Viewing a Start/Stop Policy

### NOTE

Policies in the **Not executed** and **Executing** states cannot be viewed.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Start/Stop Policy Configuration** module.

**Step 4** Select the target policy and click **Execution Details** in the **Operation** column.

**Step 5** View the execution status of the start/stop policy.

----End

# 9.6 Configuring System Network

## 9.6.1 Configuring Network Bandwidth

CAE displays the public IP address (outbound IP address) of the worker node in the cluster and the IP address (inbound IP address) to be associated with the public IP address for accessing components in CAE.

You can view and modify both the outbound and inbound bandwidths. The default bandwidth is 20 Mbit/s.

## Viewing System Network Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

- Step 3** Click **Edit** in the **System Network Configuration** module.
- Step 4** View the outbound IP address, outbound bandwidth, inbound IP address, and inbound bandwidth.

**Figure 9-5** Viewing system network configuration

### System Network Configuration

---

#### Connectivity Between CAE and Public Network

##### | Access Public Network in the CAE Environment

Outbound IP Address 100. [redacted] .19

Outbound Bandwidth 20  Mbit/s

##### | Access CAE Environment from the Public Network

Network Access IP Address 100. [redacted] 71

Inbound Bandwidth 20  Mbit/s

----End

## Modifying Inbound and Outbound Bandwidths


- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **System Network Configuration** module.
- Step 4** Click  and change the inbound and outbound bandwidths as required. The value must be an integer ranging from 1 to 300.



Figure 9-6 Modifying the bandwidths

## System Network Configuration

### Connectivity Between CAE and Public Network

#### | Access Public Network in the CAE Environment

Outbound IP Address 100. [redacted] 19

Outbound Bandwidth  ✓ ✗ Mbit/s

#### | Access CAE Environment from the Public Network

Network Access IP Address 100 [redacted] 71

Inbound Bandwidth 46  Mbit/s

**Step 5** Click ✓ to confirm the modification. If "System network configurations modified" is displayed, the system network configuration is complete.

Figure 9-7 Bandwidth modified

### System Network Configuration

Outbound Bandwidth: 4 Mbit/s

Inbound Bandwidth: 46 Mbit/s

VPCs to Access CAE Environments: 1

----End

## 9.6.2 Configuring VPC to Access the CAE Environment

After [adding the configuration for VPC to access the CAE environment](#), you can access the CAE application through the VPC network.

## Adding the Configuration for VPC to Access the CAE Environment

### NOTE

To use this function, you need to use a Huawei Cloud account with the **Security Administrator** permissions to access CAE and click **Authorize**. Existing functions are not affected if you do not perform authorization.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **System Network Configuration** module.

**Step 4** Click **Add Configuration** in the **Connectivity Between CAE and VPC** area.


**Step 5** Select a subnet from the drop-down list and click **OK**.

### NOTE

- **VPC** is fixed to the VPC associated with the environment during environment creation, and set **Subnet** to the subnet to which the environment belongs.
- Currently, only one configuration can be added.

**Figure 9-8** Configuring VPC to access the CAE environment

### Configure VPC to Access CAE Environment



VPC vpc-test(192. .0/24)

Subnet cae-subnet(192. .0/24) ▼

OK Cancel

----End

## Deleting the Configuration for VPC to Access the CAE Environment

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **System Network Configuration** module.

**Step 4** Select the target configuration and click **Delete** in the **Operation** column.

**Step 5** In the displayed dialog box, enter **SWITCHOFF** and click **OK**.

----End

## 9.6.3 Configuring the CAE Environment to Access VPC

The CAE environment uses its VPC network configurations to enable its components to access services in other networks (VPC and IDC).

## Adding the Configuration for the CAE Environment to Access VPC

 NOTE

To use this function, you need to create a [VPC peering connection](#) between the VPC to be accessed and the VPC to which the CAE environment belongs.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **System Network Configuration** module.

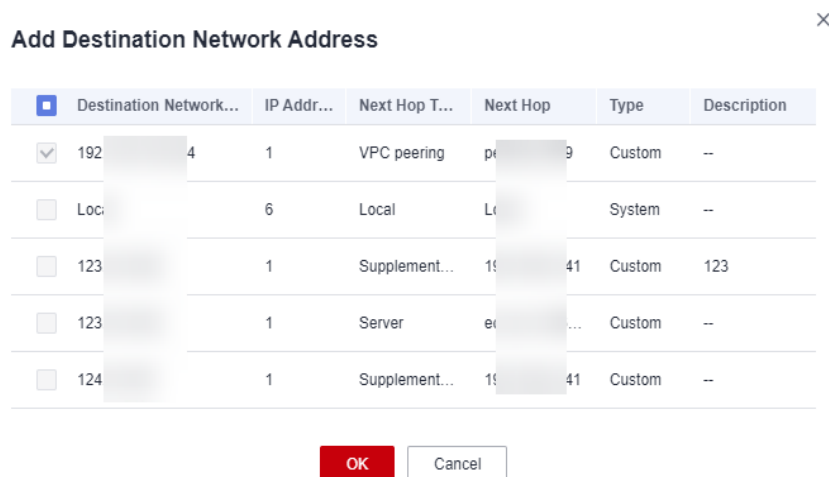
**Step 4** Click **Add Destination Network Address** in the **Access VPC in the CAE Environment** area.

**Step 5** Select the VPC to be accessed.

 NOTE

- The VPC to be accessed cannot conflict with the network segments reserved in CAE.
- Configurable addresses: VPC peering connection, VPN, Direct Connect, Cloud Connect, and Enterprise Router.

**Figure 9-9** Configuring the CAE environment to access VPC



**Step 6** Click **OK**.

----End

## Deleting the Configuration for the CAE Environment to Access VPC

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **System Network Configuration** module.

**Step 4** In the **Destination Network Address** list, select the target configuration and click **Delete** in the **Operation** column.

**Step 5** In the displayed dialog box, click **OK**.

----End

## 9.7 Configuring Event Notification Rules

This section describes how to configure event notification rules. If you have configured event notification rules, notifications will be sent when instance scheduling, health check, image pull, volume mounting, or container startup succeeds or fails. In this way, you can handle alarms in a timely manner.

### NOTE

- You can configure up to 50 event notification rules.
- The Simple Message Notification (SMN) service is charged separately. For details, see [Pricing Details](#).

### Data Privacy Statement

- The SMN service encrypts and saves the subscription endpoint information of the DingTalk robot, Lark robot, and WeCom chatbot entered by users in the database so that SMN can send messages to DingTalk, Lark, and WeCom groups.
- SMN does not use the subscription endpoint information for other purposes except sending group messages.
- After a user deletes a subscription endpoint, SMN permanently deletes the subscription endpoint information from the database.

### Creating an Event Notification Rule

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Event Notification Rules** module.

**Step 4** Click **Create Event Notification Rule** and configure basic information by referring to [Table 9-2](#).

**Table 9-2** Configuring basic information

Parameter	Description
Name	Enter an event notification rule name. The name cannot be changed after creation. The value starts and ends with a letter and contains 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_).

Parameter	Description
Trigger Event	<p>Select an event that triggers notification from the drop-down list.</p> <ul style="list-style-type: none"> <li>• Health checked</li> <li>• Health check failed</li> <li>• Image pulled</li> <li>• Pull image failed</li> <li>• Container started up</li> <li>• Container startup failed</li> <li>• Volume mounted</li> <li>• Attach volume failed</li> </ul>
Effectuated Components	<ul style="list-style-type: none"> <li>• <b>All in the environment:</b> The rule takes effect for all components in the environment.</li> <li>• <b>All in the application:</b> The rule takes effect for all components in the selected application. <b>NOTE</b> All in the environment and All in the application policies also take effect for newly added components.</li> <li>• <b>Some:</b> The rule takes effect for the selected components. <b>NOTE</b> Components in the <b>Not deployed</b> state cannot be selected.</li> </ul>
Alarm Policy	<ul style="list-style-type: none"> <li>• <b>Trigger Mode:</b> Select <b>Accumulative</b> or <b>Immediate</b>.</li> <li>• <b>Monitor for:</b> Set this parameter when <b>Trigger Mode</b> is set to <b>Accumulative</b>. <ul style="list-style-type: none"> <li>- 5 minutes</li> <li>- 20 minutes</li> <li>- 1 hour</li> <li>- 4 hours</li> <li>- 24 hours</li> </ul> </li> <li>• <b>Occurrences:</b> Set this parameter when <b>Trigger Mode</b> is set to <b>Accumulative</b>. Value range: 1 to 100. The operators &gt; and ≥ are supported.</li> </ul>

**Step 5** Configure the event notification sending mode and endpoint address.

- **WeCom chatbot:** Enter a webhook address starting with **https://qyapi.weixin.qq.com/cgi-bin/webhook/send**.

 **NOTE**

- WeCom chatbot is an OBT function. If you want to configure event notification for it, [submit a service ticket](#) to apply for OBT qualification from Huawei Cloud. After the application is approved, you can create event notification rules.
- For details about how to obtain a WeCom subscription endpoint, see [How Does DingTalk, Lark, or WeCom Chatbot Obtain Subscription Endpoints?](#)

- **Emails:** Enter an email address, for example, **12345678@163.com**.
- **SMS:** Enter the subscription endpoint address, for example, **13900000000**.

**Step 6** Click **OK**.

 **NOTE**

After creation, click the subscription confirmation link in the email or SMS to confirm the subscription. Otherwise, SMN cannot send messages when the trigger conditions are met.

----End

## Editing an Event Notification Rule

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Event Notification Rules** module.

**Step 4** Select the target rule and click **Edit** in the **Operation** column.

**Step 5** Edit the event notification rule again by referring to [Table 9-3](#).

**Table 9-3** Editing an event notification rule

Parameter	Description
Trigger Event	<p>Select an event that triggers notification from the drop-down list.</p> <ul style="list-style-type: none"> <li>• Health checked</li> <li>• Health check failed</li> <li>• Image pulled</li> <li>• Pull image failed</li> <li>• Container started up</li> <li>• Container startup failed</li> <li>• Volume mounted</li> <li>• Attach volume failed</li> </ul>
Effectuated Components	<ul style="list-style-type: none"> <li>• <b>All in the environment:</b> The rule takes effect for all components in the environment.</li> <li>• <b>All in the application:</b> The rule takes effect for all components in the selected application.</li> </ul> <p><b>NOTE</b> All in the environment and All in the application policies also take effect for newly added components.</p> <ul style="list-style-type: none"> <li>• <b>Some:</b> The rule takes effect for the selected components.</li> </ul> <p><b>NOTE</b> Components in the <b>Not deployed</b> state cannot be selected.</p>

Parameter	Description
Alarm Policy	<ul style="list-style-type: none"> <li>• <b>Trigger Mode:</b> Select <b>Accumulative</b> or <b>Immediate</b>.</li> <li>• <b>Monitor for:</b> Set this parameter when <b>Trigger Mode</b> is set to <b>Accumulative</b>. <ul style="list-style-type: none"> <li>- 5 minutes</li> <li>- 20 minutes</li> <li>- 1 hour</li> <li>- 4 hours</li> <li>- 24 hours</li> </ul> </li> <li>• <b>Occurrences:</b> Set this parameter when <b>Trigger Mode</b> is set to <b>Accumulative</b>. Value range: 1 to 100. The operators &gt; and ≥ are supported.</li> </ul>

**Step 6** Click **OK**.

After editing, the event notification rule is enabled.

----End

## Deleting an Event Notification Rule

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Event Notification Rules** module.

**Step 4** Select the target rule and click **Delete** in the **Operation** column.

**Step 5** If **Deleted** is displayed, the rule is deleted.

----End

## Viewing an Event Notification Rule

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Event Notification Rules** module.

**Step 4** On the event notification rule details page, you can view the name, status, and configuration of the created event notification rules.

----End

## Enabling or Disabling an Event Notification Rule



You can enable or disable a created event notification rule.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Event Notification Rules** module.

**Step 4** In the event notification rule list, select a rule and click the button in the **Status** column.

-  indicates that the rule is enabled.
-  indicates that the rule is disabled.

**Step 5** If **Event notification rule updated** is displayed, the rule is enabled or disabled.

----End

## 9.8 Configuring the Monitoring System

CAE supports APM 2.0 probes. The collection mode can be enhanced probe.

After you configure the monitoring system and [enable performance management](#), APM Agents periodically collect performance metric data to measure the overall health status of applications.

### Precautions

- This function can be enabled only when APM of the corresponding version is deployed and enabled in the environment.
- JDK 7 and JDK 8 are supported.
- Tomcat 6.x, 7.x, and 8.x are supported. For details, see [Usage Restrictions](#).
- Currently, CAE supports performance management only for Java 8, Java 11, Tomcat 8, Tomcat 9, and Docker components.

### Adding the Monitoring System Configuration

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Monitoring System Configuration** module.

**Step 4** Configure the monitoring system by referring to [Table 9-4](#) and [Table 9-5](#).

**Table 9-4** Basic Info

Parameter	Description
Monitoring System	Currently, only APM 2.0 is supported.
Collection Mode	<p><b>Enhanced Probe</b> is recommended.</p> <ul style="list-style-type: none"> <li>• <b>Enhanced Probe</b>: provides richer and more stable performance.</li> <li>• <b>OpenTelemetry</b>: provides open source observable framework.</li> </ul>



Parameter	Description
Code Configuration Mode	<b>Enable auto probe injection (Java only)</b> is selected by default.
Probe Version	Select a probe version from the drop-down list.
Upgrade Policy	Select a probe upgrade policy. By default, <b>Automatic upgrade upon restart</b> is selected. <ul style="list-style-type: none"> <li>• <b>Automatic upgrade upon restart:</b> The system downloads the image upon each restart.</li> <li>• <b>Manual upgrade:</b> If a local image is available, it will be used. If no local image is available, the system downloads the probe image.</li> </ul>

**Table 9-5** Access Info

Parameter	Description
APM Application	Select the APM application to be connected from the drop-down list. If the application does not exist, click <b>Go to APM to create an APM application</b> .
Access Point	The value is automatically obtained.
AccessKey	The first access key of APM 2.0 is automatically obtained. If no access key is available, click <b>Go to APM to create an access key</b> .
SecretKey	The value is automatically obtained.


**Figure 9-10** Configuring Enhanced Probe

**Monitoring System Configuration**

i Once modified, reconfigure performance management in Component Configurations and apply the changes. ✕

**Basic Info**

\* Monitoring System APM 2.0

\* Collection Mode Recommended  
  
**Enhanced Probe**  
Provides richer and more stable performance.

Code Configuration Mode  Enable auto probe injection (Java only)

\* Probe Version 2.4.5-profiler-x86\_64 ▼

\* Upgrade Policy Automatic upgrade upon r... ▼


---

**Access Info**

\* APM Application default ▼ C [Go to APM to create an APM application](#)

Access Point https://

\* AccessKey ff ▼ C [Go to APM to create an access key](#)

SecretKey \*\*\*\*\* 

**Step 5** Click **OK**.

----End

## Modifying the Monitoring System Configuration

 **NOTE**

Once modified, reconfigure performance management in **Component Configurations** and apply the changes.

**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Monitoring System Configuration** module.

**Step 4** Update the monitoring system configuration by referring to [Table 9-6](#) and [Table 9-7](#).

**Table 9-6** Basic Info

Parameter	Description
Monitoring System	Currently, only APM 2.0 is supported.
Collection Mode	<p><b>Enhanced Probe</b> is recommended.</p> <ul style="list-style-type: none"> <li>• <b>Enhanced Probe</b>: provides richer and more stable performance.</li> <li>• <b>OpenTelemetry</b>: provides open source observable framework.</li> </ul>
Code Configuration Mode	<b>Enable auto probe injection (Java only)</b> is selected by default.
Probe Version	Select a probe version from the drop-down list.
Upgrade Policy	<p>Select a probe upgrade policy. By default, <b>Automatic upgrade upon restart</b> is selected.</p> <ul style="list-style-type: none"> <li>• <b>Automatic upgrade upon restart</b>: The system downloads the image upon each restart.</li> <li>• <b>Manual upgrade</b>: If a local image is available, it will be used. If no local image is available, the system downloads the probe image.</li> </ul>

**Table 9-7** Access Info

Parameter	Description
APM Application	Select the APM application to be connected from the drop-down list. If the application does not exist, click <b>Go to APM to create an APM application</b> .
Access Point	The value is automatically obtained.
AccessKey	The first access key of APM 2.0 is automatically obtained. If no access key is available, click <b>Go to APM to create an access key</b> .
SecretKey	The value is automatically obtained.

**Step 5** Click **OK**.

----**End**

## 9.9 Configuring a DEW Secret

After configuring a secret, you can import it into a component as an environment variable in **Component Configurations**.

### Application Scenario

Each enterprise has its own core sensitive data, which needs to be encrypted. To improve data security, CAE allows you to add DEW secrets and import them into components as environment variables to protect data.

### Restrictions

You must authorize KMS CMKFullAccess and CSMS ReadOnlyAccess to agency cae\_trust.

Otherwise, you need to re-authorize the agency when accessing CAE.

### Adding a Secret

 **NOTE**

You can add up to 20 secrets.

**Step 1** [Log in to CAE](#).

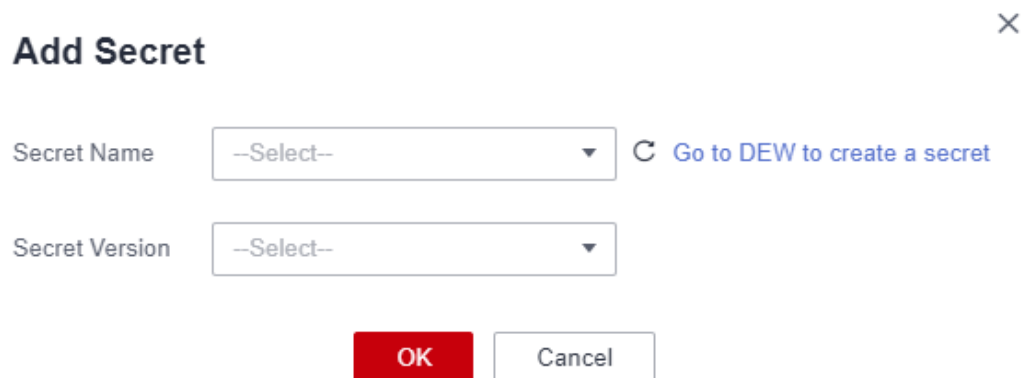
**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Secret Configuration** module.

**Step 4** Click **Create Secret**. In the displayed dialog box, select the secret name and version.

If no secret is available, click **Go to DEW to create a secret** and create one. For details, see [Creating a Secret](#).

**Figure 9-11** Adding a secret



**Add Secret** ×

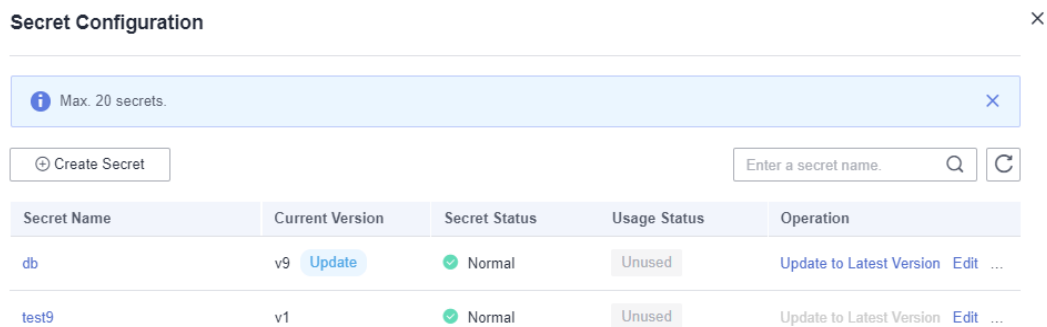
Secret Name  ↻ [Go to DEW to create a secret](#)

Secret Version

OK Cancel

**Step 5** Click **OK**.

**Figure 9-12** Viewing secret details



After the secret is added, choose **Component Configurations > Environment Variable** to configure it and make it take effect. For details, see [Adding an Environment Variable](#).

----End

## Viewing a Secret

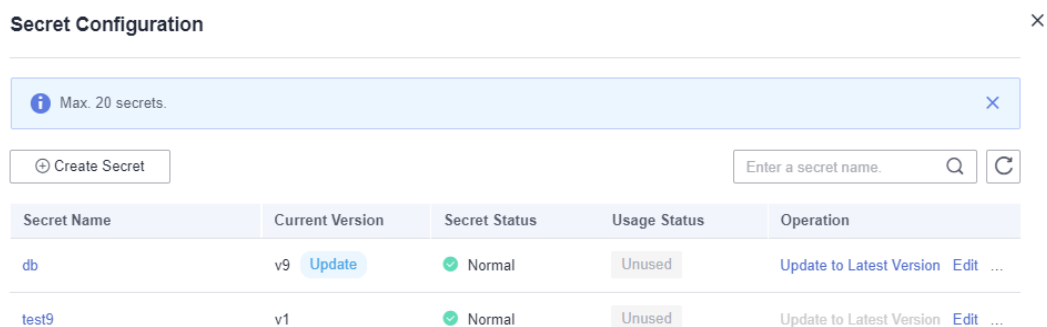
**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Secret Configuration** module.

**Step 4** On the **Secret Configuration** page, view the list of bound secrets, including the name, version, status, and usage status.

**Figure 9-13** Viewing secret details



----End

## Modifying a Secret

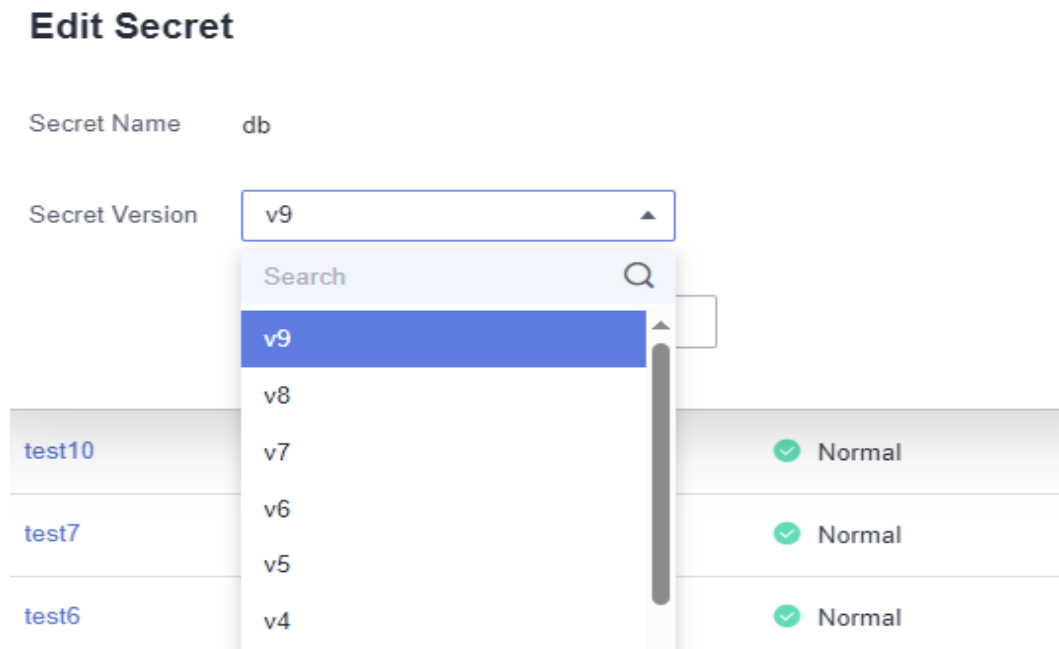
**Step 1** [Log in to CAE](#).

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Secret Configuration** module.

- Step 4** Select the target secret and click **Edit** in the **Operation** column.
- Step 5** Select a secret version from the drop-down list and click **OK**.

**Figure 9-14** Editing a secret

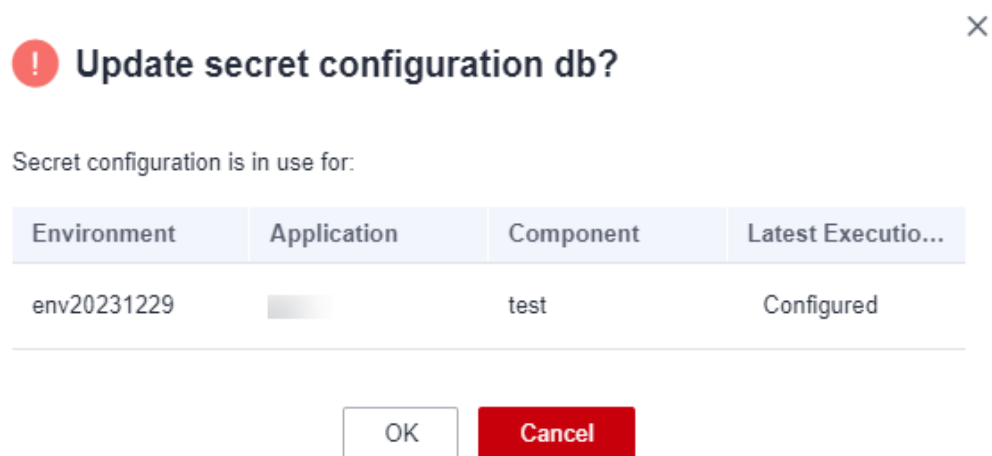


- Step 6** (Optional) If the secret has been configured in **Component Configurations** > **Environment Variable** and has taken effect, confirm the component usage in the displayed dialog box and click **OK**.

**NOTE**

After the update is confirmed, the environment variables that have been configured using this secret will be updated synchronously.

**Figure 9-15** Confirming update



- Step 7** If "Secret configuration updated." is displayed, the secret has been updated.  
----End

## Updating a Secret

- Step 1** [Log in to CAE](#).
- Step 2** Choose **System Settings**.
- Step 3** Click **Edit** in the **Secret Configuration** module.
- Step 4** Select the target secret and click **Update to Latest Version**.

**Figure 9-16** Updating a secret

### Secret Configuration

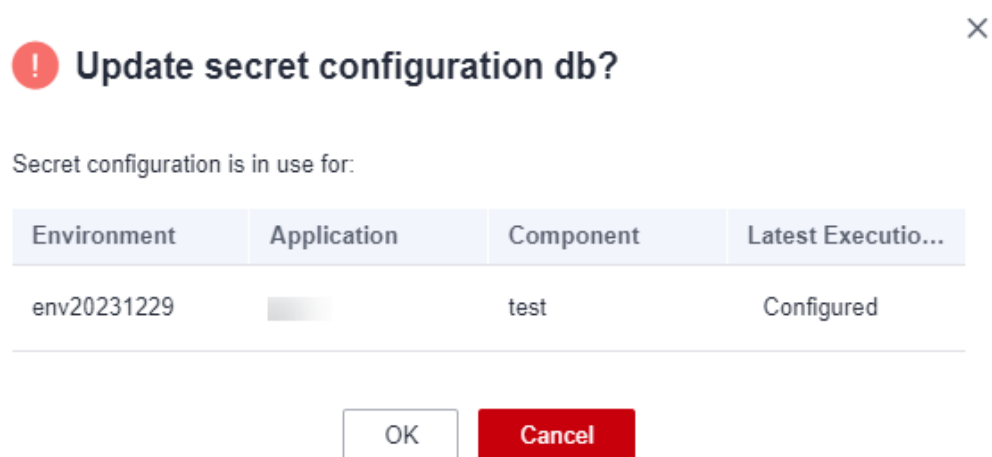
Secret Name	Current Version	Secret Status	Usage Status	Operation
db	v9 <a href="#">Update</a>	Normal	Using	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> ...
test9	v1	Normal	Unused	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> ...

- Step 5** (Optional) If the secret has been configured in **Component Configurations** > **Environment Variable** and has taken effect, confirm the component usage in the displayed dialog box and click **OK**.

### NOTE

After the update is confirmed, the environment variables that have been configured using this secret will be updated synchronously.

**Figure 9-17** Confirming update



- Step 6** If "Secret configuration updated." is displayed, the secret has been updated.

The secret will be automatically updated to the latest version.

----End

## Deleting a Secret

### NOTE

The secret that has been used cannot be deleted. Modify it and try again.

**Step 1** Log in to CAE.

**Step 2** Choose **System Settings**.

**Step 3** Click **Edit** in the **Secret Configuration** module.

**Step 4** Select the target secret and click **Delete** in the **Operation** column.

**Figure 9-18** Deleting a secret

Secret Configuration

Max. 20 secrets.
×

+ Create Secret

Enter a secret name. Q C

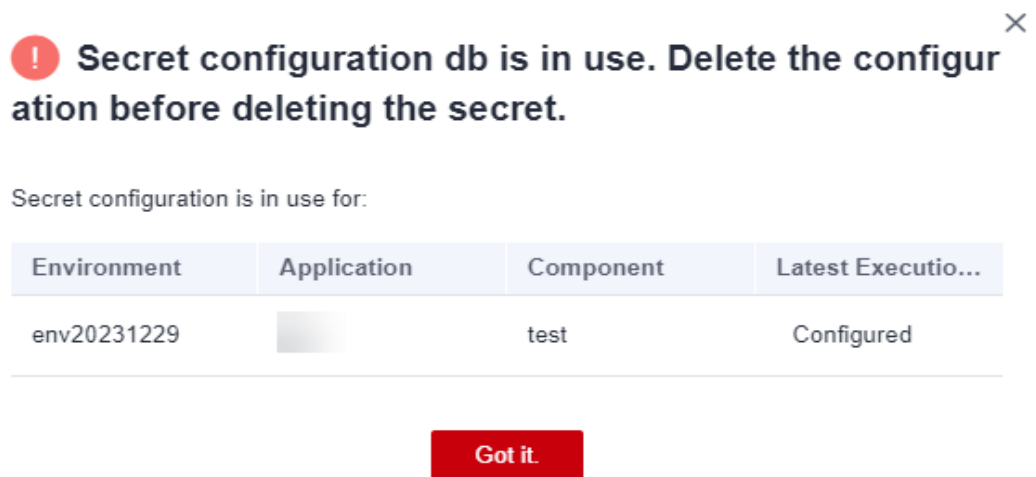
Secret Name	Current Version	Secret Status	Usage Status	Operation
db	v9 <span style="background-color: #add8e6; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Update</span>	<span style="color: green;">✔</span> Normal	<span style="background-color: #e0ffe0; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Using</span>	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> <a href="#">Delete</a>
test9	v1	<span style="color: green;">✔</span> Normal	<span style="background-color: #f2f2f2; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Unused</span>	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> <a href="#">Delete</a>
test8	v1	<span style="color: green;">✔</span> Normal	<span style="background-color: #f2f2f2; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Unused</span>	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> <a href="#">Delete</a>
test10	v1	<span style="color: green;">✔</span> Normal	<span style="background-color: #f2f2f2; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Unused</span>	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> <span style="border: 2px solid red; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Delete</span>
test7	v1	<span style="color: green;">✔</span> Normal	<span style="background-color: #f2f2f2; padding: 2px 5px; border-radius: 3px; font-size: 12px;">Unused</span>	<a href="#">Update to Latest Version</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Step 5** (Optional) If the secret has been configured in **Component Configurations > Environment Variable** and has taken effect, confirm the component usage in the displayed dialog box and click **Got it**.

Modify the component environment variables in use as prompted and try again.



**Figure 9-19** Confirming deletion



**Step 6** If "Secret configuration deleted." is displayed, the secret has been deleted.

----End

# 10 Key Operations Recorded by CTS

## 10.1 CAE Operations That Can Be Recorded by CTS

With CTS, you can record operations associated with CAE for future query, audit, and backtrack operations.

After CTS is **enabled**, the system starts recording operations on CAE resources. You can view the operation records of the last seven days on the CTS console.

**Table 10-1** CAE operations that can be recorded by CTS

Operation	Resource Type	Event Name
Creating a component	component	createComponent
Deleting a component	component	deleteComponent
Upgrading a component	component	upgradeComponent
Starting a component	component	startComponent
Stopping a component	component	stopComponent
Restarting a component	component	restartComponent
Scaling a component	component	scaleComponent
Rolling back a component	component	rollbackComponent

Operation	Resource Type	Event Name
Deploying a component	component	deployComponent
Configuring a component	component	configureComponent
Creating an application	application	createApplication
Deleting an application	application	deleteApplication
Creating an environment	environment	createEnvironment
Deleting an environment	environment	deleteEnvironment
Binding cloud storage	cloudStorage	bindCloudStorage
Unbinding cloud storage	cloudStorage	unbindCloudStorage
Creating a certificate	Certificate	createCertificate
Updating a certificate	Certificate	updateCertificate
Deleting a certificate	Certificate	deleteCertificate
Creating a domain name	Domain	createDomain
Deleting a domain name	Domain	deleteDomain
Creating a scheduled start/stop policy	TimerRules	createTimerRules
Updating a scheduled start/stop policy	TimerRules	updateTimerRules

Operation	Resource Type	Event Name
Deleting a scheduled start/stop policy	TimerRules	deleteTimerRules

## 10.2 Querying Archived Traces

### Scenarios

CTS periodically sends trace files to OBS buckets. A trace file is a collection of traces. CTS generates trace files based on services and transfer cycle, and adjusts the number of traces contained in each trace file as needed. CTS can also save audit logs to LTS log streams.


This section describes how to view historical operation records in trace files downloaded from OBS buckets and in LTS log streams.

### Prerequisites

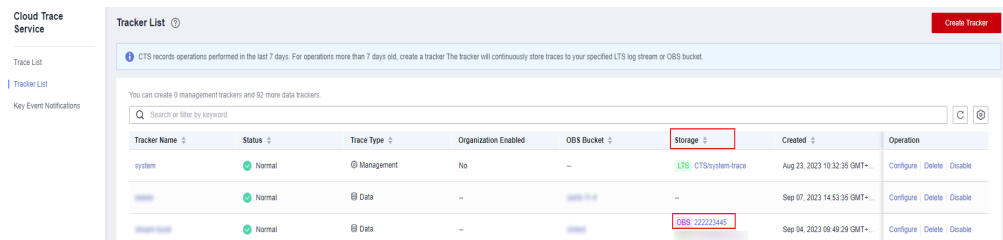
You have configured a tracker in CTS and enabled **Transfer to OBS** or **Transfer to LTS**. For details, see [Configuring a Tracker](#).

### Querying Traces Transferred to OBS

If you enable **Transfer to OBS** when configuring the tracker, traces will be periodically transferred to a specified OBS bucket as trace files for long-term storage.

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
3. Choose **Tracker List** in the navigation pane on the left.
4. Click a bucket in the **OBS Bucket** column.

**Figure 10-1** Selecting an OBS bucket



5. In the OBS bucket, locate the file storage path to view the desired trace, and click **Download** on the right to download the file to the default download path of the browser. If you need to save it to a custom path, click **More > Download As** on the right.

- The trace file storage path is as follows:  
***OBS bucket name > CloudTraces > Region > Year > Month > Day > Tracker name > Service directory***  
An example is ***User-defined name > CloudTraces > region > 2016 > 5 > 19 > system > ECS***.
- The trace file naming format is as follows:  
***Trace file prefix\_CloudTrace\_Region/Region-project\_Time when the trace file was uploaded to OBS: Year-Month-DayT Hour-Minute-SecondZ\_Random characters.json.gz***  
An example is ***File Prefix\_CloudTrace\_region-project\_2016-05-30T16-20-56Z\_21d36ced8c8af71e.json.gz***.

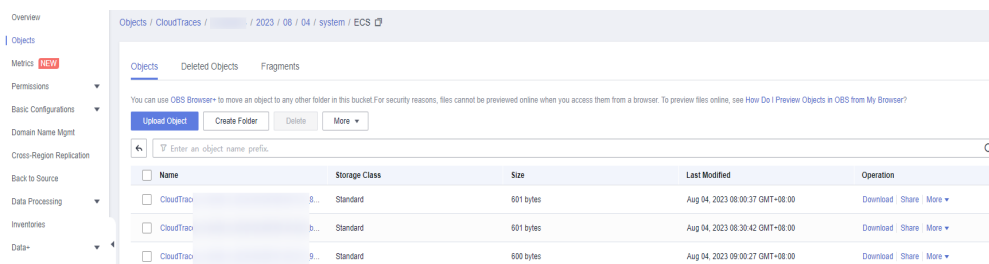
 **NOTE**

The OBS bucket name and trace file prefix are user-defined, and other parameters are automatically generated.

Downloading the file will incur request fees and traffic fees.

For details about key fields in the CTS trace structure, see [Trace Structure](#) and [Example Traces](#).


**Figure 10-2** Viewing trace file content




6. Decompress the downloaded package to obtain a JSON file with the same name as the package. Open the JSON file using a text file editor to view traces.

## Querying Traces Transferred to LTS

If you enable **Transfer to LTS** when configuring a tracker, traces will be transferred to the **CTS/{Tracker Name}** log stream for long-term storage. **{Tracker Name}** indicates the name of the current tracker. For example, the log stream path of the management tracker is **CTS/system-trace**.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and choose **Management & Governance > Cloud Trace Service**. The CTS console is displayed.
- Step 3** Choose **Tracker List** in the navigation pane on the left.
- Step 4** Click an LTS log stream in the **Storage** column.
- Step 5** On the **Log Stream** tab page in the **CTS** log group page, select the **{Tracker name}** log stream to view trace logs.

For details about key fields in the CTS trace structure, see [Trace Structure](#) and [Example Traces](#).

**Step 6** Click  to download the log file to your local PC.

 **NOTE**

Each time you can download up to 5,000 log events. If the number of selected log events exceeds 5000, you cannot download them directly from LTS. Transfer them to OBS and then download them from OBS.

----**End**

# 11 Change History

---

Released Date	Description
2024-05-24	This issue is the first official release.